
В. Г. Иваненко (д. т. н., профессор), И. А. Кириллов
Московский инженерно-физический институт (государственный университет)

ЗАЩИТА АВТОРСКОГО ПРАВА НА АУДИОДААННЫЕ С ПОМОЩЬЮ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Рассматриваются проблема защиты авторских прав на цифровые аудиоданные и способ ее решения с помощью цифровых водяных знаков. Приводятся и анализируются основные методы встраивания цифровых водяных знаков в аудиосигналы.

Бурно развивающиеся глобальные сети предоставляют практически неограниченные возможности для распространения информации. Возможность использовать, модифицировать, копировать без потери качества цифровые данные становится общедоступной. Такое интенсивное использование цифровых данных остро поднимает проблему защиты авторского права на них.

Проблема защиты авторского права на данные, представленные в электронном виде, включает в себя, помимо защиты прав собственности и доказательства прав на собственность (распространение), проблему защиты от несанкционированного копирования. Проблема защиты от несанкционированного копирования заключается в разрешении законного копирования (например, резервного) и блокировании случаев незаконного копирования. Однако определить законность копирования часто представляется невозможным. Поэтому средства защиты авторских прав зачастую запрещают любое копирование, нарушая тем самым права пользователей [1].

Решение проблемы защиты авторского права — процесс сложный. Эта проблема может быть решена лишь огромным комплексом мер и средств, как технических, так и правовых. Среди технических средств защиты авторского права в первую очередь стоит отметить шифрование данных. С помощью криптографических средств возможно обеспечить контроль доступа к данным, сделав их недоступными для неавторизованных пользователей. Однако при преодолении криптографической защиты контроль над доступом и распространением информации теряется. Среди технических средств защиты от несанкционированного копирования стоит отметить подход, основанный на блокировании опций копирования на различных устройствах воспроизведения цифровой информации, таких как CD и DVD-проигрыватели. Однако на сегодняшний день подобный подход не в состоянии эффективно ограничить неправомерное копирование цифровых данных.

Существует еще один подход к защите авторских прав на цифровые данные, основанный на применении цифровых водяных знаков (ЦВЗ). Концепция цифровых водяных знаков возникла при попытке решить проблему защиты авторских прав в области цифровых данных. Цифровой водяной знак — это данные о владельце или авторе, перманентно встроенные в цифровые аудиоданные, видео, изображение или текст, которые могут быть обнаружены и извлечены специальными способами для предъявления претензий. Цифровой водяной знак встраивается в несущие данные таким образом, что он неотделим от них. Данные со встроенным в них цифровым водяным знаком являются общедоступными, но перманентно помеченными [2]. В отличие от криптографических средств защиты, целью которых является ограничение доступа к данным неавторизованных пользователей, цифровые водяные знаки позволяют получить доступ к информации всем желающим, однако если возникает вопрос о правах на эту цифровую информацию, то встроенный ЦВЗ позволяет определить владельца.

Особенно актуально в настоящее время стоит вопрос о защите авторских прав на цифровые аудиоданные. Под цифровыми аудиоданными обычно понимают оцифрованный или синтезированный звук, представленный в виде аудиофайлов различных форматов. Распространение аудиофайлов в глобальных сетях и их использование во многих случаях носят незаконный характер. Цифровые водяные знаки могут помочь в решении проблем, связанных с защитой авторских прав на цифровые аудиоданные [3].



Встраивание цифрового водяного знака в аудиосигналы — это процесс встраивания определенного пользователем потока битов в цифровое аудио таким образом, что искажение, вызванное добавлением этого битового потока, оказывается незначительным для восприятия [4]. В общем случае встраивание цифрового водяного знака в аудиосигнал можно представить следующим образом: $A^{op} \times K \times W \rightarrow A^{цвз}$, где A^{op} — контейнер, представляющий собой оригинальный аудиосигнал, K — ключ внедрения, W — цифровой водяной знак, $A^{цвз}$ — полученный в результате встраивания аудиосигнал со встроенной информацией. Процесс извлечения ЦВЗ из аудиосигнала $A^{цвз}$ можно представить как $A^{цвз} \times K' \rightarrow W$, где ключ K' может быть равен ключу K , а в качестве полученного W может выступать не только встроенный ранее цифровой водяной знак, но и какая-либо информация, подтверждающая его наличие в аудиосигнале $A^{цвз}$.

Встроенные цифровые водяные знаки извлекаются при помощи процесса, обратного тому, с помощью которого они были встроены. Это означает, что любая система цифровых водяных знаков состоит как минимум из двух частей: системы встраивания цифровых водяных знаков и системы их извлечения. Для того чтобы система встраивания цифровых водяных знаков считалась надежной, она должна удовлетворять следующим требованиям:

- скрываемый цифровой водяной знак не должен вносить в сигнал искажения, воспринимаемые системой слуха человека;
- попытка удаления цифрового водяного знака должна приводить к заметному повреждению контейнера;
- цифровой водяной знак не должен вносить заметных изменений в статистику контейнера;
- цифровой водяной знак должен быть стойким к различного рода преобразованиям аудиосигнала (добавлению шумов, сжатию с потерями, фильтрованию, аналогово-цифровому и цифро-аналоговому преобразованиям и др.).

Методы встраивания цифрового водяного знака в аудиосигналы основываются на использовании особенностей слуховой системы человека, которую можно представить как анализатор частотного спектра, обнаруживающий и распознающий сигналы в диапазоне 20–20000 Гц. Систему слуха человека можно смоделировать как 26 пропускающих фильтров, полоса пропускания которых увеличивается с увеличением частоты [5]. Система слуха человека различает изменения фазы сигнала слабее, нежели изменения амплитуды или частоты, а также является чувствительной к аддитивному белому шуму [6].

На сегодняшний день существует большое количество методов встраивания цифровых водяных знаков в аудиосигналы, абсолютное большинство которых основывается на следующих методах встраивания информации (и является их развитием): методы кодирования наименее значащих бит, методы фазового кодирования, методы расширения спектра, методы встраивания информации за счет изменения времени задержки эхосигнала и методы маскирования цифровых водяных знаков.

Метод кодирования наименее значащих бит использует для встраивания временную область и позволяет встраивать информацию путем замены наименее значащих бит цифровых отсчетов аудиосигнала, представленных двоичной последовательностью [6]. Метод обеспечивает высокую пропускную способность и позволяет встраивать до 44 килобит информации в секунду аудиопоследовательности с частотой дискретизации 44 кГц. Главным его недостатком является слабая устойчивость к изменениям контейнера (робастность). Встроенная информация может быть легко уничтожена практически любым преобразованием несущего аудиосигнала. В настоящее время для улучшения робастности метода применяются различные подходы. Например, чтобы сделать цифровой водяной знак более устойчивым к локализованному фильтрованию, используется псевдослучайный генератор чисел для распределения цифрового водяного знака по всей аудиопоследовательности случайным образом. В последнее время часто предлагается использовать метод наименее значащих бит не во временной области, а в частотной. В этом случае различными способами кодируются наименее значащие биты коэффициентов преобразований. Чаще других для этих целей используются дискретное преобразование Фурье, дискретное косинусное преобразование и вейвлет-преобразование.



Главная идея методов на основе расширения спектра состоит во встраивании узкополосного сигнала, представляющего собой цифровой водяной знак, в широкополосный канал (аудиосигнал) [6]. Методы, основанные на расширении спектра, обладают высокой устойчивостью к изменениям контейнера, но обеспечивают невысокую пропускную способность стегоканала. Для уменьшения вносимых искажений и улучшения других характеристик данной группы методов некоторыми авторами предлагаются методы, совмещающие методы расширения спектра и психоакустические методы [7].

Методы встраивания информации за счет изменения времени задержки эхосигнала позволяют встраивать цифровые водяные знаки путем изменения задержки между сигналом и введенным в аудиопоследовательность и неслышимым (при определенной начальной амплитуде, скорости затухания и задержки) эхом. Метод обладает невысокой пропускной способностью, и потому большинство его модификаций призваны улучшить этот параметр. Так как эхо воспринимается системой слуха человека лишь как дополнительный резонанс, данные методы обладают хорошей незаметностью [6, 8].

Популярны в последнее время методы перцепционного (аудиального) маскирования и методы, использующие психоакустические модели [2, 7].

Методы, основанные на фазовом кодировании, используют для встраивания цифрового водяного знака слабую чувствительность системы слуха человека к незначительным изменениям фазы аудиосигнала [6]. Встраивание цифрового водяного знака методом кодирования фазы аудиосигнала — это метод, при котором фаза начального сегмента аудиосигнала модифицируется в зависимости от внедряемых данных. Фаза последующих сегментов согласовывается с ним для сохранения разности фаз, поскольку к разности фаз человеческое ухо более чувствительно. Фазовое кодирование является одним из наиболее эффективных способов кодирования по критерию отношения сигнал—шум. Методы фазового кодирования обеспечивают невысокую пропускную способность стегоканала, которая в экспериментальных результатах варьируется от 8 до 32 бит в секунду в зависимости от частоты дискретизации аудиосигнала. Для улучшения характеристик данной группы методов можно предложить несколько направлений: изменение способа кодирования бита информации для уменьшения влияния изменений абсолютной фазы аудиосигнала на качество звучания, использование всех имеющихся в аудиосигнале каналов для увеличения пропускной способности стегоканала, использование в процессе кодирования специальных маркеров синхронизации для обеспечения более надежного извлечения цифрового водяного знака. Возможно также применение адаптивных моделей кодирования информации к данной группе методов.

В последнее время появляются новые методы встраивания цифровых водяных знаков в аудиосигналы. Круг задач, решаемых с помощью цифровых водяных знаков, постоянно расширяется. Существуют алгоритмы встраивания цифровых водяных знаков, работающие в реальном времени [9]. Такие методы позволяют использовать цифровые водяные знаки в приложениях интернет-радиовещания. Методы встраивания цифровых водяных знаков в аудиосигналы постоянно улучшаются, становясь более устойчивыми к удалению их из несущего аудиосигнала и более «незаметными». При этом решаются проблемы, связанные с одновременным заявлением о правах на цифровые аудиоданные нескольких лиц или организаций. Крупнейшие производители программного обеспечения представляют свои продукты с возможностями встраивания в аудиофайлы цифровых водяных знаков для решения проблем, связанных с пиратством [10]. Таким образом, проблема защиты авторских прав на цифровые аудиоданные далека от своего полного решения, главный путь к которому — применение перспективной и быстро развивающейся технологии цифровых водяных знаков.

СПИСОК ЛИТЕРАТУРЫ:

1. Ларичев В. Д., Трунцевский Ю. В. Защита авторского права в аудиовизуальной сфере. Уголовно-правовой и криминологический аспекты. 2004 г. — 352 с.



-
2. Chun-Shien Lu. Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing, 2005.
 3. Bassia P., Pitas I. Robust audio watermarking in the time domain. Department of Informatics, University of Tressaloniki. <http://poseidon.csd.auth.gr/voyatzis/creus>.
 4. Katzenbeisser S., Fabien A., Petitcolas P. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House computing library, 2000.
 5. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. 2002. — 272 с.
 6. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for Data Hiding // IBM System Journal. 1996. 5 (3&4). P. 313–336.
 7. Ricardo A. Garcia. Digital Watermarking of Audio Signals Using a Psychoacoustic Auditory Model and Spread Spectrum Theory. University of Miami, 1999.
 8. Gruhl D., Lu A., Bender W. Echo Hiding, Information Hiding Workshop. Cambridge, 1996.
 9. Cassuto Y., Lustig M., Mizrahy S. Real-Time Digital Watermarking System for Audio Signals Using Perceptual Masking. Signal and Image Processing Lab. Faculty of EE. Technion IIT. Haifa, Israel. www.sipl.technion.ac.il.
 10. Digital Audio Watermarking, Technical Pre-Release/Prototype Product Overview. Microsoft Corporation, 2006. http://download.microsoft.com/download/d/6/b/d6bde980-5568-4926-8c71-dea63befed64/audio_watermark.

Н. Ю. Налютин, С. В. Сеницын, О. И. Хлытчиев
Московский инженерно-физический институт (государственный университет)

СИСТЕМА УПРАВЛЕНИЯ КОНФИГУРАЦИЯМИ ДОКУМЕНТОВ В ПРОГРАММНЫХ ПРОЕКТАХ

В работе рассматривается проблема построения системы управления конфигурациями документов и вычисления их состояний применительно к программным проектам. Предлагается метод построения системы документооборота, основанной на динамике самих документов, метод выявления основных типов документов и их жизненных циклов. Рассматривается метод вычисления состояний конфигураций документов и способы упрощения задания правил вычисления.

Введение

Практически любая компания, занимающаяся разработкой и верификацией программных систем, сталкивается с необходимостью хранить и обрабатывать огромное количество информации. Чем сложнее проект, чем выше его критичность и значимость, тем выше требования к процессу управления данными. Более того, для обеспечения гарантии качества выходного продукта необходимо установить и поддерживать определенные процессы, регламентируемые деятельностью компании и отраслевыми стандартами.

Задачи хранения, управления и обеспечения безопасности документов¹ решаются системами документооборота, которые управляют информацией и доступом к ней в соответствии с моделями бизнес-процессов предприятия.

Такие системы должны поддерживать как основной процесс предприятия — разработку программной системы, так и все обеспечивающие процессы, реализующие инфраструктуру, необходимую для функционирования предприятия.

Важнейший обеспечивающий процесс — процесс управления конфигурациями, который позволяет предотвратить хаотическое развитие процессов предприятия и обеспечить гарантии того, что все изменения, вносимые в документы, учитываются и санкционируются в соответствии с принятыми технологическими и бизнес-процессами. Управление конфигурациями контролирует эволюцию и

¹ Под документами следует понимать некий набор структурированной информации, в общем случае — произвольный объект.

