Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

На правах рукописи

УДК 004.056.55

РЫТОВА
Анна Валерьевна

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В МЕДИА-ПРОСТРАНСТВЕ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологии

по специальности 1-39 81 01 «Компьютерные технологии проектирования электронных систем»

Минск 2018

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель:	**Цырельчук Игорь Николаевич**, кандидат технических наук, доцент кафедры проектирования информационно-компьютерных систем, декан факультета инновационного непрерывного образования
Рецензент:	**Рудикова Лада Владимировна**, кандидат физико-математических наук, доцент, заведующая кафедрой «Современных технологий программирования» Гродненского государственного университета имени Янки Купалы

Защита диссертации состоится «27» января 2018 г. года в $10^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г.Минск, ул. П.Бровки, 6, 1 уч. корп., ауд. 415, тел.: 293-20-80, e-mail: kafpiks@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

КРАТКОЕ ВВЕДЕНИЕ

Медиа – обширное понятие, включающее в себя средства коммуникации, способы передачи информации, а также образовываемую ими среду (медиа-пространство). В современном контексте медиа включает в себя всю совокупность технологических средств и приемов коммуникаций, служащих для передачи конкретному потребителю информационного сообщения в том или ином виде: текст, музыка, изображение.

Использование цифровых форматов мультимедиа в настоящее время стало повсеместным. Но наряду с этим в современном информационном обществе, исследования и разработки в области стеганографии становятся все более популярными. Это связано с тем, что существуют проблемы управления цифровыми ресурсами и контроля использования прав собственности на компьютерные файлы. Отсюда возникает актуальнейшая задача сокрытия информации в условиях развитой инфраструктуры сетевого общения пользователей – интернет-участников открытого и неконтролируемого взаимодействия в медиа-пространстве. Сокрытие конфиденциальной информации в медиа-пространстве обычно производят при помощи стеганографических алгоритмов.

Одним из наиболее эффективных методов защиты мультимедийной информации является встраивание в защищаемый объект невидимых меток – цифровых водяных знаков (ЦВЗ). Стегосистемы ЦВЗ, в частности, должны выполнять задачу защиты авторских и имущественных прав на электронные сообщения при различных попытках активного нарушителя искажения или стирания встроенной в них аутентифицирующей информации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

На начальном этапе диссертационных исследований был проведен анализ состояния в области стеганографических алгоритмов, предназначенных для сокрытия информации в медиа-пространстве. В результате этого анализа был сделан вывод о необходимости разработки стеганографического алгоритма, скрывающего большие объемы данных в неподвижных изображениях широко используемых графческих форматах.

Применение стегоалгоритма позволяет создать систему скрытой передачи информации между абонентами. Посторонние лица такие процессы будут воспринимать как обычные обмены цифровыми файлами.

В ходе диссертационных исследований был выбран формат *JPEG*, являющимся одним из наиболее распространенных форматов при использовании цифровой графики, например - цифровых фотографий.

Существует огромное количество внешних воздействий на изображение, причем некоторые из них имеют специфический характер и вероятность их использования для коммерческого применения изображений мала. Это такие воздействия как: различного рода зашумления, фильтрация, модифика-

ция геометрии, смена палитры и т.д. Другие виды воздействий, наоборот, часто применяют при коммерческой эксплуатации фотографий. Например, масштабирование и сжатие с потерями, фрагментация, перевод в другой цифровой формат, обрезка.

Таким образом из вышесказанного следует, что тема диссертационной работы является актуальной.

Степень разработанности проблемы

На сегодняшний день существует достаточно большое количество работ в области методов и средств защиты конфиденциальной информации в медиа-пространстве.

Исследование методов и средств защиты конфиденциальной информации в медиа-пространстве на базе стеганографических методов осуществлялось на основе построения теоретических моделей с использованием работ российских и белорусских ученых: А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов, А.В. Лейман, И.М. Кутузов и др.

Одним из недостатков исследований, представленных в современной технической литературе, является неполное рассмотрение методов и средств защиты конфиденциальной информации в медиа-пространстве.

Предложенное исследование направлено на устранение этого недостатка на базе стеганографических методов защиты конфиденциальной информации в медиапространстве.

Цель и задачи исследования

Целью диссертационной работы является рассмотреть и разработать методы и средства защиты конфиденциальной информации на базе стеганографических алгоритмов, встраивающие и скрывающие большие объемы информации в графические изображения формата *JPEG* с последующей передачей этой информации.

Для достижения поставленной цели в ходе диссертационного исследования необходимо решить следующие задачи:

1. Проанализировать классы стеганографических алгоритмов.
2. Разработать стеганоалгоритм, выполняющий операции внедрения большого объема информации в графическое цифровое изображение на передающей стороне, и извлечения внедренной информации на принимающей стороне. Реализовать надежное функционирование разработанного стеганографического алгоритма при потере битов, выполняя межформатные преобразования.
3. Протестировать разработанный стеганографический алгоритм и доступные аналогичные системы, сравнивая по быстродействию и объему внедренных данных.

Теоретическая и методологическая основа исследования

В основу диссертации легли результаты известных исследований белорусских и зарубежных технологов в области методов и средств защиты кон-

фиденциальной информации в медиапространстве.

Для получения теоретических результатов исследования использовались статьи, книги и публикации специалистов в области стеганографических методов и алгоритмов средств защиты конфиденциальной информации в медиа-пространстве.

Информационная база методов и средств защиты конфиденциальной информации в медиа-пространстве сформирована на основе ранее проведенных исследований в области стеганографии с последующим построением алгоритмов.

Научная новизна работы заключается в получение следующих результатов:

1. Проведен качественный анализ классов стеганографических алгоритмов, специализирующихся на встраивании данных в цифровые изображения, для задачи скрытой передачи данных;
2. Разработаны алгоритмы для работы со структурами цифровых изображений форматов *JPEG* и *BMP*;
3. Был разработан метод, сочетающий в себе пространственый и форматный методы встраивания. Этот метод позволяет скрывать данные большого объема.

Основные положения, выносимые на защиту

1. Систематизация информации о стеганографии, понятие цифрового водяного знака, рассмотрение требований, предъявляемых к ЦВЗ, классификации стеганосистем ЦВЗ, представление математической модели стеганосистем ЦВЗ.
2. Анализ стеганоалгоритмов для графических контейнеров, рассмотрение стеганоалгоритмов пространственной области и области встраивания. Стеганоалгоритм на основе пространственного и форматного подходов к внедрению информации
3. Методы построения системы скрытой передачи информации большого объема в цифровых файлах формата *JPEG*. Метод расчета максимального объема информации при встраивании в файл формата *JPEG*.

Теоретическая значимость диссертации состоит в том, что были рассмотрены методы и средства защиты конфиденциальной информации на базе стеганографических алгоритмов, предложена стегосистема встраивающая и скрывающая большие объемы информации в графических изображениях формата JPEG с последующей передачей этой информации.

Практическая значимость работы заключается в том, что:

1. Разработан новый стеганоалгоритм для сокрытия информации большого объема в цифровых изображениях;
2. Реализованы функции работы с форматами *JPEG* и *BMP*, анализирующие и изменяющие структуру сегментов файлов;
3. Разработаны сценарии использования программной реализации стеганографического алгоритма в автоматическом режиме.

Апробация и внедрение результатов исследования

Результаты исследования были представлены на 52-я научно-техническая конференция аспирантов, магистрантов и студентов БГУИР, международная научно-практическая конференция «Инновационные процессы в научной среде» (шифр KON-143), VII международной научно-практической конференции «Технические науки: проблемы и решения», Москва, Россия, 2018 г.

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 6 печатных работах. В их числе 4 статьи в сборнике материалов научной конференции, 2 тезиса докладов на научных конференциях.

Структура и объем работы.

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трёх глав и заключения, библиографического списка и приложений. Общий объем диссертации − 100 страниц. Работа содержит 4 таблицы, 18 рисунков. Библиографический список включает 54 наименования.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении было проведено обоснование актуальность темы исследований, сформулирована цель работы, определены основные защищаемые положения, отмечена научная новизна и практическая ценность, кратко изложено основное содержание работы.

В **общей характеристике работы** сформулированы ее цель и задачи, показана связь с научными программами и проектами, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также, структура и объем диссертации.

В первой главе дан исторический обзор возникновения стеганографии, проанализированы тенденции и закономерности развития стеганографических систем, определено понятие цифрового водяного знака (ЦВЗ), рассмотрены требования, предъявляемые к ЦВЗ, дана классификация стеганосистем ЦВЗ, представлена математическая модель стеганосистем ЦВЗ.

Задача защиты информации от несанкционированного доступа была поставлена и решалась человечеством очень давно. Для решения этой задачи выделилось два основных направления, существующие и сейчас: криптография и стеганография. Целью криптографии является скрытие содержимой информации за счет ее шифрования. А стеганография скрывает сам факт наличия передаваемой информации.

Объекты, в которые встраивается информация, называют контейнерами, имеющие различную природу Для цифровой стеганографии контейнера-

ми, например, являются файлы различных мультимедийных форматов (видео, изображений и музыкальных).

Встраивание информации в изображение базируется на особенностях форматов хранения данных и избыточности служебных данных. Цифровые фотографии, музыка и видео представлены матрицами, где записана интенсивность сигналов в дискретные моменты в пространстве и/или времени. Например, если контейнер является изображением, то это матрица чисел, соответствующих интенсивности света в заданный момент времени.

Младшие биты байтов представления информации содержат неиспользуемую информацию. Поэтому их перезапись, то есть внедрение какой-то информации, практически не влияет на восприятие изображения человеческим глазом. Это является основой для встраивания в графический файл дополнительной информации.

Задачу встраивания и выделения информации из полученного контейнера решает стегосистема, состоящая из представленных на рисунке 1 следующих основных элементов.

– прекодер — устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в сигнал-контейнер. (Контейнером называется информационная последовательность, в которой прячется сообщение);

– стегокодер — устройство, предназначенное для осуществления вложения скрытого сообщения в другие данные с учетом их модели;

– устройство выделения встроенного сообщения;

– стегодетектор — устройство, предназначенное для определения наличия стегосообщения;

– декодер — устройство, восстанавливающее скрытое сообщение.

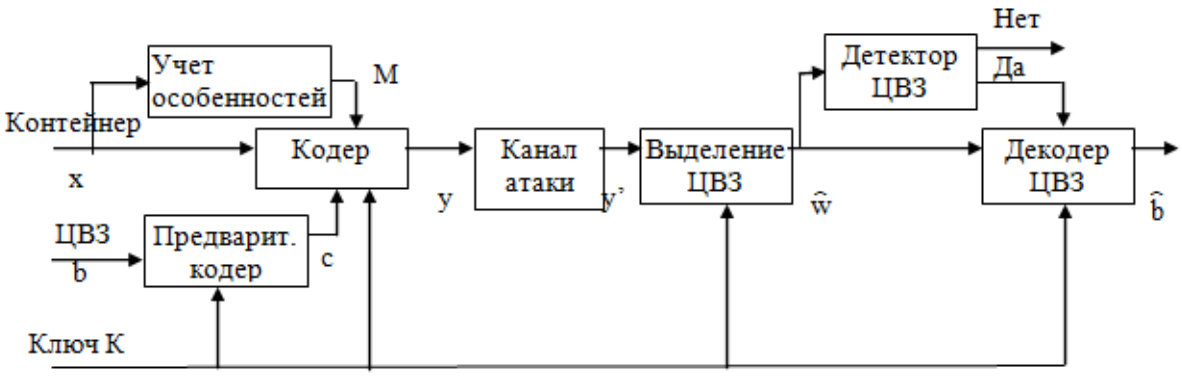

Рисунок 1 – Структурная схема типичной стегосистемы ЦВЗ

Во второй главе дан анализ стеганоалгоритмов для графических контейнеров, рассмотрены стеганоалгоритмы пространственной области и области встраивания.

Стеганоалгоритмы этого класса встраивают информацию в область самого изображения. Достоинство в том, что для внедрения информации не

надо проводить вычислительно-трудоемкие линейные преобразования изображений. Информация встраивается манипуляциями цветовыми составляющими или яркостью.

В стеганоалгоритмах области наиболее популярны два преобразования: дискретное косинусное преобразование (ДКП) и вейвлет-преобразование (ВП).

ДКП применяется при сжатии *JPEG*-изображений. Этот факт объясняет большую популярность применения ДКП в стеганографии *JPEG*. А вот ВП служит базой для сжатия в алгоритме *JPEG 2000*.

ДКП применяют или ко всему изображению, или к отдельным блокам. Обычно контейнер разделяют на блоки 88 пикселей. Затем к каждому блоку применяют ДКП. Полученные матрицы коэффициентов ДКП имеют размер 88.

Одной из самой применяемой метрикой при вычислении уровня модификаций, которые внедряются стеганографический контейнер встраивая ЦВЗ, есть максимум соотношения «сигнал/шум», то есть *PSNR (Peak Signal Noise Range)*. В роли сигнала принимается исходная фотография, а за шум - изменения, появляющиеся при внедрении ЦВЗ.

Главным изъяном перечисленных выше метрик служит нулевая корреляция с системой человеческого зрения (СЧЗ). Расчет оценки изменений для этих метрик проводится по всей фотографии. А поэтому и оценка изменений получается по всей фотографии, не учитывая локальных изменяющихся воздействий

Метрики, которые учитывают особенности СЧЗ, базируются на: чувствительности к яркостной флуктуации фотографии, эффект маскировки в пространственной области и т.д.

Одним из методов, использующихся при создании таких метрик, есть метод предварительной фильтрации фотографии полосовым фильтрам, моделирующего СЧЗ.

В другом методе создания таких метрик происходит вейвлет преобразование оригинальной и модифицированной фотографии. В полученном результате фотография представляется в разных масштабах.

Затем в любом вейвлет-поддиапазоне выбирается свой вес (масштабный), который умножается на свою метрику, рассчитанную для локальной области. Для каждой задачи веса свои. К примеру, когда необходим учет высокочастотных (ВЧ) составляющих (четкость линий и т. д.), то их (веса) увеличивают. К основным трудностям при построении таких метрик относят большие вычислительные затраты. Кроме того, необходим подбор множества коэффициентов, размера окон и типов фильтрации. Результатом работы правильно настроенной метрики, является достоверная оценка. Но этот результат появляется только для конкретного возмущающего действия.

В ходе диссертационных исследований была разработана метрика оценки качества исходной фотографии и модифицированной различными стеганографическими алгоритмами внедрения информации.

Метрика базируется на дискретном косинус-преобразовании (ДКП),

которое применяется к блокам 8x8 пикселей исходной фотографии. Матрица коэффициентов ДКП модифицированной фотографии вычитается из матрицы ДКП блока исходной фотографии.

Полученная матрица делится на матрицу квантующих коэффициентов стандарта *JPEG*. Использование такой матрицы дает возможность учета особенностей СЧЗ. Выходным результатом рассмотренной метрики является карта изменений блоков фотографии и просуммируемый коэффициент изменений.

Разработанные метрика и методика сравнительного анализа были использованы при расчете оценки устойчивости ЦВЗ к сжатию с потерями *JPEG*-2000. Изображениями-контейнерами являлись полутоновых цифровых фотографий с разрешением 640x640 пикселов.

Для стегоалгоритмов, которые производят внедрение в ВЧ поддиапазоны, внедрение происходило в поддиапазоны максимальной глубины разложения. Коэффициент качества *K jpeg*-2000 изменялся в пределах от 0 до 100. Стеганографические алгоритмы, производящие внедрение в ВЧ поддиапазоны, показывают слабую устойчивость к сжатию с потерями *JPEG-2000*.

Небольшая разница в отличии в устойчивости стегоалгоритмов, производящих внедрение в НЧ поддиапазон, объясняется отличиями в методе внедрения.

В третьей главе проведена разработка стеганоалгоритма *StegoKS*, используя форматные и пространственные принципы сокрытия данных.

Для эффективной работы, исходя из анализа структуры формата файлов *JPEG*, были определены маркеры, которые не участвуют в *JPEG* преобразовании и не влияют на качество изображения, и поэтому их игнорируют программы просмотра: *COM*, *APP15*, *DAC*, *DNL*, *SOF SOF10*, неспецифицированные сегменты. В сегментах, определяемых этими маркерами, можно скрытно хранить информацию. Но надо учитывать ограниченность объема сегмента, а именно задаваемое двумя байтами величину – 0xFFFF.

Далее была проведена разработка стеганоалгоритма.

Сначала были разработаны и реализованы в виде программы парсеров алгоритмы разбора (парсинга) файлов *JPEG* и *BMP*-файлов.

Результат работы этих программных средств есть структурированное представление блоков, служащий для последующего исследования потенциально-пригодных байтов для записи информации.

Стегосистема должна обеспечить тайную передачу информации, применяя неподвижное изображение в *JPEG*-файле в качестве контейнера. Информация внедряется в графический файл – контейнер.

Затем этот файл доставляется адресату, который извлекает из полученного изображения переданную тайную информацию

Стегосистема принимает исходные входные данные и проверяет их корректность:

1. Наличие исходных файлов на носителе;
2. Соотношения размеров исходных файлов;
3. Соответствие формату *JPEG* файла-контейнера.

В соответствии с требованиями к стегосистеме, до внедрения информация должна быть зашифрована и сжата. Затем, подготовленная таким образом информация должна быть проанализирована на возможность внедрения учитывая настраиваемые параметры встраивания и объема контейнера. Схема алгоритма подготовки информации к внедрению представлена на рисунке 2.

Рисунок 2 – Стеганоалгоритм подготовки информации к встраиванию

Алгоритм внедрения битов информации представлен на рисунке 3.

С целью минимального изменения пространственной области, реализованная стегосистема, по умолчанию использует только младший бит такого байта. Это позволяет получить минимальную вероятность даже на изображениях с большой площадью заливки синего цвета. Самый простой метод замещения битов состоит в последовательной замене в каждом b-байте.

Jstg и JPHS выбранные стегоалгоритмы для сравнения и разработанный стегоалгоритм оценивались максимальному размеру информации (*txt*-файл, текст на русском языке), который можно внедрить в *JPEG*-файл объемом 2560212 байт (цифровое фото отличного качества).

Рисунок 3 – Стегоалгоритм внедрения информации

На рисунке 4 представлены результаты сравнительного анализа (отсортировано по убыванию размеров). Этот рисунок показывает, что разработанный стегоалгоритм получает результат значительно лучше, по сравнению с *JPHS* и *JSteg*. И это даже работая в режиме с 1 *LSB.*

Выходные *JPEG*-файлы с встроенной информацией разного объема проверялись при помощи программы проверки детектирования факта встраивания *Stegdetect*. Эта программа производит поиск байтовых сигнатур, которые показывают, что было стегомешательство.

Существуют различные опции функционирования, приспособленные на обнаружение внедрения информации, сделанные *JPHS* и *JSteg*.

Проведенные экспериментальные исследования показали, что *Stegdetect* не определяет факта встраивания информации разработанным стегоалгоритмом.

Кроме того, внедрение информации при помощи человеческого глаза, тоже не обнаруживается. Сравнивался исходный (без внедренного сообщения) *JPEG*-файл и обработанный. возможно сказать, где фотография с внедренной информацией.

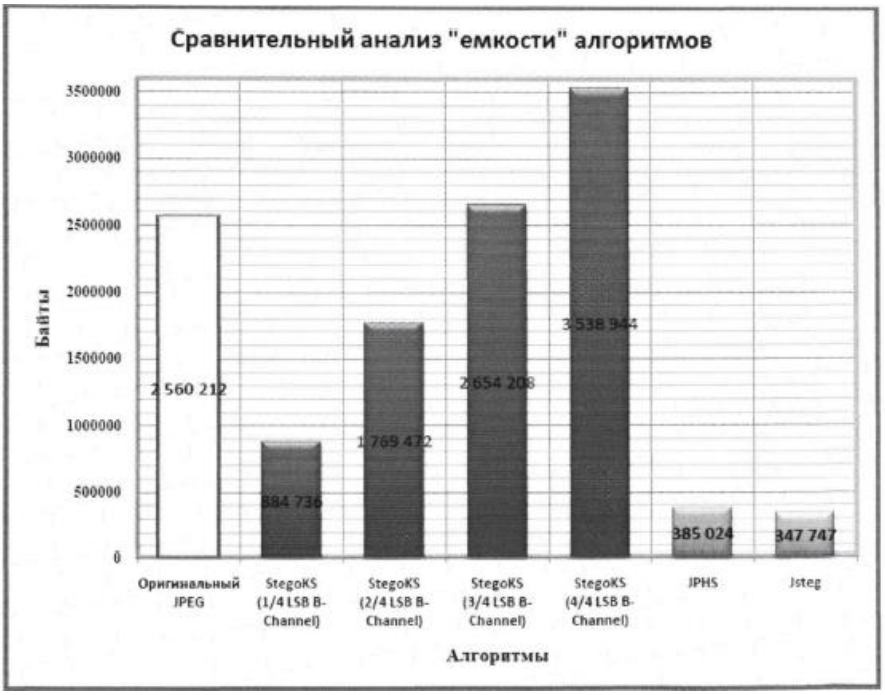

Рисунок 4 – Результат сравнительного анализа

ЗАКЛЮЧЕНИЕ

Основные результаты диссертационной работы:

1. Проведен анализ классов стеганоалгоритмов. Определены основные тенденции и закономерности развития стеганосистем. Показано, что разработка стеганосистем, используя различные подходы, является актуальной задачей. Проведен анализ применения различных подходов при разработке стеганоалгоритмов.

2. Разработан стеганоалгоритм, позволяющий выполнять операции встраивания большого объема информации в стегоконтейнер изображения на передающей стороне и извлечения этой информации на принимающей стороне. Обеспечено надежное функционирование разработанного стеганоалгоритма в условиях потерь битов при межформатных преобразованиях. Предложена метрика оценки искажений изображений, обеспечивающая объективность сравнительного анализа устойчивости различных стеганоалгоритмов в области встраивания. Проведено сравнение по критерию возможного объема внедряемой информации разработанного стеганоалгоритма и имеющихся в свободном доступе стегосистем.

3. Проведенные исследования общедоступной программой *Stegdetect* на предмет внедрения в контейнер ЦВЗ разработанным алгоритмом, показали, что *Stegdetect* не детектирует ЦВЗ. Разработанный стеганоалгоритм показывает более лучшие результаты, чем алгоритмы *JPHS* и *JSteg*. И это даже в режиме применения лишь 1 *LSB* в качестве хранилища данных.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

Статьи в сборниках материалов научных конференций

[1] Рытова А.В. / Атаки мобильных устройств на основе коммуникаций // VII международной научно-практической конференции «Технические науки: проблемы и решения», Москва, Россия, 2018. – в печати.

[2] Рытова А.В. / Вредоносные программы мобильных устройств // VII международной научно-практической конференции «Технические науки: проблемы и решения», Москва, Россия, 2018. – в печати.

[3] Рытова А.В. / Понятие об аудио и видео отпечатках // VII международной научно-практической конференции «Технические науки: проблемы и решения», Москва, Россия, 2018. – в печати.

[4] Рытова А.В. / Понятие о цифровых водяных знаках // VII международной научно-практической конференции «Технические науки: проблемы и решения», Москва, Россия, 2018. – в печати.

Тезисы конференций

Рытова А.В. / Механизмы защиты от инфраструктурных DDoS-атак / А.О. Давидовский, А.В. Рытова, А.И. Якубашко, // материалы 52-ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно-компьютерных систем», Минск, Респ. Беларусь, 25–30 апреля 2016 г. / УО «БГУИР». – Минск, 2016. – 66-67.

Рытова А.В. / Data loss prevention системы. Выбор DLP-системы / А.В. Рытова, А.О. Давидовский // материалы 52-ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно-компьютерных систем», Минск, Респ. Беларусь, 25–30 апреля 2016 г. / УО «БГУИР». – Минск, 2016. – 68.

РЕЗЮМЕ

Рытова Анна Валерьевна

Методы и средства защиты конфиденциальной информации в медиа-пространстве

***Ключевые слова*:** стеганография, цифровые водяные знаки, стеггоалгоритм, стегосистема.

Цель работы: разработать алгоритм защиты конфиденциальной информации на базе стеганографии, встраивающие и скрывающие большие объемы информации в графические изображения формата JPEG с последующей передачей этой информации.

Полученные результаты и их новизна: проведен качественный анализ классов стеганографических алгоритмов, специализирующихся на встраивании данных в цифровые изображения, для задачи скрытой передачи данных. Разработаны алгоритмы для работы со структурами цифровых изображений форматов JPEG и BMP. Был разработан метод, сочетающий в себе пространственый и форматный методы встраивания. Этот метод позволяет скрывать данные большого объема.

Разработан стеганоалгоритм, позволяющий выполнять операции встраивания большого объема информацию в стегоконтейнер изображение на передающей стороне и извлечения этой информации на принимающей стороне. Обеспечено надежное функционирование разработанного стеганоалгоритма в условиях потерь битов при межформатных преобразованиях.

Проведенные исследования общедоступной программой Stegdetect на предмет внедрения в контейнер ЦВЗ разработанным алгоритмом, показали, что Stegdetect не детектирует ЦВЗ. Разработанный стеганоалгоритм показывает более лучшие результаты, чем алгоритмы JPHS и JSteg. И это даже в режиме применения лишь 1 LSB в качестве хранилища данных.

Степень использования: результаты внедрены в учебный процесс Белорусского государственного университета информатики и радиоэлектроники в лекционный курс «Проектирование электронных систем безопасности».

Область применения: защита конфиденциальной информации в медиапространстве.

РЭЗЮМЭ

Рытаў Ганна Валер'еўна

Метады і сродкі для абароны канфідэнцыйнай інфармацыі ў мэдыя-прасторы

Ключавыя словы: стеганография, лічбавыя вадзяныя знакі, стеггоалгоритм, стегосистема.

Мэта працы: распрацаваць алгарытм абароны канфідэнцыйнай інфармацыі на базе стеганографии, ўбудавальных і хаваюць вялікія аб'ёмы інфармацыі ў графічныя выявы фармату JPEG з наступнай перадачай гэтай інфармацыі.

Атрыманыя вынікі і іх навізна: праведзены якасны аналіз класаў стеганографических алгарытмаў, якія спецыялізуюцца на ўбудаванні дадзеных у лічбавыя выявы, для задачы схаванай перадачы дадзеных. Распрацаваны алгарытмы для працы са структурамі лічбавых малюнкаў фарматаў JPEG і BMP. Быў распрацаваны метад, які спалучае ў сабе прасторавага і фарматны метады ўбудавання. Гэты метад дазваляе хаваць дадзеныя вялікага аб'ёму.

Распрацаваны стеганоалгоритм, які дазваляе выконваць аперацыі ўбудавання вялікага аб'ёму інфармацыю ў стегоконтейнер малюнак на які перадае боку і забору гэтай інфармацыі на прымаючага боку. Забяспечана надзейнае функцыянаванне распрацаванага стеганоалгоритма ва ўмовах страт бітаў пры межформатных пераўтварэннях.

Праведзеныя даследаванні агульнадаступнай праграмай Stegdetect на прадмет ўкаранення ў кантэйнер ЦВЗ распрацаваным алгарытмам, паказалі, што Stegdetect ня дэтэктуе ЦВЗ. Распрацаваны стеганоалгоритм паказвае больш лепшыя вынікі, чым алгарытмы JPHS і JSteg. І гэта нават у рэжыме прымянення толькі 1 LSB у якасці сховішча дадзеных.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс Беларускага дзяржаўнага універсітэта інфарматыкі і радыёэлектронікі ў лекцыйны курс «Праектаванне электронных сістэм бяспекі».

Вобласць ужывання: абарона канфідэнцыйнай інфармацыі ў медыя-прасторы.

SUMMARY

Rytova Anna Valeryevna

Methods and means of protecting confidential information in the media space

Keywords: steganography, digital watermarks, steggoalgorithm, stegosystem.

Objective: to develop an algorithm for protecting confidential information based on steganography, embedding and hiding large amounts of information in graphics images of JPEG format with the subsequent transfer of this information.

The results and their novelty: A qualitative analysis of the classes of steganographic algorithms specializing in embedding data in digital images for a hidden data transmission task was carried out. Algorithms for working with structures of digital images of JPEG and BMP formats are developed. A method was developed that combines the spatial and format methods of embedding. This method allows you to hide large data.

A steganogalgorithm has been developed that allows you to perform operations of embedding a large amount of information in a stegocontainer image on the transmitting side and extracting this information on the receiving side. The reliable functioning of the developed stegano algorithm in the conditions of bit loss during inter-format conversions is ensured.

The studies conducted by the publicly available Stegdetect program for the introduction into the CEH container of the developed algorithm have shown that Stegdetect does not detect the CEH. The developed steganoalgorithm shows better results than the algorithms JPHS and JSteg. And this is even in the mode of applying only 1 LSB as a data store.

Use degree: the results are introduced into the educational process of the Belarusian State University of Informatics and Radioelectronics in the lecture course "Design of Electronic Security Systems".

Field of application: Protection of confidential information in the media space.