Тойтонов Дмитрий Николаевич
канд. пед. наук, студент
Христофорова Аэлита Григорьевна
преподаватель
Гаенкова Ирина Владимировна
канд. пед. наук, доцент
Технологический институт
ФГАОУ ВПО «Северо-Восточный федеральный
университет им. М.К. Аммосова»
г. Якутск, Республика Саха (Якутия)

АНАЛИЗ МЕТОДОВ СТЕГАНОГРАФИИ

Аннотация*: в статье приводится сравнительно-сопоставительный анализ технологий стеганографии и криптографии.*

Ключевые слова*: стеганография, криптография, защита информации.*

В настоящее время являются актуальными научные исследования в области защиты информации, в частности, компьютерной стеганографии, так как у пользователей существует потребность защиты прав собственности на цифровую информацию, защиты различных информационных систем от утечки конфиденциальных данных, внешних и внутренних угроз и т. д.

Стеганография – это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо и т. д. Стеганографию обычно используют совместно с методами криптографии и таким образом ее дополняют.

Преимущество стеганографии над криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех

странах, в которых запрещена криптография. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий (таблица 1).

Таблица 1

Сравнение технологий стеганографии и криптографии

№	*Стеганография*	*Криптография*
1.	Защищает информацию о наличии каких-либо сообщений.	Защищает содержание сообщения.
2.	Помещение информации в какой-либо нейтральный объект (контейнер) (текстовый, графический, аудио- или видеофайл) и незаметное распределение в нем информации.	Использование ключа в процессе шифровки и дешифровки и алгоритма обеспечивающего, дешифрование только с помощью ключа.
3.	Определение «гнезд» выступает авторским шифром такого сообщения. В «гнезда» вносится информация, порядок ее внесения, внешняя незаметность изменений контейнера, сохранение различных статистических характеристик контейнера.	Алгоритмы с использованием ключа делятся на два класса: симметричные (или алгоритмы секретным ключом) и ассиметричные (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки.

Е.А. Голубев и Г.В. Емельянов считают, что по существу стеганография – это наложение на реализацию сильного цифрового медиа процесса слабого шумового процесса, адекватного маскируемой (скрываемой) информации. Это наложение может происходить в естественный цифровой процесс (форматы без сжатия) либо в его спектральное представление – дискретные косинусные преобразования, вейвлет-преобразования – основы форматов сжатия с потерями, разработанных для уменьшения технической избыточности с учетом требований психофизиологических моделей восприятия звука и визуальных образов [1].

Особое внимание, по мнению Е.А. Голубева и Г.В. Емельянова, следует уделить стеганографии как, с одной стороны, новому источнику потенциальных угроз информационной безопасности за счет ослабления эффективности государственного контроля инфокоммуникационной среды, так, с другой стороны,

новому инструменту защиты информации от доступа, искажения или подделки [1].

М.О. Жмакин выражает общий процесс стеганографии простой формулой:

$$К + СС + СКл = СК,$$

где:

– контейнер (К) – любая информация, предназначенная для встраивания тайных сообщений;

– скрываемое (встраиваемое) сообщение (СС) – тайное сообщение, встраиваемое в контейнер;

– стегоключ (СКл) – секретный ключ, необходимый для скрытия (шифрования) информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей;

– стегоконтейнер (СК) – контейнер, содержащий встроенное сообщение;

– стеганографический канал (стегоканал) – канал скрытой передачи информации [2].

В настоящее время стеганографию можно условно разделить на три раздела:

1. Классическая стеганография, которая включает в себя все «некомпьютерные методы».

2. Компьютерная стеганография – направление классической стеганографии, основанное на особенностях компьютерной платформы и использовании специальных свойств компьютерных форматов данных.

3. Цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, что вызывает некоторые искажения этих объектов. Чаще всего в этих целях используется избыточность аудио и визуальной информации.

В сети Интернет имеется большое количество свободно распространяемых и легкодоступных программ, позволяющих осуществлять пользователям стеганографическое сокрытие данных. Такая легкодоступность стеганографического

программного обеспечения привела к появлению широких возможностей несанкционированного распространения информации, которые трудно контролировать, например, в локальных сетях коммерческих предприятий или государственных учреждений. Поэтому во всем мире ведутся активные исследования по разработкам методов выявления сокрытий информации в нейтральных объектах (контейнерах) (таблица 2).

Таблица 2

Школы стеганографии [4]

Конференции по стеганографии			
1	Ежегодная международная конференция «Information Hiding» («IH», «Сокрытие информации»).	Издательство «Springer в серии LNCS» (Lecture Notes on Computer Science).	
2	Ежегодная международная конференция «International Workshop on Digital Watermarking» («IWDW»).		
Школы стеганографии			
№	Учебное заведение	Факультет	Лидеры школы
1	Кампус государственного университета штата Нью-Йорк (SUNY, State University of New York), г. Бинхемптон США	Факультет электрического и компьютерного машиностроения (Department of Electrical and Computer Engineering), Лаборатория внедрения цифровых данных (Digital Data Embedding Laboratory)	Джессика Фридрих, Мирослав Гольян, Ян Кодовски, Войтех Холуб
2	Дрезденский технический университет (Dresden University of Technology), Германия	Факультет компьютерных наук (Department of Computer Science)	Андреас Вестфельд, Андреас Пфитцманн, Рейнер Боме, Элке Франц
3	Оксфордский университет, Великобританя	Факультет компьютерных наук (Department of Computer Science)	Эндрю Кера
4	Университет Ингемара Кокса, г. Лондон, Англия	Факультет компьютерных наук (Department of Computer Science)	Ингемара Кокса – цифровые водяные знаки
5	Бизнес-университет, г. Гуандонг (Guangdong University of Business Studies), Китай	Факультет компьютерных наук	Юн Чжань

Стеганоанализ – это выявление стеганографии, принципы и методы. Исследователи А.С. Сизова, Е.И. Никутина, С.В. Котенко, предлагая новые методы

стегоанализа, уделяют внимание именно методам, предназначенным для решения первичной задачи стегоанализа – задачи обнаружения факта присутствия скрытой информации [3]. В связи с этим выделяются следующие методы стеганографического анализа:

– статистические;

– сигнатурные;

– целенаправленные;

– слепые;

– количественные.

Статистические методы стегоанализа основываются на анализе таких статистических характеристиках, как коэффициенты корреляции, оценки энтропии, условные распределения, вероятности появления и зависимости между элементами последовательностей и др.

Сигнатурные методы стегоанализа основываются на поиске предопределённых сигнатур – последовательностей битов, с высокой вероятностью указывающих на присутствие в анализируемом файле информации, скрытой соответствующей стегосистемой.

Целенаправленные методы стегоанализа используют знания о методах стеганографического скрытия информации и опираются на концепцию различающих статистик.

Слепые методы стегоанализа используют некоторые парадигмы скрытия информации и основываются на предположении о том, что естественное изображение может быть охарактеризовано некоторым набором численных характеристик.

Количественные методы стегоанализа основываются на оценке количества изменений контейнера, вызванных встраиванием стегосообщения.

Список литературы

1. Голубев Е.А. Стеганография как одно из направлений обеспечения информационной безопасности / Е.А. Голубев, Г.В. Емельянов // T-Comm: Телекоммуникации и транспорт. – 2009. – С. 185–186.

2. Жмакин М.О. Стеганография и перспективы ее применения в защите печатных документов // Безопасность информационных технологий. – 2010. – С. 74–77.

3. Сизов А.С. Обзор и тенденции развития методов анализа стеганографических сообщений / А.С. Сизов, Е.И. Никутин, С.В. Котенко // Известия Юго-Западного государственного университета. Серия: управление, вычислительная техника, информатика, медицинское приборостроение. – 2013. – С. 43–48.

4. Елисеев А.С. Исследование и разработка методов и алгоритмов стеганографического анализа отдельных контейнеров и их связанных наборов: Дисс. на соиск. уч. ст. канд. тех. наук. – Ростов н/Д, 2013. – С. 4.