



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

Методы обеспечения целостности информации

	<i>(наименование дисциплины (модуля) в соответствии с учебным планом)</i>
Уровень	бакалавриат
	<i>(бакалавриат, магистратура, специалитет)</i>
Форма обучения	очная
	<i>(очная, очно-заочная, заочная)</i>
Направление(-я) подготовки	09.03.02 «Информационные системы и технологии»
	<i>(код(-ы) и наименование(-я))</i>
Институт	кибербезопасности и цифровых технологий (ИКБ)
	<i>(полное и краткое наименование)</i>
Кафедра	Разработка программных решений и системное программирование
	<i>(полное и краткое наименование кафедры, реализующей дисциплину (модуль))</i>
Лектор	К.т.н. Ермакова Алла Юрьевна
	<i>(сокращенно – ученая степень, ученое звание; полностью – ФИО)</i>
Используются в данной редакции с учебного года	2023/24
	<i>(учебный год цифрами)</i>
Проверено и согласовано « ____ » _____ 2023 г.	
	<i>(подпись директора Института/Филиала с расшифровкой)</i>

Москва 2023 г.

Лекция 8. Методы стеганографии. Компьютерная стеганография

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, появилось новое направление в области защиты информации - компьютерная стеганография (КС). Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах).

Классификация методов компьютерной стеганографии

Подавляющее большинство методов компьютерной стеганографии (КС) базируется на двух ключевых принципах: · файлы, которые не требуют абсолютной точности (например, файлы с изображением, звуковой информацией и т.д.), могут быть видоизменены (конечно, до определенной степени) без потери своей функциональности. · органы чувств человека неспособны надежно различать незначительные изменения в модифицированных таким образом файлах и/или отсутствует специальный инструментарий, который был бы способен выполнять данную задачу.

В основе базовых подходов к реализации методов КС в рамках той или иной информационной среды лежит выделение малозначительных фрагментов этой среды и замена существующей в них информации информацией, которую необходимо скрыть. Поскольку в КС рассматриваются среды, поддерживаемые средствами вычислительной техники и компьютерных сетей, то вся информационная среда в результате может быть представлена в цифровом виде. Таким образом, незначительные

для кадра информационной среды фрагменты относительно того или иного алгоритма или методики заменяются фрагментами скрываемой информации.

Под кадром информационной среды в данном случае подразумевается определенная его часть, выделенная по характерным признакам. Такими признаками зачастую являются семантические характеристики выделяемой части информационной среды. Например, кадром может быть избрано какое-нибудь отдельное изображение, звуковой файл, Web-страница и т.д. Для существующих методов компьютерной стеганографии вводят следующую классификацию (рисунок 3).



Рисунок 3. Классификация методов компьютерной стеганографии

По способу выбора контейнера различают суррогатные (или так называемые эрзац-методы), селективные и конструирующие методы стеганографии. В суррогатных (безальтернативных) методах стеганографии полностью отсутствует возможность выбора контейнера, и для скрытия сообщения избирается первый попавшийся контейнер - эрзац-контейнер,

который в большинстве случаев не оптимален для скрытия сообщения заданного формата.

В селективных методах КС предусматривается, что скрытое сообщение должно воспроизводить специальные статистические характеристики шума контейнера. Для этого генерируют большое количество альтернативных контейнеров с последующим выбором наиболее оптимального из них для конкретного сообщения. Особым случаем такого подхода является вычисление некоторой хэш-функции для каждого контейнера. При этом для скрытия сообщения выбирается тот контейнер, хэш-функция которого совпадает со значением хэш-функции сообщения (то есть стеганограммой является избранный контейнер).

В конструирующих методах стеганографии контейнер генерируется самой стегосистемой. При этом существует несколько вариантов реализации. Так, например, шум контейнера может имитироваться скрытым сообщением.

Это реализуется с помощью процедур, которые не только кодируют скрываемое сообщение под шум, но и сохраняют модель изначального шума. В предельном случае по модели шума может строиться целое сообщение.

По способу доступа к скрываемой информации различают методы для потоковых (беспрерывных) контейнеров и методы для фиксированных (ограниченной длины) контейнеров.

По способу организации контейнеры, подобно помехоустойчивым кодам, могут быть систематическими и несистематическими.

В первых можно указать конкретные места стеганограммы, где находятся информационные биты собственно контейнера, а где - шумовые биты, предназначенные для скрытия информации (как, например, в широко распространенном методе наименее значащего бита). В случае несистематической организации контейнера такое разделение невозможно.

В этом случае для выделения скрытой информации необходимо обрабатывать содержимое всей стеганограммы. По используемому принципу скрытия методы компьютерной стеганографии делятся на два основных класса: методы непосредственной замены и спектральные методы.

Если первые, используя избыток информационной среды в пространственной (для изображения) или временной (для звука) области, заключаются в замене малозначительной части контейнера битами секретного сообщения, то другие для скрытия данных используют спектральные представления элементов среды, в которую встраиваются скрываемые данные (например, в разные коэффициенты массивов дискретно-косинусных преобразований, преобразований Фурье, Карунена-Лоева, Адамара, Хаара и т.д.).

Основным направлением компьютерной стеганографии является использование свойств именно избыточности контейнера-оригинала, но при этом следует принимать во внимание то, что в результате скрытия информации происходит искажение некоторых статистических свойств контейнера или, же нарушение его структуры. Это необходимо учитывать для уменьшения демаскирующих признаков. В особую группу можно выделить методы, которые используют специальные свойства форматов представления файлов:

- зарезервированные для расширения поля файлов, которые зачастую заполняются нулями и не учитываются программой;
- специальное форматирование данных (сдвиг слов, предложений, абзацев или выбор определенных позиций символов);
- использование незадействованных участков на магнитных и оптических носителях;
- удаление файловых заголовков-идентификаторов и т.д.

В основном для таких методов характерны низкая степень скрытности, низкая пропускная способность и слабая производительность.

По назначению различают стеганометоды собственно для скрытой передачи (или скрытого хранения) данных и методы для скрытия данных в цифровых объектах с целью защиты авторских прав на них.

По типам контейнера выделяют стеганографические методы с контейнерами в виде текста, аудиофайла, изображения и видео.

Метод замены наименее значащего бита

Метод замены наименее значащего бита (НЗБ, LSB - Least Significant Bit) наиболее распространен среди методов замены в пространственной области. Младший значащий бит изображения несет в себе меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, НЗБ - это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения.

При этом для изображения в градациях серого (каждый пиксель изображения кодируется одним байтом) объем встроенных данных может составлять 1/8 от общего объема контейнера. Если же модифицировать два младших бита (что также практически незаметно), то данную пропускную способность можно увеличить еще вдвое. Популярность данного метода обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах большие объемы информации (пропускная способность создаваемого скрытого канала связи составляет при этом от 12,5 до 30%).

Метод зачастую работает с растровыми изображениями, представленными в формате без компрессии (например, BMP и GIF). Метод НЗБ имеет низкую стеганографическую стойкость к атакам пассивного и активного нарушителей. Основной его недостаток - высокая чувствительность к малейшим искажениям контейнера. Для ослабления этой чувствительности часто дополнительно применяют помехоустойчивое кодирование.

Метод псевдослучайного интервала

В рассмотренном выше простейшем случае выполняется замена НЗБ всех последовательно размещенных пикселей изображения. Другой подход - метод случайного интервала, заключается в случайном распределении битов секретного сообщения по контейнеру, в результате чего расстояние между двумя встроенными битами определяется псевдослучайно.

Эта методика особенно эффективна в случае, когда битовая длина секретного сообщения существенно меньше количества пикселей изображения. Интервал между двумя последовательными встраиваниями битов сообщения может являться, например, функцией координат предыдущего модифицированного пикселя.

Методы сокрытия данных в пространственной области

Алгоритмы, описанные в данном в данном разделе, встраивают скрываемые данные в области первичного изображения. Их преимущество заключается в том, что для встраивания не нужно выполнять вычислительно сложные и длительные преобразования изображений. Цветное изображение S будем представлять через дискретную функцию, которая определяет вектор цвета $s(x,y)$ для каждого пикселя изображения (x,y) , где значение цвета задает трехкомпонентный вектор в цветовом пространстве.

Наиболее распространенный способ передачи цвета - это модель RGB, в которой основные цвета - красный, зеленый и синий, а любой другой цвет может быть представлен в виде взвешенной суммы основных цветов. Вектор цвета $s(x,y)$ в RGB-пространстве представляет интенсивность основных цветов. Сообщения встраиваются за счет манипуляций цветовыми составляющими $\{R(x,y), G(x,y), B(x,y)\}$ или непосредственно яркостью $\lambda(x,y) \in \{0, 1, 2, \dots, LC\}$. Общий принцип этих методов заключается в замене избыточной, малозначимой части изображения битами секретного

сообщения. Для извлечения сообщения необходимо знать алгоритм, по которому размещалась в контейнере скрытая информация.

Заклучение Стеганография, как метод защиты информации, появилась очень давно. Тем не менее данная наука не теряет своей актуальности и сейчас. В развивающемся мире высоких технологий задача сохранения информации обладателя в секрете остается первостепенной, поэтому стеганография тоже не стоит на месте.