Предисловие

Стеганография — это искусство отправки скрытых или невидимых сообщений.

Современная стеганография, как правило, имеет дело с информацией в электронной форме, а не с физическими объектами и текстами. Это имеет смысл для целого ряда причин. Прежде всего, размер информации, как правило, (обязательно) весьма мал по сравнению с размером данных, в которых она должна быть скрыта (текстовый контейнер). Во-вторых, само извлечение может быть автоматизировано, когда данные в электронной форме, так как компьютеры могут эффективно обрабатывать их и выполнить алгоритмы, необходимые для получения сообщения. Электронные данные также часто включают в себя избыточные, ненужные и незаметные пространства данных, которые можно использовать, чтобы скрыть сообщения. В каком-то смысле эти пустые пространства обеспечивают своего рода «скрытый отсек», в который могут быть вставлены секретные сообщения и отправлены принимающей стороне.

Стеганографическая информация может быть скрыта почти везде, и некоторые объекты контейнера больше подходят для скрытия информации, чем другие.

Стеганография в изображениях стала более популярной в последние годы, чем другие виды стеганографии, возможно из-за большого потока изображений в электронном виде, доступного с появлением цифровых камер и высокоскоростной интернет-передачи. Стеганография в изображении часто включает в себя скрытие информации в естественно возникающих «шумах» изображения и предоставляет хорошие наглядные примеры для таких методов.

Развитие вычислительной техники в последнее время дало новый толчок в развитии компьютерной стеганографии. Исследуются новые области применения. Скрываемые сообщения теперь встраиваются в цифровые данные (изображения, видео и аудиофайлы). Также существуют методы по внедрению данных в текстовые файлы и даже в исполняемые файлы программ.

В учебном пособии рассмотрены основные методы и алгоритмы стеганографии, а также анализируются современные методы стеганоанализа.

Учебное пособие состоит из семи глав.

В **первой главе** рассмотрены история появления и современное состояние стеганографии. Приводятся основные задачи и определения стеганографии. Даётся классификация методов скрытия данных в контейнерах различной природы. На основании анализа структуры цифровой стеганографической системы рассматриваются методы и алгоритмы современной компьютерной стеганографии (КС). Приводятся методы оценки качества стеганосистемы.

Во **второй главе** рассматриваются важные для практического использования вопросы сокрытия информации в текстовых документах. Подробно излагаются синтаксические и семантические методы, а также критерии оценочных тестов. Анализируется сокрытие информации в файлы формата PDF, RTF и внедрение скрываемого текста в текстовом редакторе Word. Рассматривается сетевая стеганография для скрытия данных, передаваемых по каналам связи. Анализируется комбинированный метод с использованием модификации полей заголовков IP и TCP. Рассматриваются методы скрытой связи с использованием ключа.

В **третьей главе** рассматриваются методы модификации аудиосигналов в стеганографических системах скрытия данных. Приводится оценка степени пригодности аудиосигналов для стеганографической модификации. Анализируется кодирование наименее значащих бит (временная область), метод фазового кодирования (частотная область); широкополосное кодирование; эхо-кодирование. Рассматриваются алгоритмы встраивания информации путем модификации спектральных характеристик сигналов аудиоконтейнеров. В заключение анализируются вопросы применения водяных аудиознаков в индустрии звукозаписи.

В **четвертой главе** рассматриваются вопросы скрытия информации в неподвижных изображениях. Здесь рассматривается модель системы человеческого зрения, а также физиологические особенности человеческого восприятия, высокоуровневые (психофизиологические) особенности человеческого восприятия. Проводится классификация методов маркировки изображений цифровыми водяными знаками. Подробно анализируются алгоритмы скрытия данных в пространственной области изображений; методы замены наименее значащего бита; метод псевдослучайной перестановки; метод блочного скрытия, метод Куттера–Джордана–Боссена, алгоритм Брайндокса, а также некоторые другие.

Анализируются методы скрытия данных в частотной области изображения на основе информативности коэффициентов дискретного косинусного преобразования изображений. Анализируется методы относительной замены величин коэффициентов ДКП (метод Коха и Жао), метод Бенгама–Мемона–Эо–Юнга, алгоритмы Фрид-

риха и Хсу, методы расширения спектра (в том числе расширение спектра прямой последовательностью). Рассматривается программная реализация внедрения цифрового водяного знака в контейнер методом расширения спектра прямой последовательностью.

В заключительной части главы анализируются и другие методы скрытия данных в пространственной области, такие как использование псевдослучайного шаблона, встраивание в одно изображение нескольких битов или логотипов. Анализируются методы повышения устойчивости ЦВЗ к атакам, устойчивость к геометрическим преобразованиям.

Пятая глава посвящена рассмотрению вопросов внедрения водяных знаков на основе вейвлет-преобразований. Здесь проведена классификация алгоритмов внедрения водяных знаков, оперирующих в вейвлет-области. Анализируются алгоритмы с гауссовской последовательностью. Важное место в главе занимают вопросы внедрения ЦВЗ методом скалярного и векторного квантования. Анализируется встраивание ЦВЗ в изображения форматов сжатия с потерями JPEG и JPEG 2000.

Шестая глава посвящена вопросам встраивания водяных знаков в потоковое видео. Здесь рассматриваются корреляционные методы встраивания водяных знаков в область коэффициентов MPEG, а также встраивания путем модификации DC-коэффициентов. Анализируется оценка эффективности алгоритма встраивания водяных знаков в битовую область. Рассматривается реализация программного обеспечения для создания водяного знака и его обнаружения в частотной области видеопотоков H.264. Анализируется встраивание водяных знаков на основе анализа изменения сцен.

Седьмая глава посвящена некоторым вопросам стеганографического анализа. Рассматриваются статистические критерии обнаруживаемости стегосистем. В том числе: критерии относительной энтропии; критерий стойкости стегосистемы, основанный на вычислении расстояния Бхаттачариа; методы слепого стегоанализа. Подробно анализируется целевой стегоанализ для метода вложений, визуальный метод стегоанализа; стегоанализ на основе статистики 1-го и 2-го порядков.

Материал этих глав излагается доступным доходчивым языком и в целом отражает основные современные концепции построения стеганографии.

Материал глав не перегружен математическими выкладками, в целом отражает современное состояние вопроса в этой области и будет полезен практикующим специалистам в области информационной безопасности.

Основное отличие предлагаемого пособия от ранее изданных заключается в том, что здесь помимо теоретических аспектов и алгоритмов рассмотрено большое число программно выполненных примеров с использованием современных пакетов прикладных программ Mathworks MatLab и Mathcad, а также языков программирования Python, C++, C# и других.

Учебное пособие предназначено для бакалавров и магистрантов, обучающихся по направлению 11.03.02 и 11.04.02 «Инфокоммуникационные технологии и системы связи» и может быть использовано для выполнения магистерских диссертаций, дипломных и курсовых работ.

В основу учебного пособия положен курс лекций, читаемых одним из авторов бакалаврам и магистрантам МТУСИ.

Особую признательность авторы выражают рецензентам книги: зав. кафедрой «Информационная безопасность телекоммуникационных систем» Южного федерального университета, г. Ростов-на-Дону, Заслуженному работнику высшей школы РФ, доктору технических наук, профессору К.Е. Румянцеву и профессору кафедры «Информационная безопасность» МГТУ им. Баумана, доктору ф.-м. наук, профессору М.А. Басарабу.