На правах рукописи

ВАЛИШИН Марат Фаритович

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ВСТРАИВАНИЮ СКРЫТОЙ ИНФОРМАЦИИ В ГРАФИЧЕСКИЕ ФАЙЛЫ

Специальность:
05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2015

Работа выполнена на кафедре телекоммуникационных технологий и сетей ФГБОУ ВПО «Ульяновский государственный университет»

Научный руководитель: доктор технических наук, профессор
Смагин Алексей Аркадьевич

Официальные оппоненты: доктор физико-математических наук, профессор
Леухин Анатолий Николаевич,
ФГБОУ ВПО «Марийский государственный университет», заведующий кафедрой информационной безопасности

кандидат технических наук, доцент
Аникин Игорь Вячеславович
ФГБОУ ВПО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», заведующий кафедрой систем информационной безопасности

Ведущая организация: ФНПЦ АО «Научно-производственное объединение «Марс», г. Ульяновск

Защита диссертации состоится «11» марта 2016 г. в 10^{00} часов на заседании диссертационного совета Д 212.288.07 на базе ФГБОУ ВПО «Уфимский государственный авиационный технический университет» по адресу: 450000, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВПО «Уфимский государственный авиационный технический университет» и на сайте *www.ugatu.su*.

Автореферат разослан «___» _____ 2016 года.

Ученый секретарь
диссертационного совета,
д.т.н., доцент И. Л. Виноградова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Стремительное развитие информационных систем и средств коммуникации становится вызовом для обеспечения информационной безопасности. Все большему числу пользователей становятся доступны программные средства для обеспечения скрытой передачи данных, которые позволяют преодолевать системы контроля трафика. Подобный скрытый канал связи между пользователями компьютерной сети может использоваться в противоправных целях.

Одним из способов организации скрытого канала связи является внедрение информационных сообщений в цифровые объекты, свободно распространяемые по сети. В качестве таких объектов выступают цифровые изображения, аудио- и видеофайлы и т.д. Объединение методов и средств, используемых для сокрытия информации, называется стеганографической системой (СГС).

Эффективность выявления факта передачи данных пропорциональна размеру скрываемого сообщения, а значит, исходное сообщение может быть передано небольшими частям в разных контейнерах, минуя существующие программные комплексы. В связи с этим следует рассмотреть возможность применения активных атак с целью разрушения встроенной скрытой информации путем модификации контейнера. Вносимые при модификации контейнера искажения, с одной стороны, должны быть достаточными для противодействия работе СГС, с другой стороны - незаметными для простых пользователей.

Таким образом, создание надежных систем противодействия встраиванию скрытой информации, объединяющих методы пассивного стегоанализа с алгоритмами целенаправленного разрушения скрытой информации методами цифровой обработки графических файлов, является актуальной задачей.

Степень разработанности темы исследования

Методам противодействия стеганографическим системам посвящены работы отечественных и зарубежных исследователей: Г. Симмонс (G. Simmons), К. Качин (C. Cachin), Дж. Фридрих (J. Fridrich), Х. Фарид (H. Farid), Г.Ф. Конахович, А.Ю. Пузыренко, Б.Я. Рябко, В.Г. Грибунин, М.Ю. Жилкин и многих других. Разработаны программные комплексы автоматического сканирования дискового пространства с целью выявления стеганограмм.

Предлагаемые в большинстве работ решения направлены на выявление факта передачи скрытой информации. Разработанные методы анализа позволяют надежно находить стеганограммы только при заполнении контейнера свыше некоторого порогового значения, что обеспечивает возможность передачи скрытой информации с помощью ограничения пропускной способности СГС.

Таким образом, актуальной является задача противодействия встраиванию скрытой информации небольшими частями в разные контейнеры.

Цель работы

Основной целью диссертации является повышение эффективности методов противодействия внедрению скрытой информации на основе создания алгоритмов и комплексов программных средств.

Задачи исследования

1. Разработка метода стегоанализа с применением активной атаки на контейнер.
2. Разработка критериев эффективности методов активного противодействия внедрению скрытой информации в графические файлы.
3. Разработка и реализация программного комплекса для получения количественных оценок методов активного противодействия скрытию информации.
4. Анализ границ применимости наиболее чувствительного метода пассивного стегоанализа графических файлов.
5. Анализ эффективности распространенных алгоритмов цифровой обработки графических файлов для противодействия скрытию информации методом имитационного моделирования.

Методы исследования

В процессе исследований были использованы основные положения и методы теории информации, теории вероятностей и математической статистики, теории дискретного кодирования, теории имитационного моделирования сложных систем, а также методы объектно-ориентированного программирования.

Основные положения, выносимые на защиту

1. Метод стегоанализа, основанный на объединении алгоритма выявления стеганограмм и активной атаки на контейнер, позволяющий обеспечить защиту от передачи скрытой информации при малом заполнении контейнера.
2. Критерии эффективности методов активного противодействия скрытию информации в графических файлах.
3. Программный комплекс для получения количественных оценок методов активного противодействия скрытию информации.
4. Результаты анализа границ применимости наиболее чувствительного метода пассивного стегоанализа графических файлов.
5. Результаты анализа эффективности алгоритмов цифровой обработки для противодействия скрытию информации в графических файлах.

Научная новизна

1. Разработан метод стегоанализа, отличающийся от традиционных пассивных методов стегоанализа тем, что позволяет надежно защитить от передачи скрытой информации при малом заполнении контейнера.
2. Разработаны критерии эффективности методов активного противодействия скрытию информации в графических файлах на основе количественных оценок снижения пропускной способности стегоканала при наличии помех и величины вносимого искажения в результате применения активной атаки на контейнер, что позволяет рассчитать верхнюю и нижнюю границы вносимого искажения для достоверного предотвращения скрытия информации.
3. Разработан и реализован программный комплекс для автоматизированного получения количественных оценок методов активного противодействия скрытию информации на основе проведения имитационного моделирования работы стеганографической системы, которая, в отличие от существующих СГС, позволяет скрывать информацию в одной из младших битовых плоскостях методами LSB-внедрения и ±1-стеганографии в краевой или однородной области.
4. Получена оценка границы применимости наиболее чувствительного метода пассивного стегоанализа графических файлов, что в отличие от известных результатов анализа эффективности данного метода, позволяет вычислить максимальный объём недетектируемой скрытой информации.
5. Проведен анализ эффективности алгоритмов цифровой обработки графических файлов для противодействия скрытию информации в графических файлах с помощью методов имитационного моделирования, что позволило получить количественные оценки в условиях скрытия информации с помощью СГС.

Научная и практическая значимость результатов

Научная ценность полученных результатов состоит в возможности повышения эффективности противодействия скрытию информации в графических файлах за счёт применения активной атаки на контейнеры с целью достоверного разрушения возможного стегоканала. Предложенные критерии эффективности методов активного противодействия скрытию информации позволяют оценить различные существующие и разрабатываемые алгоритмы цифровой обработки графических файлов и выбрать оптимальный алгоритм для решения прикладных задач.

Практическая значимость обусловлена тем, что разработан программный комплекс, который позволяет автоматизировать процесс получения численных оценок и, таким образом, ускорить и автоматизировать процесс анализа и подбора подходящих алгоритмов при решении прикладных задач. Предложенный метод

противодействия скрытию информации позволяет повысить безопасность компьютерных систем от утечки данных.

Степень достоверности результатов работы

Достоверность основных результатов и положений диссертационного исследования обеспечена корректностью применения математического аппарата, применением современных методов проведения численных экспериментов, согласованностью результатов теоретических расчетов с экспериментальными данными, полученных автором при компьютерном моделировании.

Публикации

По материалам диссертации опубликовано 9 печатных работ, в том числе 4 статьи в научных журналах и изданиях, которые включены в перечень российских рецензируемых научных журналов и изданий для опубликования основных научных результатов диссертаций на соискание ученых степеней доктора и кандидата наук.

Структура и объем диссертации

Диссертация содержит 106 страницы машинописного текста и состоит из введения, трех глав, заключения, списка использованных источников. В работе присутствует 36 рисунков и 10 таблиц. Список использованных источников включает 100 источников.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассматривается актуальность работы, определяются цель и задачи исследования, определяются объект и методы исследования. Определены научная новизна и практическая значимость результатов. Дается краткая характеристика содержания диссертации.

В первой главе рассматривается общая модель стеганографической системы, основные принципы её функционирования. Описываются наиболее распространенные алгоритмы скрытия информации в графических файлах, а также методы пассивного стегоанализа, позволяющие их детектировать.

Наиболее распространенными алгоритмами скрытия информации в графических файлах являются Jsteg, Outguess, F5, HUGO. Данные алгоритмы послужили толчком к развитию методов пассивного стегоанализа, таких как гистограммный анализ, метод машинного обучения и разностный стегоанализ на основе двойной статистики (RS-стегоанализ).

Разностный стегоанализ на основе двойной статистики предложен группой исследователей под руководством Дж. Фридрих и сокращенно назван RS-стегоанализ от Regular-Singular («регулярный-сингулярный»). Данный количественный метод стегоанализа основан на выявлении пространственной

корреляции в пустых контейнерах.

Следует отметить, что эффективность известных методов стегоанализа напрямую зависит от пропускной способности стеганографической системы. В настоящее время методы пассивного стегоанализа позволяют с приемлемой достоверностью детектировать скрытие информации в графических файлах при заполнении контейнера не менее 10% от его ёмкости. Таким образом, существует угроза тайной передачи секретного сообщения частями в нескольких контейнерах. Показано, что противодействовать скрытой передаче данных при малом заполнении контейнера следует с помощью методов активного стегоанализа, нацеленных на внесении модификаций в контейнер для достоверного разрушения стеганограммы.

Во второй главе рассматривается задача построения метода противодействия скрытию информации в графических файлах, который включает в себя методы пассивного и активного стегоанализа. Приводится модель эталонной стеганографической системы для исследования методов активного стегоанализа. Вводится количественная оценка степени разрушения стегоканала в результате применения активной атаки на контейнер. Дается верхняя и нижняя границы эффективности методов активного противодействия скрытию информации. Описываются алгоритмы автоматического анализа методов активного противодействия скрытой передачи данных с применением эталонной СГС. Предлагаются алгоритм локализации стеганограмм внутри контейнера, основанный на RS-анализе групп пикселей.

Анализ существующих алгоритмов пассивного стегоанализа показал, что в процессе принятия решения о присутствии стеганограммы в контейнере происходит численный расчет внутреннего параметра K и, в зависимости от его знака, контейнер маркируется как пустой или заполненный. Следует отметить, что точность обнаружения стеганограмм для большинства современных алгоритмов стегоанализа прямо пропорциональна абсолютной величине данного параметра K. Это означает, что существует некоторая δ-окрестность около нуля, для которой надежность обнаружения скрытой информации недостаточна.

В целях повышения эффективности существующих методов пассивного стегоанализа предложен принципиально новый метод противодействия скрытию информации, который включает в себя активную атаку на контейнеры, отнесенные к δ-окрестности.

Проведенный предварительный анализ показал, что существующие стегосистемы не позволяют в полной мере оценить влияние активных атак на стеганограмму. Поэтому предложена модель эталонной (тестовой) стеганографической системы, предназначенной для исследования различных алгоритмов модификации графических файлов, в которую заложены следующие принципы функционирования: принцип минимальной достаточности, принцип минимизации технической сложности и принцип воспроизводимости результата.

Параметрами функционирования эталонной СГС являются:

- размер стеганограммы;
- область сокрытия стеганограммы внутри контейнера;

- номер битовой плоскости, в которую происходит внедрение стеганограммы;
- метод внедрения отдельных бит стеганограммы.

Секретное сообщение генерируется на основе специального шаблона и подвергается симметричному шифрованию с помощью алгоритма AES.

В качестве контейнера принято использовать стандартное тестовое изображение «Lena» (рисунок 1, а). Сокрытие информации производится равномерно по всей цифровой фотографии или только в её краевую область (рисунок 1, б), в зависимости от входных параметров.

а б

Рисунок 1 - Стандартное тестовое изображение «Lena» (а)
и его краевая область (б)

В качестве алгоритма выделения краев предложено использовать оператор Собеля. Данный алгоритм основан на вычислении приближенного значения градиента яркости. Преимуществом оператора Собеля является простота вычислений, так как алгоритм основан на свертке изображения небольшими сепарабельными целочисленными фильтрами в вертикальном и горизонтальном направлениях.

Сокрытие данных может происходить в любую из битовых плоскостей, но, во избежание визуального обнаружения, принято решение использовать для внедрения стеганограмм только младшие битовые плоскости, 1-4 по схеме нумерации бит «LSB».

Для модели эталонной СГС приняты два метода сокрытия отдельного бита стеганограммы в фиксированную битовую плоскость:

1. метод замены бита в значении яркости пикселя;
2. метод модификации значения яркости пикселя.

Первый метод тривиален и статистически более заметен. Второй метод является обобщением метода ±1 на все битовые плоскости.

Таким образом, модель эталонной СГС позволяет формировать заполненные контейнеры в 16 режимах работы. Сокрытие информации может происходить в одной из 2-х областей исходного контейнера, в одной из 4-х битовых плоскостей, 2-мя различными способами внедрения.

Для обозначения режима работы эталонной СГС принята следующая маркировка: [**1-4**][**A**|**C**][**R**|**M**], где [**1-4**] – номер битовой плоскости, **A** – сокрытие происходит в краевой области, **C** – сокрытие происходит по всему контейнеру, **R** – применяется метод замены бит, **M** – применяется обобщенный метод ±1.

Одним из основных параметров алгоритма активной атаки на контейнер является оценка разрушения стеганограммы. Для того чтобы оценить, насколько уменьшится пропускная способность СГС при внесении искажений в контейнер, предложена модель бинарного канала передачи связи при наличии помех. В данной модели каждый из двоичных сигналов с вероятностью p может перейти в другой сигнал.

Получено, что скрытая в цифровом объекте информация будет полностью разрушена, если вероятность искажения сигнала будет равна 0,5. Это может быть достигнуто, если инвертировать бит на той позиции, в которую происходит внедрение секретного сообщения, у половины пикселей исходного изображения, выбранных случайным образом.

Для получения численной оценки вероятности искажения сигнала предлагается использовать коэффициент однобитовых ошибок (BER).

Вторым важным критерием эффективности применения активной атаки является оценка вносимого искажения. На основании проведенного исследования различных разностных и корреляционных оценок, было предложено использовать разностную оценку «пиковое соотношение сигнал/шум» (PSNR).

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_I^2}{MSE}\right), \tag{1}$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left|I(i,j) - K(i,j)\right|^2, \tag{2}$$

где $I(i,j)$, $K(i,j)$ – значение яркости пикселя на позиции (i,j) в исходном и искаженном изображениях; MAX_I – максимальное значение, принимаемое пикселем; m,n – высота и ширина изображения в пикселях. Когда пиксели имеют разрядность 8 бит, MAX_I равен 255.

Для оценки вносимого искажения были рассчитаны верхняя и нижняя границы. Максимальное значение PSNR при достоверном разрушении стеганограммы вычисляется по формуле:

$$PSNR_{\max} = 10 \times \log_{10}\left(\frac{255^2}{2^{2s-3} \times bpp}\right), \tag{3}$$

где ***bpp*** – пропускная способность стеганографической системы, равная отношению длины стеганограммы, выраженной в битах, к количеству пикселей изображения, ***s*** – номер битовой плоскости, которая содержит стеганограмму.

Минимальное значение PSNR при достоверном разрушении стеганограммы соответствует тривиальной атаке на контейнер, а именно инвертированию бит на той позиции, в которую происходит внедрение секретного сообщения, у половины пикселей исходного изображения, выбранных случайным образом.

$$PSNR_{\min} = 10 \times \log_{10}\left(\frac{255^2}{2^{2s-3}}\right), \tag{4}$$

где ***s*** – номер битовой плоскости, которая содержит стеганограмму.

Были разработаны алгоритмы автоматического анализа методов активного противодействия встраиванию скрытой информации с применением эталонной СГС.

Процедура исследования активной атаки заключается в проведении численных экспериментов над тестовой выборкой, полученной с помощью эталонной СГС. Рассматриваемый алгоритм модификации контейнера применяется в автоматическом режиме к сгенерированным заполненным контейнерам, а затем происходит расчет следующих численных показателей: оценка разрушения стеганограммы и оценка вносимого искажения. Тестовая выборка формируется в 16 режимах работы эталонной СГС во всем диапазоне пропускной способности: минимальная пропускная способность принята в размере 0,01 бит/пиксель, сокрытие в краевой области ограничено сверху 0,2 бит/пиксель.

Была рассмотрена задача локализации стеганограммы внутри контейнера с целью повышения эффективности методов активной атаки. Для формального описания процесса локализации секретного сообщения вводятся следующие обозначения. Пусть на множестве пикселей изображения определена вещественная функция локализации стеганограмм:

$$F_{x,y}(I) \in \Re . \tag{5}$$

Причем, чем больше значение функции локализации для пикселя с координатами *(x, y)*, тем больше вероятность того, что в данный пиксель был внедрен бит стеганограммы. Тогда с помощью функции локализации формируется ограниченная область сокрытия *E* следующим образом:

$$E = \left\{ (x, y) \middle| F_{x,y}(I) > \sigma \right\}, \tag{6}$$

где σ – некоторое пороговое значение.

Количество пикселей в ограниченной области с одной стороны не менее длины стеганограммы, равной *l* бит, а с другой – не более количества пикселей в исходном изображении, равного $M \times N$. Таким образом можно получить явное задание для мощности ограниченной области в следующем виде:

$$|E| = l + (1 - \mu_{эфф}) \times (M \times N - l), \tag{7}$$

где $\mu_{эфф}$ – эффективность локализации стеганограммы внутри контейнера с помощью выбранной функции локализации.

Разработан алгоритм автоматического анализа функции локализации с применением эталонной СГС с целью нахождения требуемого порогового значения. Алгоритм вычисления параметра σ состоит из следующих действий:

1. Получить заполненный контейнер.
2. Найти значение функции локализации для всех пикселей, в которые были сохранены биты стеганограммы.
3. Выбрать наименьшее среди найденных значений. Данное значение и будет параметром σ.

Следует отметить, что в зависимости от пропускной способности, выбранного контейнера и других факторов, может варьироваться параметр σ. Поэтому для

получения достоверного значения параметра σ необходимо провести серию расчетов по вышеизложенному алгоритму и найти усредненное значение σ.

В качестве функции локализации может применяться эвристический алгоритм. Было предложено использовать разностный стегоанализ на основе двойной статистики для построения функции локализации стеганограммы. Алгоритм расчета состоит из следующей последовательности действий:

1. Из множества пикселей исходного контейнера формируется подмножество для проведения RS-анализа.
2. На выбранном подмножестве пикселей происходит расчет оценки длины секретного сообщения с помощью метода пассивного стегоанализа RS.
3. Полученная оценка приписывается ко всем пикселям выбранного подмножества.
4. Пункты 1-3 повторяются n-раз для получения оценки для всех пикселей.
5. Значение функции локализации для выбранного пикселя рассчитывается как среднее значение приписанных к нему оценок.

Подмножество пикселей из исходного контейнера формируется методом скользящего окна или методом случайной выборки.

Третья глава посвящена подробному описанию программной реализации модели тестовой стеганографической системы. Приводятся результаты расчетного исследования чувствительности RS-стегоанализа, дается обоснование выбора порогового значения для классификации контейнеров на пустые и заполненные. Для разностного стегоанализа на основе двойной статистики представлена оценка недетектируемой пропускной способности LSB-стеганографии. В главе также показаны результаты исследования применения наиболее распространенных алгоритмов цифровой обработки графических файлов в качестве методов активного стегоанализа.

Для проведения тестирования алгоритмов активного противодействия встраиванию скрытой информации, методов локализации стеганограмм внутри контейнера и расчета области применения методов активных атак для пассивного стегоанализа была реализована модель эталонной СГС в виде программного комплекса “Эталонная СГС” на высокоуровневом языке программирования Python 2.7.

В программном комплексе “Эталонная СГС” предусмотрена возможность в автоматическом режиме построения тестовой выборки заполненных контейнеров для различных режимов и объемов сокрытия информации.

Для проведения тестирования алгоритмов активных атак разработаны подпрограммы BER и PSNR. Первая служит для расчета коэффициента однобитовых ошибок для переданного графического файла, вторая – для оценки вносимого искажения.

Известно, что RS-стегоанализ является одним из наиболее чувствительных методов к LSB-стеганографии. Выходным значением RS-анализа является предполагаемая длина сообщения в исследуемом изображении, которое может быть сравнено с некоторым пороговым значением для классификации контейнера.

Для того чтобы рассчитать максимальный размер секретного сообщения, который не обнаруживается RS стегоанализом, проведен следующий численный эксперимент по получению количественной оценки объема сокрытой информации методом RS-стегоанализа на множестве пустых контейнеров.

Для разностного стегоанализа на основе двойной статистики задавались следующие параметры:

- количество пикселей в группе принято равным 4;
- изображение разбивается на группы пикселей слева направо, сверху вниз;
- маска M принята равной (0, 1, 1, 0).

В качестве источника цифровых изображений, свободных от присутствия стеганограмм, выбрана коллекция изображений BOSSBase, которая состоит из 10000 цифровых фотографий в градациях серого, разрешением 512x512 пикселей. Для каждой фотографии из коллекции BOSSBase рассчитана оценка длины внедренного сообщения методом RS-стегоанализа. На рисунке 2 показана гистограмма распределения полученных оценок.

Следует отметить, что расчётное значение объёма сокрытой информации, получаемое с помощью метода RS-стегоанализа, совпадает с истинным значением только при LSB-внедрении значительного количества информации. В том случае, если пропускная способность стеганографической системы ограничивается небольшой величиной, расчётная оценка RS-стегоанализа может отклоняться от истинного значения. Более того, алгоритм расчёта в принципе может выдавать для анализируемого контейнера отрицательное значение.

Все расчётные оценки, полученные для пустых контейнеров, лежат в диапазоне от минус 37% до 87%. Наиболее вероятное значение, получаемое RS-стегоанализом свободных от LSB-внедрения изображений, составляет 1,2% при среднеквадратичном отклонении, равном 3,7%.

Рисунок 2 - Гистограмма распределения расчётной оценки объёма сокрытой информации, полученной с помощью RS-стегоанализа пустых контейнеров

На основании исследования результатов RS-стегоанализа получено, что для 99% цифровых изображений из коллекции BOSSBase оценка длины секретного сообщения составляет менее 15%. Таким образом, чтобы вероятность ложноположительного обнаружения LSB-внедрения методом RS-стегоанализа составляла не более 1%, необходимо при классификации цифровых изображений на пустые и заполненные контейнеры в качестве порогового значения принимать 15%.

Согласно результатам проведенного расчетного исследования, злоумышленник может организовать недетектируемый RS-стегоанализом скрытый канал передачи данных, если введет ограничение сверху на объем внедренной в один контейнер информации таким образом, чтобы оценка длины разностным стегоанализом на основе двойной статистики была меньше установленного порогового значения.

Для того чтобы получить количественную оценку пропускной способности описанной выше стеганографической системы, была рассчитана зависимость между объемом LSB-внедрения и значением, рассчитанным методом RS-стегоанализа.

Для некоторых цифровых изображений из коллекции BOSSBase моделированием стеганографической системы, основанной на LSB-внедрении, получена зависимость между длиной секретного сообщения и её расчётной оценкой RS-стегоанализом (рисунок 3). Расчетным путем получено, что оценка длины стеганограммы линейно растет с увеличением объема LSB внедрения, причем для цифровых изображений, оценка которых без стеганограммы соответствует наиболее вероятному значению 1,2% (изображения №№ 3115, 4354, 8824), коэффициент линейной зависимости практически равен единице. Для фотографии из коллекции BOSSBase с наименьшей исходной оценкой длины секретного сообщения коэффициент равен 1,45 (изображение №6956).

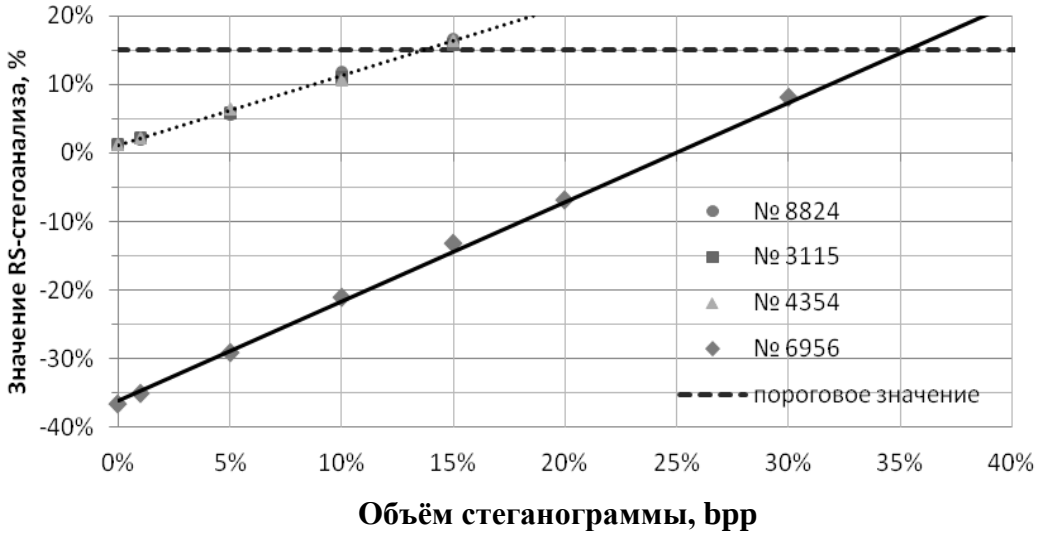

Рисунок 3 - Зависимость между объёмом стеганограммы и её расчётной оценкой RS-стегоанализом

Расчетным путем получено, что использование в качестве контейнера цифровых изображений, с исходной оценкой 1,2% и разрешением 512x512

пикселей, позволяет внедрить до 4,5 Кб секретной информации методом LSB без обнаружения RS-стегоанализом при уровне значимости 1%.

В качестве методов активного стегоанализа рассматривались распространенные алгоритмы цифровой обработки изображений. Несмотря на то, что эти алгоритмы не были разработаны специально для противодействия сокрытию информации в графических файлах, тем не менее, могут быть эффективно использованы. Достоинствами программных комплексов цифровой обработки изображений являются:

- распространенность;
- высокая производительность;
- автоматизация выполнения повторяющихся действий.

Наиболее известным программным пакетом для автоматической обработки графических файлов является ImageMagick. Данное программное средство включает в себя множество утилит для работы с изображениями. Входящая в состав ImageMagick утилита mogrify позволяет осуществлять коррекцию изображения и применение различные фильтры к графическим файлам или их последовательностям.

На основе проведенного анализа алгоритмов из программного пакета ImageMagick, были отобраны следующие фильтры для применения в качестве активной атаки на контейнер:

- подавление мультипликативного шума (despeckle);
- размытие по Гауссу (gaussian-blur);
- автоматическая гамма-коррекция (auto-gamma);
- повышение контраста (contrast);
- увеличение резкости (sharpen);
- удаление шума (noise).

Следует отметить, что вносимое в результате применения фильтра искажение превосходит нижнюю границу эффективности методов активного противодействия для младших битовых плоскостей. Для того чтобы повысить эффективность применения алгоритмов программного комплекса ImageMagick предложено объединить результирующее и исходное изображения по следующему правилу:

$$I^{s}_{filter}(x,y) = \left(I_{filter}(x,y) \oplus I(x,y)\right) \wedge 2^{s-1} \oplus I(x,y), \tag{8}$$

где I^{s}_{filter} - выходное изображение, I_{filter}, I - результирующее и исходное изображения, $\boldsymbol{s}$ – номер битовой плоскости, в которой происходит сокрытие стеганограммы.

В этом случае, в исходном изображении изменению подвергаются только та битовая плоскость, которая используется для организации встраивания стеганограмм. Предложенная схема позволяет существенно уменьшить вносимое искажение (таблица 1).

Таблица 1 - Оценка вносимого искажения, дБ

Алгоритм цифровой обработки изображений	Номер битовой плоскости			
	1	2	3	4
Подавление мультипликативного шума (Despeckle)	51,5	45,6	40,0	35,6
Размытие по Гауссу (Gaussian blur)	51,1	45,2	39,8	35,3
Автоматическая гамма-коррекция (Auto-gamma)	50,1	45,7	37,2	34,2
Повышение контраста (Contrast)	50,3	45,7	38,4	32,7
Увеличение резкости (Sharpen)	51,1	45,2	40,1	35,7
Удаление шума (Noise)	52,2	46,2	40,7	36,3

Было проведено расчетное исследование активной атаки с помощью эталонной стеганографической системы согласно описанному выше алгоритму.

Полученные численные значения коэффициента однобитовых ошибок для всех исследуемых алгоритмов цифровой обработки изображений практически не зависят от длины секретного сообщения.

В таблице 2 представлены результаты численного эксперимента по расчету коэффициента однобитовых ошибок для различных режимов функционирования эталонной стеганографической системы.

Таблица 2 - Результат расчета коэффициента однобитовых ошибок с применением программного комплекса «Эталонная СГС»

Маркировка режима работы СГС	Despeckle	Gaussian blur	Auto-gamma	Contrast	Sharpen	Noise
1AR	0,36	0,50	0,52	0,60	0,50	0,29
1AM	0,36	0,50	0,52	0,60	0,50	0,29
1CR	0,46	0,50	0,63	0,60	0,50	0,40
1CM	0,46	0,50	0,63	0,60	0,50	0,40
2AR	0,35	0,50	0,34	0,45	0,50	0,30
2AM	0,34	0,50	0,35	0,45	0,50	0,30
2CR	0,45	0,50	0,43	0,44	0,49	0,40
2CM	0,45	0,50	0,43	0,44	0,49	0,40
3AR	0,39	0,50	0,82	0,62	0,50	0,31
3AM	0,39	0,49	0,82	0,62	0,50	0,31
3CR	0,46	0,50	0,76	0,59	0,48	0,41
3CM	0,46	0,48	0,77	0,59	0,48	0,41
4AR	0,35	0,50	0,41	0,52	0,49	0,35
4AM	0,35	0,49	0,41	0,52	0,49	0,35

Маркировка режима работы СГС	Despeckle	Gaussian blur	Auto-gamma	Contrast	Sharpen	Noise
4CR	0,45	0,48	0,38	0,54	0,45	0,43
4CM	0,45	0,48	0,38	0,54	0,45	0,43

На основании полученных численных значений рассчитывалась пропускная способность стеганографической системы в случае применения активного противодействия встраиванию скрытой информации в графических файлах (таблица 3).

Таблица 3 - Пропускная способность эталонной СГС при атаке на контейнер, в % от номинальной

Маркировка режима работы СГС	Despeckle	Gaussian blur	Auto-gamma	Contrast	Sharpen	Noise
1AR	5,73	0,00	0,12	2,90	0,00	13,13
1AM	5,73	0,00	0,12	2,90	0,00	13,13
1CR	0,46	0,00	4,93	2,90	0,00	2,90
1CM	0,46	0,00	4,93	2,90	0,00	2,90
2AR	6,59	0,00	7,52	0,72	0,00	11,87
2AM	7,52	0,00	6,59	0,72	0,00	11,87
2CR	0,72	0,00	1,42	1,04	0,03	2,90
2CM	0,72	0,00	1,42	1,04	0,03	2,90
3AR	3,52	0,00	31,99	4,20	0,00	10,68
3AM	3,52	0,03	31,99	4,20	0,00	10,68
3CR	0,46	0,00	20,50	2,35	0,12	2,35
3CM	0,46	0,12	22,20	2,35	0,12	2,35
4AR	6,59	0,00	2,35	0,12	0,03	6,59
4AM	6,59	0,03	2,35	0,12	0,03	6,59
4CR	0,72	0,12	4,20	0,46	0,72	1,42
4CM	0,72	0,12	4,20	0,46	0,72	1,42

Здесь в первой колонке идут маркировки различных режимов функционирования тестовой стеганографической системы, а по строкам – результаты автоматизированного анализа эффективности применения алгоритмов цифровой обработки графических файлов.

Таким образом, наилучшие результаты показал алгоритм цифровой обработки изображений «фильтр Гаусса» (Gaussian blur). В тоже время, остальные алгоритмы также могут применяться при решении прикладных задач. Следует отметить, что представленные алгоритмы являются адаптивными и результат их применения зависит от исходного изображения. Это означает, что можно разработать устойчивый к данному влиянию стеганографический алгоритм. В отличие от адаптивных методов, инвертирование бит на той позиции, в которую

происходит внедрение секретного сообщения, у половины пикселей исходного изображения позволяет предотвратить встраивание скрытой информации для любой СГС.

В заключении сформулированы основные результаты, полученные в диссертационной работе.

Перспективы дальнейшей разработки темы

В рамках дальнейших исследований планируется снижение вносимого искажения методами активного противодействия внедрению скрытой информации за счёт локализации стеганограмм, а также исследование подходящих функций локализации стеганограмм.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Разработан принципиально новый метод противодействия встраиванию скрытой информации в графических файлах, основанный на объединении методов пассивного и активного стегоанализа, применение которого позволяет повысить эффективность противодействия сокрытию информации в графических файлах.
2. Разработаны количественные критерии эффективности разрушения скрытого канала связи для методов активного стегоанализа, основанные на оценке снижения пропускной способности стеганографической системы от вероятности внесения искажения в результате активной атаки на контейнер и оценке вносимого искажения по метрике «пиковое соотношение сигнал/шум».
3. Разработан и реализован программный комплекс для получения количественных оценок методов активного противодействия встраиванию скрытой информации, в рамках которого предложена модель тестовой стеганографической системы.
4. Разработан алгоритм исследования чувствительности метода пассивного стегоанализа с целью нахождения границ его применимости и экспериментально получены численные оценки чувствительности RS-стегоанализа к LSB-стеганографии.
5. Получены количественные оценки эффективности применения алгоритмов цифровой обработки графических файлов из программной библиотеки ImageMagick в качестве методов активного противодействия встраиванию скрытой информации, предложен алгоритм минимизации вносимого искажения и даны рекомендации к выбору метода активной атаки на контейнер.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Журналы из перечня ВАК

1. Валишин М.Ф. Устойчивые к атакам на контейнер стеганографические алгоритмы / Валишин М.Ф., Смагин А. А. // Инфокоммуникационные технологии. – 2015. – № 1. – С. 82-87.
2. Валишин М.Ф. Оценка применения алгоритмов цифровой обработки изображений для противодействия скрытой передачи данных / М.Ф. Валишин // Перспективы науки. – Тамбов: Изд-во «ТМБпринт», 2015. – №4(67). – С. 115-120.
3. Валишин М.Ф. Повышение надежности сокрытия данных в цифровых фотографиях методом LSB с помощью оператора Собеля / М.Ф. Валишин // Глобальный научный потенциал.– 2015. – № 4(49). – С. 72-76.
4. Валишин М.Ф. Оценка недетектируемой RS-стегоанализом пропускной способности LSB-стеганографии / М.Ф. Валишин // М.: Наука и бизнес: пути развития. – № 6(48). – 2015. – С. 41-47.

Другие издания

5. Валишин М.Ф. Применение фильтра Гаусса в качестве метода активного противодействия скрытой передачи данных в графических файлах / М.Ф. Валишин // Инновации и инвестиции.–2014. –№11. – С. 216-217.
6. Смагин А.А. Модели разбиений: моногр. – Ульяновск: УлГУ, 2013. – 217с.
7. Валишин М.Ф. История стеганографии / М.Ф. Валишин // Ученые записки Ульяновского государственного университета. Сер. Математика и информационные технологии. – Ульяновск, 2012.
8. Валишин М.Ф. Метод построения относительно надежных стеганографических систем / М.Ф. Валишин // Ученые записки Ульяновского государственного университета. Сер. Математика и информационные технологии. – Ульяновск, 2012. – Вып. 1(4). – С. 135-145.
9. Смагин А.А., Петрищев И.О. Построение моделей угроз и расчетных показателей эффективности комплексной безопасности при анализе уязвимости складов нефтепродуктов. // АПУ. Ульяновск. ФНПЦ ОАО. «НПО МАРС», 2010, №3 (21), с.28-34.

Диссертант  Валишин М.Ф.

ВАЛИШИН Марат Фаритович

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ ВСТРАИВАНИЮ СКРЫТОЙ ИНФОРМАЦИИ В ГРАФИЧЕСКИЕ ФАЙЛЫ

Специальность:
05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук