Д.С. Гизунов, О.А. Демченко, Е.И. Никутин

МЕТОДИКА АВТОМАТИЗИРОВАННОГО ОБНАРУЖЕНИЯ СКРЫТОЙ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ ФАЙЛАХ

Бурное развитие электронных платежных систем, внедрение новых информационных технологий создает вместе с тем предпосылки к росту риска совершения экономических преступлений с использованием систем электронных платежей. Важной особенностью защиты систем электронных платежей является необходимость обеспечения безопасности каналов передачи платежных документов, обусловливающая требования к качеству передачи критичной к подделке информации. С другой стороны, стремительное развитие технологий цифровой передачи данных, в частности методов и средств обеспечения конфиденциальности информации в компьютерных сетях, привело к значительному возрастанию объемов информации, передаваемой с помощью стеганографических методов. Проведенный анализ [1-5] показал, что в настоящее время существует определенное отставание в развитии методов стегоанализа от методов стегосинтеза, хотя для некоторых методов синтеза в области цифровой стеганографии [3] разработаны соответствующие методы стегоанализа, формализованные описания которых встречаются во многих публикациях.

В ходе решения основной задачи стегоанализа (установление факта присутствия в контейнере скрытой информации [4, 5]) аналитиком могут использоваться реализации различных методов анализа. Однако при попытке автоматизации процесса на множестве контейнеров возникает проблема выбора метода анализа, поскольку *реализации различных методов могут давать противоречивые результаты,* что обусловлено, в первую очередь, неравенством вероятностей возникновения ошибок распознавания (рис. 1) для этих реализаций.

Кроме того, в условиях априорной неопределённости относительно типа стегосистемы значительную сложность представляет вопрос выбора исходных данных для анализа. Снижение объёма анализируемых данных потенциального контейнера ведёт к увеличению вероятности возникновения ошибки первого рода, увеличение – к ошибкам второго рода. Изменение правил выборки анализируемых данных влечёт общее возрастание ошибок распознавания.

Таким образом, в настоящее время для решения задачи стегоанализа и последующего извлечения скрытой информации необходима *методика*, позволяющая выделить на множестве результатов те из них, которые способствуют минимизации вероятности ошибки второго рода при заданном уровне вероятности ошибки первого рода.

Проведенный анализ существующих методов стегоанализа показал, что в зависимости от используемых исходных данных они делятся на три основных класса: сигнатурные, статистические и схемные.

Наиболее точными (вероятность возникновения ошибки первого или второго рода наиболее близка к нулю) являются сигнатурные методы. Суть этих методов заключается в синтаксическом анализе предъявленной на вход распознающего устройства последовательности терминальных символов, определяющих контейнер. В случае обнаружения принадлежности предъявленной на вход распознавателя цепочки терминальных символов языку, описывающему ту или иную стегосистему, принимается решение об ее использовании для организации канала связи. К достоинствам этих методов относится возможность получения результата, который однозначно характеризует примененную для сокрытия данных стегосистему. Основным же недостатком

является довольно небольшое (менее 10%) число стегопрограмм, оставляющих в контейнерах, используемых для сокрытия данных, свои сигнатуры.

Наименее точными являются статистические методы, базирующиеся на понятии “естественного” контейнера. Суть этих методов заключается в оценивании вероятности существования стегоканала с неизвестной стегосистемой на основе критерия оценки близости исследуемого контейнера к “естественному”. К достоинствам этой группы методов относится практически неограниченная область применения, что довольно существенно как при отработке гипотезы о наличии стегоканала с неизвестной стегосистемой, так и при разработке схемных методов стегоанализа. Основным недостатком методов этого класса является само предположение о существовании “естественного” контейнера. Так, например, файл с изображением, записанным в наиболее простом из графических форматов Windows BMP 24bit, может содержать произвольные данные, что вполне естественно, но далеко от любых известных моделей “естественного” контейнера.

Схемные методы используются для отработки гипотез о наличии стегоканала с априорно известной стегосистемой. В работе [7] приведено формализованное описание применения статистического метода Хи^2 для проверки гипотезы о наличии данных, скрытых стегопрограммами Jsteg, JPHide (Jpeg Hide&Seek) и OutGuess. При этом используются знания о распределении статистики по данным контейнеров, которые характерны именно для результатов работы указанных программ. Достоинством методов данного класса является относительно низкая вероятность возникновения ошибок (рис. 1), а также тот факт, что по положительному результату анализа аналитик *идентифицирует стегосистему,* не оставляющую «следов» (сигнатур) в контейнере, что позволяет предпринять попытку извлечения скрытой информации.

При исследовании были рассмотрены различные варианты заполнения контейнеров скрываемой информацией: от нескольких байт до максимально возможного заполнения (по данным, предоставляемым производителями исследованных стегопрограмм). В качестве скрываемых данных были использованы текстовые, исполняемые и архивные файлы. В результате проведенных экспериментальных исследований в разработанную методику были включены методы, последовательное применение которых позволяет принять решение о наличии в анализируемом контейнере стеганографического контента.

В общем случае эта последовательность методов выглядит следующим образом.

1. Сигнатурные методы [5].
2. Схемные методы [7,8].

Статистические методы:

3. Оценка по критерию частот переходов [10].
4. Оценка по критерию серий [10].
5. Оценка по критерию Хи^2 [6].
6. Сравнение “четырёхсвязных” блоков [9].
7. Оценка гистограммы изображения [9].
8. Построение гистограммы распределения элементов [11].
9. Построение распределения элементов на плоскости [11].
10. Проверка частот *k*-битных серий [11].
11. Проверка на монотонность [11].

При анализе контейнеров, представляющих собой графические файлы формата Windows BMP, в качестве элементов анализируемой последовательности следует выбирать все наименее значащие биты. Кроме того, при анализе не применяются пункты 6 и 7 методики.

При исследовании на предмет наличия стегоинформации контейнеров формата Baseline JPEG следует анализировать коэффициенты дискретного косинусного преоб-

разования и их наименее значащие биты. Третий пункт методики для анализа не применяется. Отличительной особенностью пунктов 6 и 7 методики является использование методов, работающих *в пространственной области* JPEG-контейнера: сравнение "четырёхсвязных" блоков и оценка гистограммы изображения.

При исследовании на наличие скрытой информации графических контейнеров в формате CompuServe GIF рекомендуется выполнять только первые два пункта методики стегоанализа. Анализу подвергаются палитры, используемые для кодирования изображений. Примененные сигнатурные и схемные методы позволили получить результаты, характеризующиеся низкими значениями вероятностей возникновения ошибок (менее 0,02). Авторы не имеют достаточной информации о широком применении статистических методов для автоматизированного анализа файлов данного формата.

Методы анализа, составившие разработанную методику, применяются к потенциальному контейнеру последовательно. Они ранжированы в порядке убывания степени доверия положительным результатам их применения (скрытая информация обнаружена), полученных опытным путём. При получении положительного отклика в результате работы очередного метода анализ следует остановить, а исследуемый контейнер считать носителем информации, скрытой с использованием стеганографических методов. В случае отсутствия положительного отклика после применения всех включенных в методику методов анализируемый контейнер следует считать пустым.

На рис. 1 приведены численные характеристики исследованных методов стегоанализа, возникающих при их применении к пустым контейнерам (фиксируются ошибки второго рода) и к стегоконтейнерам (фиксируются ошибки первого рода) при фиксированном объёме анализируемых данных (250 контейнеров). Под каждой диаграммой обозначены формат контейнера и стегосистема, используемая для сокрытия факта передачи информации.

Анализ представленных диаграмм исследований позволяют сделать следующие выводы.

1. Разработанная методика позволяет обнаружить стегоканал, использующий графические файлы форматов BMP, JPEG или GIF. При этом для компрометации канала связи достаточно однократного срабатывания первого или второго пунктов методики.

2. Компрометация канала связи в условиях многократных срабатываний статистических методов при условии несрабатывания сигнатурных и схемных методов носит условный характер. При использовании исключительно статистических методов необходимо длительное наблюдение за каналом связи и значительные усилия опытного аналитика. В целом, статистические методы следует рассматривать только как инструмент для исследования стегосистем.

3. Получение скрытого контента невозможно без компрометации канала связи. Помимо того, необходимо полное знание алгоритма функционирования компрометированной стегосистемы. Ввиду ресурсоёмкости извлечения информации критическим условием, необходимым для получения доступа к скрытой информации, является срабатывание первого или второго пункта методики.

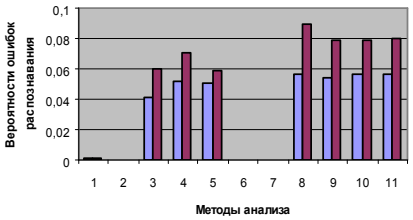
Для обеспечения анализа компьютерных файлов, передаваемых в электронных платежных системах, может быть рекомендован следующий комплекс мероприятий.

Обозначим S – множество стегопрограмм, пустых контейнеров C, сообщений M, заполненных контейнеров C', статистических методов стегоанализа G. Требуется:

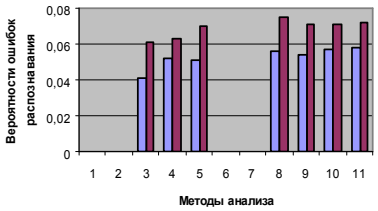
а) разработать сигнатурные и статистические методы стегоанализа $t_i \in T$ для каждой стегопрограммы из $s_i \in S$. Для этого:

– проанализировать исходные данные C, M, и результаты работы $C^{'}$ стего-программы $s_i \in S$ на множествах C и M статистическими методами из G;
– провести исследования исходных текстов или исполняемых модулей стегопрограмм из S на предмет выявления супермножества уязвимостей $\boldsymbol{D}=\{D_1, D_2, \ldots, D_n\}$, где D_i – множество уязвимостей стегопрограммы s_i;
– разработать методы стегоанализа T на основе выявленных уязвимостей $\boldsymbol{D}$;

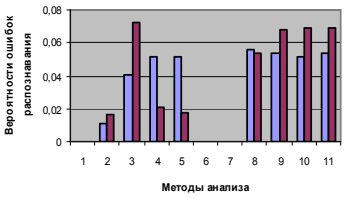
б) разработать устройство фильтрации потока контейнеров.



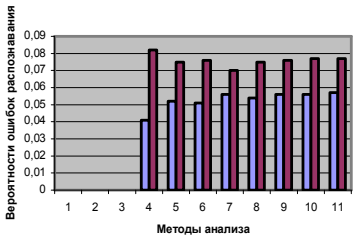
а) BMP, BlindSide 0.9b



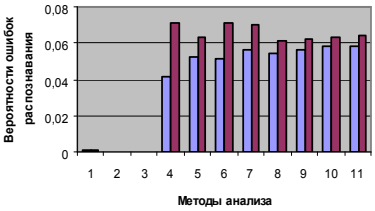
б) BMP, Image Hide



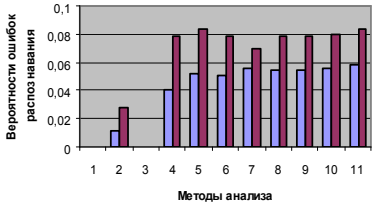
в) BMP, S-Tools 4.0



г) JPEG, Data Stash 1.0a



д) JPEG, Image Hide



е) JPEG, JPHide 0.5

– вероятности ошибок первого рода; – вероятности ошибок второго рода

Рис. 1. Вероятности ошибок распознавания

Суть работы устройства заключается в следующем.

На вход устройства подаётся контейнер (графические файлы в формате BMP, JPEG и GIF). Устройство состоит из набора программно-аппаратных фильтров, реализующих разработанные на шаге (а) методы стегоанализа *T*. После осуществления параллельной обработки поданного на выход устройства контейнера на выход устройства выдается один из двух возможных результатов работы: в случае наличия положительного отклика от одного из фильтров – идентификатор стегопрограммы Id_i, с помощью которой осуществлено скрытие информации в исходном контейнере; в случае наличия отрицательных откликов от всех фильтров – вывод об отсутствии стегоинформации в контейнере. Обобщенная функциональная схема такого устройства представлена на рис. 2.

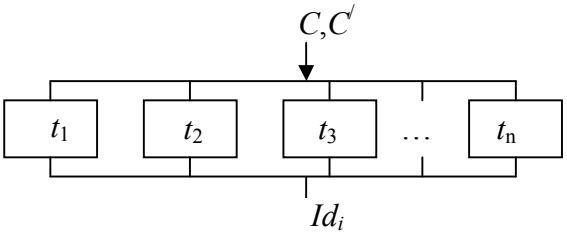


Рис.2. Обобщённая функциональная схема устройства для фильтрации потока контейнеров

в) выполнить анализ исходных текстов или исполняемых модулей стегопрограмм *S* с целью выделения алгоритмов извлечения скрытых данных $a_i \in A$;

г) использовать супермножество уязвимостей ***D*** и алгоритмы извлечения скрытых данных $a_i \in A$ для разработки методов и алгоритмов перебора паролей и проверки результатов для специализированных вычислительных комплексов.

Таким образом, предложенная методика позволяет выделять на множестве результатов те из них, которые способствуют минимизации вероятности ошибки второго рода при заданном уровне вероятности ошибки первого рода. Для реализации методики могут быть использованы как программные, так и аппаратные фильтры, предназначенные для идентификации отдельных стегоконтейнеров.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. http://www.stegoarchive.com
2. http://www.autex.spb.ru
3. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. М.: СОЛОН-Пресс, 2002.
4. *Грибунин В.Г.* Вейвлеты в стеганографии // http://www.autex.spb.ru
5. *Голубев Е.А., Летяго А.Г.* Компьютерная стеганография – новое явление в комплексной проблеме информационной безопасности. М., 2002.
6. *Bender W., Gruhl D.* Techniques for data hiding//IBM systems journal, v.35, n.3, 1996.
7. Provos N., Honeyman P. Detecting Steganographic Content on the Internet
8. *Гуськов В.Н., Демченко О.А.* Исследование возможностей и путей создания аппаратно-программных средств выявления стеганографической информации в глобальных компьютерных сетях. Курск, 2004.
9. *Ломако А.Г., Ткаченко С.Ф. и др.* Исследование возможностей и путей создания аппаратно-программных средств выявления стеганографической информации в глобальных компьютерных сетях. С.Пб, 2004.
10. Стеганография//http://www.viku.spb.ru.
11. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.