А. В. Гурин
А. А. Жарких
В. Ю. Пластунов

Технологии встраивания цифровых водяных знаков в аудиосигнал

Под общей редакцией
профессора А. А. Жарких

Москва
Горячая линия - Телеком
2015

УДК 621.391:[002.1-028.17:004.056.53:004.942]
ББК 32.811.3+32.973−018.2+22.18
Г95

Рецензенты: доктор филол. наук, профессор, директор Института прикладной и математической лингвистики Московского Государственного Лингвистического Университета *Р. К. Потапова*; Лаборатория региональных информационных систем Института информатики и математического моделирования технологических процессов Кольского научного центра РАН, ученый секретарь ИИММ КНЦ РАН, кандидат техн. наук *А. М. Фёдоров*

Гурин А. В., Жарких А. А., Пластунов В. Ю.

Г95 Технологии встраивания цифровых водяных знаков в аудиосигнал / Под общей редакцией А. А. Жарких. − М.: Горячая линия − Телеком, 2015. − 116 с.: ил.

ISBN 978-5-9912-0515-3.

Представлены различные аспекты одного из наиболее перспективных направлений стеганографии − технологий встраивания цифровых водяных знаков (ЦВЗ) в аудиосигнал. Приведены общие принципы встраивания ЦВЗ. Рассмотрены вопросы, связанные с встраиванием ЦВЗ в аудиосигналы − физика звука, физиология восприятия звука человеком, принципы цифро-аналогового и аналого-цифрового преобразования сигналов, а также некоторые форматы аудиофайлов. Обсуждаются перспективы развития технологий встраивания ЦВЗ в аудиосигнал. Технологии встраивания ЦВЗ представлены как известными, так и разработанными авторами новыми методами встраивания данных в аудиосигнал.

Для специалистов в области защиты информации, будет полезна аспирантам и студентам старших курсов.

Адрес издательства в Интернет WWW.TECHBOOK.RU

ISBN 978-5-9912-0515-3

© А. В. Гурин, А. А. Жарких, В. Ю. Пластунов, 2015
© Издательство «Горячая линия − Телеком», 2015

Предисловие редактора

Бурное развитие компьютерных и телекоммуникационных технологий требует исследования существующих и развития новых методов защиты информации. Криптографические методы защиты компьютерной информации изложены во многих руководствах, реализованы в общепризнанных на мировом уровне стандартах и жестко регламентированы международным законодательством. Иная ситуация сложилась со стеганографическими методами защиты компьютерной информации. Криптографические методы были активно развиты уже тогда, когда компьютеры не использовались. Методы стеганографии получили активное развитие только в последние 20 лет. Одно из направлений стеганографии — встраивание цифровых водяных знаков (ЦВЗ) в контейнеры, представляющие собой файлы разнородных данных.

Авторы предприняли попытку систематического изложения различных аспектов технологий встраивания ЦВЗ в аудиосигнал. Под аудиосигналом понимается цифровая последовательность его отсчетов. В нескольких разделах описываются общие принципы стеганографии, выделяется встраивание ЦВЗ как один из методов стеганографии, анализируются области применения ЦВЗ. Далее представлены физические и психофизиологические основы выбора аудиосигнала в качестве контейнера и обоснован выбор аудиоформата wav. Предлагаются три группы методов встраивания ЦВЗ, каждая из которых имеет свои преимущества и недостатки. Отражены взгляды авторов на перспективы развития технологий встраивания ЦВЗ в аудиосигнал.

Современная терминология в области стеганографии еще не совсем устоялась. Существует научно-техническое направление под названием «стегоанализ», который рассматривается иногда

как часть стеганографии, а иногда — как отдельное научное направление. В стегоанализе можно выделить два больших раздела. Первый характеризует исследование методов стеганографии разработчиками этих методов с целью улучшения характеристик. Второй предполагает включение в стеганографическую систему неавторизованного пользователя, который хочет прочитать, разрушить или модифицировать сообщение. Исследования в этом случае ориентированы на минимизацию рисков авторизованных пользователей. Авторы не включили в монографию никаких результатов исследований в области стегоанализа.

Работа над книгой была распределена между авторами следующим образом: А.В. Гурин работал над гл. 1, 2 и разд. 3.2; А.А. Жарких — над гл. 1, 2 и разд. 3.1, 3.3; В.Ю. Пластунов — над гл. 1, 2 и разд. 3.3. Введение, выводы и заключение ко всем главам написаны совместно А.В. Гуриным и А.А. Жарких. Студенты И.А. Хорев и М.А. Минасян принимали участие в написании подразд. 3.2.1 и 3.2.2 соответственно, за что авторы выражают им благодарность.

Авторы будут признательны тем читателям, которые обнаружат при прочтении книги неточности и опечатки. Все замечания Вы можете высылать по электронному адресу Zharkikh090107@mail.ru.

Введение

Актуальность технологий встраивания цифровых водяных знаков (ЦВЗ) в аудиосигнал обусловлена широким распространением объектов авторского права в виде аудиосигналов преимущественно в цифровой форме. Эти объекты распространяются при помощи средств цифровой дистрибуции, а именно «цифровых магазинов» (Itunes, Amazon), файлообменных сетей (BitTorrent, I2P). Технологии встраивания ЦВЗ используются в таких носителях, как Audio CD, Super Audio CD, DVD-Audio, Hi-MD, Blu-ray Disc и др. Распространение аудиосигналов в цифровом виде делает защиту на основе самих носителей информации малоэффективной.

В данной монографии представлены современные технологии встраивания цифровых водяных знаков (ЦВЗ) в аудиосигнал. Ее особенностью является описание оригинальных, разработанных авторами, методов встраивания данных в аудиосигнал. Известные ранее методы изложены в тщательной авторской проработке. Монография включает в себя введение, три основных главы и заключение. Каждый раздел завершается выводами, улучшающими понимание материала.

Первая глава посвящена понятию «цифровой водяной знак». В ней определяются понятия криптографии и стеганографии как методов защиты информации. В связи с определением стеганографии введены понятия контейнера, сообщения и стего-контейнера (стего). Проводится сравнение различных методов стеганографии с методами встраивания ЦВЗ. Кроме того, приводится небольшой исторический очерк о водяных знаках вообще и цифровых водяных знаках в частности. С точки зрения введенной терминологии, ЦВЗ может быть рассмотрен как разновидность сообщения в стеганографической системе. Также

проводится анализ применения ЦВЗ. Для полноты картины описаны требования, предъявляемые к технологиям ЦВЗ в системах обработки информации, анализируются критерии эффективности встраивания ЦВЗ. Завершается глава небольшой классификацией методов встраивания ЦВЗ, за которой следуют общие выводы.

Вторая глава отражает специфику монографии. В ней рассмотрены контейнеры только в виде аудиофайлов, кратко описана физика аудиосигнала, а также современные представления о восприятии аудиосигнала человеком. Это описание является важным, так как в большинстве стеганографических систем требуется, чтобы сообщение не было слышно, и не нарушалось естественное звучание контейнера. Аудиофайлы для записи звука в компьютерных системах представляют собой большие объемы цифровых данных. Несмотря на многообразие звуковых форматов файлов, все они базируются на теореме Котельникова. Перед записью в цифровой файл любого формата аналоговый аудиосигнал преобразуется в устройстве АЦП. Соответственно, перед воспроизведением цифровых данных из аудиофайла любого формата, они преобразуются в устройстве ЦАП. Далее приводится краткая характеристика нескольких форматов аудиофайлов, которые предполагают дополнительные преобразования для оптимизации аудиосистемы. С методической точки зрения предлагается анализировать файл только формата wav, так как в нем данные представлены в том виде, который им предписывает теорема Котельникова. Вторая глава также завершается общими выводами.

В третьей главе представлены три различных группы методов и алгоритмы встраивания ЦВЗ в аудиосигнал. К первой группе относятся методы замены наименее значащих бит, ко второй — перестановочные, а к третьей — нелинейные методы. Отметим особенности каждой из этих групп.

Методы замены наименее значащих бит являются, пожалуй, первыми, которые стали применять в стеганографии. В силу их простоты, в большинстве источников они описываются недостаточно подробно. В данной книге эта группа методов представлена несколькими вариантами, а именно: с возможностью замены одного наименее значащего бита, нескольких наименее значащих бит, целого блока бит. Кроме того, представлены методы, в которых блоки с заменой НЗБ чередуются с блоками пауз, где НЗБ не заменяются. Приводится также модифицированный метод НЗБ, позволяющий противостоять атакам типа

разрушения и модификации. Отдельно можно отметить метод НЗБ, позволяющий точно восстановить не только сообщение, но и контейнер. Вторую группу составляют перестановочные методы, особенностью которых является то, что после их применения не изменяется гистограмма контейнера. В монографии представлена два метода: при одном возможно восстановление исходного контейнера, при другом такое восстановление невозможно. Третья группа — нелинейные методы. Их особенность заключается в том, что сообщение должно иметь ту же структуру, что и контейнер, т. е. являться аудиофайлом. В работе представлены два нелинейных метода — одноканальный и двухканальный. Как и первые две главы, гл. 3 завершается общими выводами

В заключении приводятся основные выводы по результатам исследования, а также перспективы развития технологий встраивания ЦВЗ в перспективных системах защиты информации. Завершается монография списком использованных источников.