ЗАЩИТА ИНФОРМАЦИИ СТЕГАНОГРАФИЧЕСКИМИ МЕТОДАМИ

Павлова Т.Н.
Научный руководитель: Суханова Н.В. – к.т.н., доцент
Кафедра «Компьютерные системы управления» ФГБОУ ВПО МГТУ «СТАНКИН»

В современном мире у любого человека есть доступ к информации, в том числе и закрытой. Для обеспечения большей защиты информации необходимо скрыть факт ее передачи.

Стеганография — метод скрытой передачи данных. В отличии от криптографии стеганография скрывает сам факт передачи информации. Криптография шифрует данные таким образом, что взломщик не может расшифровать сообщение не имея ключа. Шифр состоит из алгоритма и ключа. Алгоритм – открытая часть текста, ключ – секретная. Для повышения безопасности передачи сообщения, информацию сначала шифруют криптографическими методами, а затем скрывают ее с помощью стеганографии в контейнере.

Контейнером обычно является файл произвольного формата, например: аудио дорожка, графическое изображение или видео. Преимуществом стеганографии является то, что обнаружить или предсказать нахождение сообщения в контейнере достаточно сложно, так как сам контейнер несет в себе совершенно иную информацию. Более того, после обнаружения наличия сообщения в контейнере, необходимо вычислить стегоключ – секретный ключ, с помощью которого сокрыто сообщение. Методов использования стеганографии на данный момент существует достаточно много, что и определяет сложность задачи взлома стеганографического сообщения.

Рассмотрим следующие основные виды стеганографии:

1) Семаграммы.

Способ передачи скрытых сообщений с помощью образов, знаков и символов. Например жесты руками, цвет бумаги или используемых чернил при письме, порядок предметов расположенных на столе или подоконнике. Такие сообщения не привлекают к себе внимания и могут быть прочитаны только теми, кто знает о чем идет речь – у кого есть ключ.

2) Микроточки.

Способ передачи информации, при котором в отправляемое письмо, на любую букву или знак препинания, помещали микроточку. Микроточка содержала в себе текстовую или графическую информацию, видимую только под увеличительным стеклом. Факт передачи информации скрывает письмо, в котором речь идет на тему не интересующую взломщика. И только человек, знающий в какой момент и у кого будет контейнер может нейти скрытое сообщение.

В военное время очень часто прибегали к этому методу передачи информации. В наше же время вместо точки в письмо можно встроить

штрих код, который будет нести в себе гораздо больше информации чем может уместить микроточка.

Табл. 1. Методы стеганографии.

Методы	Краткая характеристика	Недостатки	Преимущества
Методы основанные на специальных свойствах электронных форматов данных			
Метод выбора определенных позиций букв (нулевой шифр)	Акростих - частный случай этого метода (например, начальные буквы каждой строки образуют сообщение)	1. Слабая производительность метода 2. Низкая степень скрытности 3. передача небольших объемов информации	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
Метод использования специальных свойств полей форматов	Метод основан на использовании скрытых полей для организации сносок и ссылок (например, использование черного шрифта на черном фоне)		
Метод использования имитирующих функций	Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение	1.Слабая производительность метода, передача небольших объемов информации	Результирующий текст не является подозрительным для систем мониторинга сети
Методы использования избыточности аудио и визуальной информации			
LSB (Least Significant Bit, наименьший значащий бит)	Метод основан на замене последних значащих битов в контейнере на биты скрываемого сообщения.	За счет введения дополнительной информации искажаются статистические характеристики цифровых потоков	Возможность скрытой передачи большого объема информации
Метод использующий особенностей форматов данных, использующи	Метод основан на том, что данные записываются не в цветовые компоненты, а в коэффициенты дискретного косинус-преобразования, которое	Малый объем скрываемых данных	Более стоек к геометрическим преобразованиям и обнаружению канала

х сжатие с потерей данных	осуществляется при сжатии		передачи

3) Цифровая стеганография.

Вид передачи тайной информации, основанный на встраивании сообщения в цифровые объекты. В данном случае сообщение искажает информацию стегоконтейнера, но поскольку используемые цифровые объекты являются мультимедиа-объектами (изображения, видео, аудио), они имеют порог чувствительности для человека, за которым среднестатистический гражданин не способен уловить никакую информацию. Пользуясь этим, сообщение встраивают именно в «слепые зоны» и человек не в состоянии определить наличия стеганографии. Помимо этого, аналоговые объекты содержат шум, который скрывает определение наличия скрытого сообщения с помощью аппаратуры.

Согласно таблице 1 метод наименее значащих битов является наиболее надежным и больше подходит для скрытой передачи данных больших объемов. Этот метод организует скрытое хранение и передачу конфиденциальной информации по открытым каналам связи. Передача графических файлов не привлекает к себе внимания. Файлы произвольного формата являются достаточно емким контейнером и могут содержать не одно, а несколько сообщений. Пустой контейнер (рис.1,а) не отличается от заполненного (рис.1,б) и при визуальном анализе нет возможности обнаружить наличие скрытого сообщения.

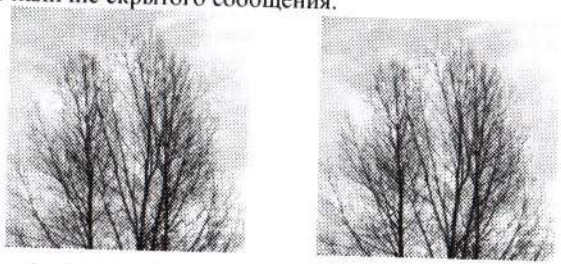


Рис. 1. а) пустой контейнер б) заполненный контейнер

В случае, когда сообщение расположено не по всему контейнеру, в неизмененные биты редактируют с целью усложнить задачу поиска и обнаружения стеганографического сообщения.

Выводы:

1. Для поставленной задачи - сокрытия факта передачи информации, наиболее подходит метод наименее значащих битов. Этот метод не привлекает к себе внимания, и является достаточно емким.
2. Как показано на рисунке 1, пустой контейнер и контейнер содержащий информацию неразличимы.

Библиографический список:

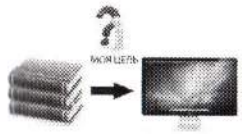
1. Позднеев Б.М., Кабак И.С., Суханова Н.В./Патент не изобретение 2481715 РФ МПК 7 H04L9/00. Способ блочного шифрования сообщений и передачи шифрованных данных с закрытым ключом/ ФГБОУ ВПО МГТУ «СТАНКИН» № 2011148733; заявл. 30.11.2011; опубл. 10.05.2013, Бюл. №13-13с.:ил.
2. Кабак И.С., Суханова Н.В., Позднеев Б.М./Патент не изобретение 2459367 РФ МПК 7 H04L9/00. Способ формирования переменного ключа для блочного шифрования и передачи шифрованных данных/ ФГБОУ ВПО МГТУ «СТАНКИН» № 2010129310; заявл. 16.07.2010; опубл. 20.08.2012, Бюл. №23-11с.:ил.

ИСПОЛЬЗОВАНИЕ ГИПЕРТЕКСТА В ОБУЧЕНИИ

Погребицкий А.С.

Научный руководитель: Рыбаков А.В. - к.т.н., доцент

Кафедра «Автоматизированных систем обработки информации и управления» ФГБОУ ВПО МГТУ «СТАНКИН»



Образование 21 века станет глобальным, ведь Интернет и другие современные средства связи не знают границ.

В будущем образование приобретет такие формы, как мобильное обучение; обучение на рабочем месте; встроенное обучение; постоянное обучение.

Будущее образования тесно связано с информационно-коммуникативными технологиями, особенно с Веб 3.0. Основными движущими силами современного образования являются Интернет и веб-технологии (рис. 1).

Рис. 1. Эволюция учебных технологий