**Рублев Дмитрий Павлович. Разработка и исследование высокочувствительных методов стегоанализа : диссертация ... кандидата технических наук : 05.13.19 / Рублев Дмитрий Павлович; [Место защиты: Юж. федер. ун-т]. - Таганрог, 2007. - 142 с. : ил. РГБ ОД, 61:07-5/5409**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ТАГАНРОГСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ ЮЖНОГО
ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА

**61** **07**-**5/5409**

На правах рукописи



Рублёв Дмитрий Павлович

**РАЗРАБОТКА И ИССЛЕДОВАНИЕ ВЫСОКОЧУВСТВИТЕЛЬНЫХ**

**МЕТОДОВ СТЕГОАНАЛИЗА**

Специальность 05 Л З Л 9 - Методы и системы защиты информации,
информационная безопасность

Диссертация на соискание учёной степени
кандидата технических наук

Научный руководитель

доктор технических наук, профессор Макаревич О. Б.

Таганрог 2007

Содержание

**ВВЕДЕНИЕ 3**

1. **Исследование и анализ существующих методов стеганографии 11**
	1. **Терминология современной стеганографии 12**
	2. **Модели стеганографических систем 14**
	3. **Методы стеганографии 23**
		1. **Методы замены наименее значимых бит (НЗБ) 23**
		2. **Методы расширения спектра 27**
	4. **Классификация методов стеганографии 28**
	5. **Методы стегоанализа 30**
		1. **Стегоанализ на основе классификации статистик 31**
		2. **Стегоанализ на основе классификации распределений 35**
		3. **Стегоанализ на основе статистик бинарного представления 35**
		4. **Разностный стегоанализ на основе палитры 38**
		5. **Разностный стегоанализ на основе двойной статистики (RS-стегоанализ) 40**
		6. **Стегоанализ модифицированного НЗБ-метода встраивания 42**
		7. **Стегоанализ на основе восстановленной гистограммы 43**
		8. **Стегоанализ как задача оценки артефактов компрессии 44**
	6. **Недостатки методов специализированного стегоанализа 46**
	7. **Выводы 47**
2. **Разработка модели стегокоптейнера па основе кратномасштабного представления 49**
	1. **Структура системы универсального стегоанализа 49**
	2. **Необходимые свойства псевдометрик контейнера в задачах стегоанализа 53**
	3. **Выбор преобразования для построения псевдометрик контейнера 59**
	4. **Формирование векторов признаков на основе вейвлет-преобразования 68**
	5. **Выбор базисного вейвлета при формировании вектора признаков 78**
	6. **Выбор дерева вейвлет-декомпозиции при формировании вектора признаков 81**
	7. **Обработка признаков в методах универсального стегоанализа 85**
		1. **Понижение размерности векторов признаков 86**
		2. **Методы классификации векторов признаков 87**
		3. **Классификатор на основе линейной регрессии 89**
		4. **Классификатор на основе нейросетей радиальных базисных функций (RBF) 90**
		5. **Классификатор на основе нейросетей прямого распространения 94**
	8. **Выводы 94**
3. **Разработка методов универсального стегоанализа 96**
	1. **Обобщённая структура универсального стеганографического метода 96**
	2. **Выбор унифицированного формата контейнеров стегосистемы 99**
	3. **Метод порогового стегоанализа контейнеров-изображений 102**
	4. **Метод количественного стегоанализа контейнеров-изображений 111**
	5. **Метод порогового стегоанализа контейнеров-аудиосигналов 113**
	6. **Выводы 115**
4. **Разработка и экспериментальное исследование системы обнаружения встроенных**

**сообщений на основе разработанных методов стегоанализа 116**

* 1. **Разработка программной модели универсального метода стегоанализа 116**
	2. **Экспериментальные исследования универсальных стеганографических методов 119**
		1. **Метод порогового стегоанализа контейнеров аудиосигналов 119**
		2. **Метод порогового стегоанализа контейнеров изображений 122**
		3. **Метод количественного стегоанализа изображений 127**
	3. **Выводы 128**

**ЗАКЛЮЧЕНИЕ 129**

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 131**

**Актуальность.**

С развитием информационных технологий и переводом основных потоков информации, в цифровую форму приобрела актуальность проблема обеспечения информационной безопасности. При этом единственным выходом для сохранения конфиденциальности и целостности информации является создание комплексной системы защиты информации. Важную роль в обеспечении информационной безопасности играет подсистема управления доступом. Однако стандартные методы и средства контроля информации на настоящий момент ориентированы на проверку лишь ограниченного числа явных атрибутов и современные средства сокрытия информации — цифровой стеганографии позволяют преодолевать существующие системы контроля доступа к сетевым ресурсам. Скрытые каналы передачи информации позволяют преодолеть ограничения стандартных средств контроля трафика. Информация может быть скрыта в любом формате данных, который разрешён к передаче данным пользователем во внешнюю сеть, в том числе в определённых полях сетевых пакетов, запрашиваемых ссылках и иных объектах. В качестве носителя скрытой информации в цифровой стеганографии могут быть использованы оцифрованные аналоговые сигналы, тексты документов, исполнимый код, пакеты сетевого трафика и т.д. с сохранением семантики. Таким образом, принципиально возможна организация скрытых каналов утечки при наличии любой избыточности в исходящем трафике. Применение стеганографических средств для сокрытия информации в файлах, передаваемых затем на сайты мультимедиа-контента и файлообменные серверы позволяет скрытно организовывать и координировать проведение различного рода противоправных действий. При получении доступа организованными преступными группировками к передающим средствам сотовой и

стационарной телефонной связи, спутниковым каналам связи, телевидения и радиовещания возможна организация скрытых каналов передачи информации глобальных масштабов. В этих условиях особенно актуальной становится задача обнаружения скрытой информации, её извлечения и уничтожения, а также анализ стойкости существующих стеганографических алгоритмов, и разработка новых методов выявления скрытой информации — стегоанализ.

В зависимости от поставленных при разработке стегоаналитической системы задач и имеющихся ресурсов могут быть использованы методы как пассивного (анализ на наличие скрытой информации), так и активного (изменение потенциальных контейнеров с целью модификации либо уничтожения скрытой информации) стегоанализа. Применение методов активного стегоанализа в большинстве случаев нежелательно, вследствие тривиальности выявления их использования и возможности разработки мер адаптивного противодействия.

Большинство широко известных на настоящий момент пассивных методов стегоанализа можно разделить на два класса — методы статистического стегоанализа и методы так называемого универсального или “слепого” стегоанализа. Методы статистического стегоанализа ориентированы на работу в области цифрового представления данных и, при условии принадлежности анализируемых контейнеров к классу, для которого была построена модель, являются априорно надёжными. Главным преимуществом стегоаналитического подхода на основе анализа статистик является низкая требовательность к вычислительным ресурсам и простота предварительного обучения, сводящегося обычно к определению пороговой величины на репрезентативной выборке контейнеров. Однако практическое применение методов ограничивается средней и низкой чувствительностью (для порога обнаружения типичны значения 30-50% от максимальной степени заполнения контейнера). Существенными недостатками методов данной группы являются зависимость от формата представления контейнера, что при отсутствии спецификации формата делает их применение малоэффективным, так как искажения, возникшие вследствие встраивания информации с сжатые форматы, расположены на макроуровне и распределены по частотным диапазонам, в то время как пространственно­временная область является их суперпозицией и не обнаруживает значимых отклонений. К числу существенных недостатков методов относится также малая стойкость к атакам противодействия вследствие существования аналитического описания. В частности, возможна разработка метода стеганографии, ориентированного на эффективное преодоление конкретного метода либо группы методов стегоанализа.

Для преодоления вышеперечисленных недостатков специализированных методов в настоящее время ведутся интенсивные разработки в области универсальных методов стегоанализа, основанных на многокритериальном анализе метрик. Основу методов универсального стегоанализа составляет нахождение для анализируемого контейнера значений набора метрик разной контекстной зависимости, формирование многомерного вектор признаков и последующая его классификация. Различают две группы методов универсального стегоанализа: пороговый и количественный. При проведении порогового стегоанализа классификатором определяется принадлежность вектора признаков к одному из классов контейнеров соответственно наличию скрытой информации в то время как результатом количественного стегоанализа является оценка объёма скрытой информации. Главным преимуществом универсальных методов стегоанализа является возможность простой адаптации, основанной на переобучении классификатора на новые алгоритмы встраивания и форматы контейнеров без необходимости разработки их явных моделей. При этом особенностью методов универсального стегоанализа является их адаптируемость к методам Для охвата максимального количества признаков в число метрик могут быть включены как инструментальные метрики, так и метрики, построенные с учётом психофизиологических особенностей восприятия человека. Анализ изменений метрик производится в частотных субполосах на основе преобразований пространственно-временного представления контейнера в ортогональный базис, как правило, косинусного или вейвлет­преобразований, преобразования Фурье.

Подходы, используемые при анализе вектора признаков, могут успешно использоваться и для создания специализированных адаптируемых методов статистического анализа срезов. Однако у методов универсального стегоанализа имеются и недостатки. Перед применением метода универсального стегоанализа необходимо предварительное обучение на представительной выборке контейнеров. Существенной проблемой при обработке многомерных векторов является их высокая размерность. Линейная классификация, применяющаяся во многих методах, в силу исходной нелинейности проблемы зачастую не в состоянии обеспечить приемлемых уровней ошибок на множестве возможных контейнеров, что нивелирует одно из главных преимуществ универсального стегоанализа.

Традиционные подходы в задачах универсального стегоанализа не обеспечивают приемлемого уровня чувствительности и для успешного решения данных проблем очевидна необходимость в исследовании новых подходов, их всестороннем анализе и установлении границ оптимальности применения. При этом основные задачи универсального стегоанализа — идентификация и кластеризация являются традиционными задачами, при решении которых успешно применяются искусственные нейронные сети (ИНС). ИНС также могут использоваться и для снижения избыточности и сокращения размерности векторов признаков. От традиционных методов анализа нейросетевой подход отличает принципиальная возможность нелинейной классификации. На основе искусственных нейронных сетей реализуются также процедуры сжатия и классификации данных с итеративным обновлением, что особенно важно при использовании стегоаналитических методов в составе систем, работающих в реальном масштабе времени. Эффективное создание мер противодействия

нейросетевому представлению классов возможно лишь при всестороннем изучении используемых метрик, и анализе весов обученной нейросети, что является вычислительно сложной задачей.Проведённый анализ публикаций открытой печати показал, что нейросетевой подход к задачам стегоанализа практически не исследован. Исходя из этого, особенно актуальными на настоящий момент являются задачи исследования возможностей открывающихся при применении нейросетевого подхода в разработке новых методов стегоанализа, оценке стойкости методов стеганографии, разработанных на основе традиционных подходов, к новым методам стегоанализа, разработке специализированных и универсальных методов стегоанализа с использованием искусственных нейронных сетей,

позволяющих установить факт наличия встроенной информации, оценить её объём, и при возможности осуществить извлечение.

Целью работы является разработка и исследование высокочувствительных методов обнаружения стеганографических

сообщений в контейнерах-изображениях и звуковых файлах, определение оптимальных процедур формирования векторов признаков, их постобработки и классификации для минимизации ошибок первого и второго рода.

Исходя из поставленной цели, определяется перечень задач исследования:

1. Исследование и анализ методов стеганографического встраивания и обнаружения встроенных сообщений, разработка структуры системы стегоанализа на основе векторов признаков.
2. Разработка модели стегоконтейнера с целью выделения векторов признаков, а также методов обработки векторов для решения задач порогового и количественного стегоанализа.
3. Разработка методов высокочувствительного порогового и количественного стегоанализа на основе вейвлет-преобразования и нейросетевой классификации.
4. Проведение экспериментальных исследований разработанных методов, сравнение с аналогами.

Методы исследования данной работы основаны на использовании теории вероятности и математической статистики, теории

кратномасштабного анализа, аппарате искусственных нейронных сетей.

Научная новизна диссертационной работы заключается в следующем

1. Разработан метод формирования признаков области

кратномасштабного представления сигналов, позволяющие проводить анализ стегоконтейнеров вне зависимости от исходного формата

представления на множестве масштабов.

1. Разработаны высокочувствительные методы порогового стегоанализа области битового представления контейнера, позволяющие при малой длине встроенного сообщения достичь высокой точности стегоанализа.
2. Разработан высокочувствительный метод количественного стегоанализа области восстановленного стегоконтейнера, позволяющий производить стегоанализ в отсутствие доступа к описанию формата компрессии.

Практическая ценность работы

Разработанные методы могут быть использованы при создании многоуровневых автоматизированных систем универсального стегоанализа, проверке анализируемых метрик на значимость в задачах стегоанализа. Методы стегоанализа области битового представления позволяют создавать адаптируемые системы обнаружения сообщений, скрытых методами изменения НЗБ. Метод универсального стегоанализа области восстановленного стегоконтейнера предназначен для анализа закрытых форматов контейнеров при условии доступности декодера формата.

Достоверность

Достоверность полученных результатов подтверждается полнотой и корректностью теоретических обоснований, а также результатами

проведённых экспериментов действующих моделей.

**Основные положения, выносимые на защиту**

1. Высокочувствительные методы порогового и количественного стегоанализа области битового представления контейнера, позволяющие обнаружить встроенные сообщения при объёмах порядка *1,5-2%* от максимальной ёмкости.
2. Высокочувствительные методы порогового и количественного стегоанализа области восстановленного стегоконтейнера, которые позволяют обнаруживать стеганографические сообщения при объёмах заполнения 2-5% в полноцветных изображениях и до 0,2% от максимального, в контейнерах, полученных из формата JPEG.
3. Экспериментальные оценки основных характеристик разработанных методов универсального стегоанализа на основе нейросетевого подхода.

**Использование результатов**

Результаты, полученные в ходе работы над диссертацией, были использованы при проведении хоздоговорной работы шифр “КАРТИНА”, исследованиях по гранту РФФИ 05-07-90372-в “Исследование и разработка высокоточных методов и средств стегоанализа”.

**Апробация**

Полученные при работе над темой диссертации результаты были представлены на:

1. VI Всероссийской научной конференции студентов и аспирантов “техническая кибернетика, радиоэлектроника и системы управления”, Таганрог, 2002.
2. VII Всероссийской научно-технической конференции «Повышение эффективности средств обработки информации на базе математического и машинного моделирования», Тамбов, 2004.
3. VII Всероссийской научной конференции студентов и аспирантов «Техническая кибернетика, радиоэлектроника и системы управления», Таганрог, 2004
4. VI Международной научно-практической конференции

«Информационная безопасность», Таганрог, 2004.

1. VII Международной научно-практической конференции

"Информационная безопасность"-2005.

1. III Международной конференции «Информационные системы и технологии» (IST’2006), Минск, 2006г.

**Публикации**

По теме диссертации опубликовано 16 статей и тезисов докладов, из них 2 статьи опубликованы: в журнале «Известия Таганрогского государственного радиотехнического университета (ТРТУ)» за 2003 год и Трудах Седьмого Международного симпозиума “Интеллектуальные системы” за 2006 год из перечня, рекомендованного ВАК РФ для публикации результатов диссертационных работ.

**Объём и структура диссертации**

Диссертация состоит из введения, 4-х глав, заключения, списка литературы и приложения. Основной текст диссертации состоит из 136 страниц и включает 59 рисунков и 5 таблиц.

**ЗАКЛЮЧЕНИЕ**

В диссертационной работе рассмотрен комплекс теоретических и практических вопросов, связанных с разработкой высокочувствительных методов универсального стегоанализа. Основу данных методов оставляют подсистемы выделения векторов признаков из многомасштабного субполосного представления стегоконтейнера и подсистема их классификации. В работе были получены следующие результаты:

1. Проведен анализ существующих методов стеганографии и стегоанализа, рассмотрены варианты действий злоумышленника по преодолению стегоаналитических систем, построенных на основе статистических методов обнаружения скрытых сообщений. Было установлено, что минимальное изменение, внесённое в метод сокрытия сообщений способно привести к полной неэффективности статистических методов стегоанализа. Помимо этого установлено, что методы статистическиго стегоанализа неэффективны при отличии области анализа от области встраивания сообщения.
2. Проанализирован подход к разработке универсальных методов стегоанализа, позволяющих преодолевать данные ограничения статистических методов стегоанализа. Сформулированы требования к модели стегоконтейнера, в частности к свойствам векторов признаков при выполнении которых сохраняется эффективность методов универсального стегоанализа. Разработана обобщённая структура универсального метода стегоанализа, удовлетворяющая вышеперечисленным требованиям, которая состоит из подсистем формирования векторов признаков и подсистемы классификации, на основе которой возможно построение как пороговых, так и количественных методов стегоанализа изображений и звуковых сигналов. Проведен анализ существующих моделей сигнала-изображения и аудиосигнала, а именно преобразования Фурье, дискретного косинусного преобразования, вейвлет преобразования. Разработана модель стегоконтейнера, в основе которой лежит многомасштабная вейвлет­декомпозиция аналогового сигнала, что даёт возможность анализа множества масштабов и направлений для изображений, а также частотных субполос для звуковых сигналов. При этом за счёт возможности выбора произвольного дерева декомпозиции, а следовательно и анализируемых особенностей сигнала сохраняется единый подход к стегоанализу как контейнеров- изображений, так и контейнеров-звуковых сигналов. Это также позволяет при необходимости адаптировать модель к особенностям стеганографических методов и форматов контейнеров. Для устранения избыточности вектора признаков предлагается использовать анализ главных компонент, позволяющий снизить размерность вектора признаков в 4,8-5 раз и значительно повысить эффективность обучения. В качестве классификатора в пороговых и интерполятора к количественных методах предлагается использовать искусственные нейронные сети. В пороговых методах стегоанализа наилучший результат был показан многослойным персептроном, в количественных — искусственной нейронной сетью на основе радиальных базисных функций.
3. Разработаны методы стегоанализа на основе предложенной модели

контейнера и нейросетевой классификации векторов признаков. Достоинством методов является адаптивность к особенностям форматов контейнеров и высокая чувствительность. Разработанный метод порогового стегоанализа изображений на основе анализа битовых плоскостей позволяет обнаружить скрытые методом замены НЗБ сообщения. Метод количественного стегоанализа изображений позволяет получать оценку длины встроенных сообщений. Разработанный метод обнаружения скрытых сообщений в аудиофайлах позволяет обнаруживать скрытые сообщения до степени заполнения 2% при точности классификации 87% и равных уровнях ошибок первого и второго рода. Метод порогового стегоанализа изображений обнаруживает наличие встроенной информации при использовании свыше 2% от максимальной ёмкости НЗБ-плоскости в полноцветных изображениях размерности 256x256 пикселей при точности классификации 80%. Точность разработанного количественного метода классификации изображений составила 90-95% для изображений формата JPEG размерности 256x256 пикселей, содержащих скрытые сообщения размером от 2 до 20% максимальной ёмкости. Точность классификации при той же размерности составляет 91% для 20% от максимального размера сообщения. При анализе контейнеров-изображений, не подвергавшихся компрессии, достигаемая точность составляет 70% при 2% изменённых НЗБ- битов контейнера.