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

УДК 004.021

Дубовик
Сергей Игоревич

Методы и средства стеганографии в графических медиафайлах

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Ярмолик В.Н.
д.т.н., профессор

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

На сегодняшний день можно выделить две основные сферы применения компьютерной стеганографии: защита авторских прав интеллектуальной сбоственности для продуктов мультимедиа индустрии с использованием цифровых водяных знаков (ЦВЗ); скрытие передачи (или хранения) конфедециальной информации. При использовании стеганографии в первом случае скрытое сообщение является информацией о скрывающем контейнере и в большинстве случаев наблюдателю известно о присутствии секретного сообщения, во втором случае контейнер используется лишь в качестве маскировки встроенной информации, что бы отвелчь внимание наблюдателя от передаваемого сообщения.

Существует множество внешних воздействий, которым может быть подвергнуто изображение, являющееся интеллектуальной собственностью. Такие воздействия как зашумления, фильтрации, изменение палитры и т.п. маловероятны в ходе коммерческого использования изображения. Однако кадрирование, сжатие, масштабирование или перевод в другой цифровой формат с большой вероятностью могут применяться к таким изображениям. При воздействии последних факторов часть информации, закодированной в контейнер, может удалиться, а значит, может исчезнуть и зашифрованное сообщение.

Защищать передаваемую (или хранимую) ифнормацию от несанкционированного использования приходится во многих случаях. Это требуется при решении государственных, дипломатических, военных задач, в работе бизнеса (коммерции), при исследовании новых научно-технических проблем, а так же при решении других задач, связанных со скрытой передачей и (или) хранением информации, которая в определенных условиях может быть запрещена. Защищать информацию требуется при государственном документообороте и при ведении частной переписки. Развитие современных теле- и интернет-коммуникационных технологий невозможно представить без защиты передаваемой информации.

Необходимость разработки и исследования новых систем со скрытой передачей информации объясняется уязвимостью существующих способов защиты информаии и их относительно слабую устойчивость к стеганоанализу.

Использование только криптографических методов шифрования данных нежелательно, поскольку наличие факта передачи секретной информации привлекает внимание злоумышлениикоов и увеличивает шанс того, что информация будет получена и расшифрована посторонними лицами.

Исходя из вышенаписанного, проблема разработки алгоритма стеганографии, сохраняющего зашифрованную информацию при сжатии изображения-контейнера, незначительных геометрических изменениях контейнера, и максимально устойчивого к стеганоанализу, является актуальной на сегодняшний день.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является анализ существующих методов и средств стеганографии в гарфических медиаданных на устойчивость к сжатию и стеганоанализу; попытаться разработать эффективный метод скрытия информации в наиболее распространенных графических форматах. Данный метод должен быть устойчив к стеганоанализу, а так же сохранять зашифрованные данные после сжатия графических объектов.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Разработать методику сравнительного анализа устойчивости различных стеганоалгоритмов к стеганоанализу и сжатию.
2. Провести анализ устойчивости к сжатию, геометрическим преобразованиям и стеганоанализу различных стеганоалгоритмов.
3. Провести анализ воздействия сжатия на внедренное сообщение и определить пределы устойчивости стеганоалгоритмов.
4. Разработать методы и алгоритмы повышения устойчивости скрытого сообщения к сжатию с потерями и стеганоанализу.

Объектом исследования являются доступные методы и средства стеганографии в графических данных.

Предметом исследования является устойчивость к стеганоанализу и различным внешним воздействиям на контейнер существующих методов стеганографии графических данных.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность встраивания скрываемой ифнормации в область низкочастотных компонентов матрицы ДКП с внесением незначительных для СЧЗ изменений. Особенности встраивания бит скрываемого сообщения в низкочастотные компоненты матрицы ДКП заключается в более высокой устойчивости к сжатию, но при этом вносятся более заметные искажения в изображение-контейнер. Скрытие сообщения в низкочастотных коэффициентах матрицы ДКП позволит значительно повысить устойчивость внедренного сообщения к сжатию.

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя В. Н. Ярмолика, заключается в формулировке целей и задач исследования, а так же в консультациях и советах по улучшению алгоритма.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на 51-ой научной конференции аспирантов, магистрантов и студентов БГУИР (Минск, Беларусь, 2015).

Опубликованность результатов диссертации

По теме диссертации опубликовано 1 печатная работ – статья в сборнике материалов 51-ой научной конференции аспирантов, магистрантов и студентов БГУИР.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, пяти глав, заключения, списка использованных источников и приложений. В первой главе представлен исторический обзор развития стеганографии, даны некоторые основные понятие и определения, используемые в области стеганографии, проведен анализ основных направлений стеганографии. Вторая глава посвящена анализу существующих алгоритмов встраивания данных, проведена оценка устойчивости встроенных данных к внешним воздействиям. В третьей главе проведен анализ деградирующего воздействия JPEG сжатия и некоторых геометрических преобразований на встроенное сообщение. В четвертой главе предложены методы повышения устойчивости скрываемых данных к JPEG сжатию. Пятая глава посвящена разработе алгоритма встраивания данных, устойчивого к JPEG сжатию и некоторым геометрическим преобразованиям.

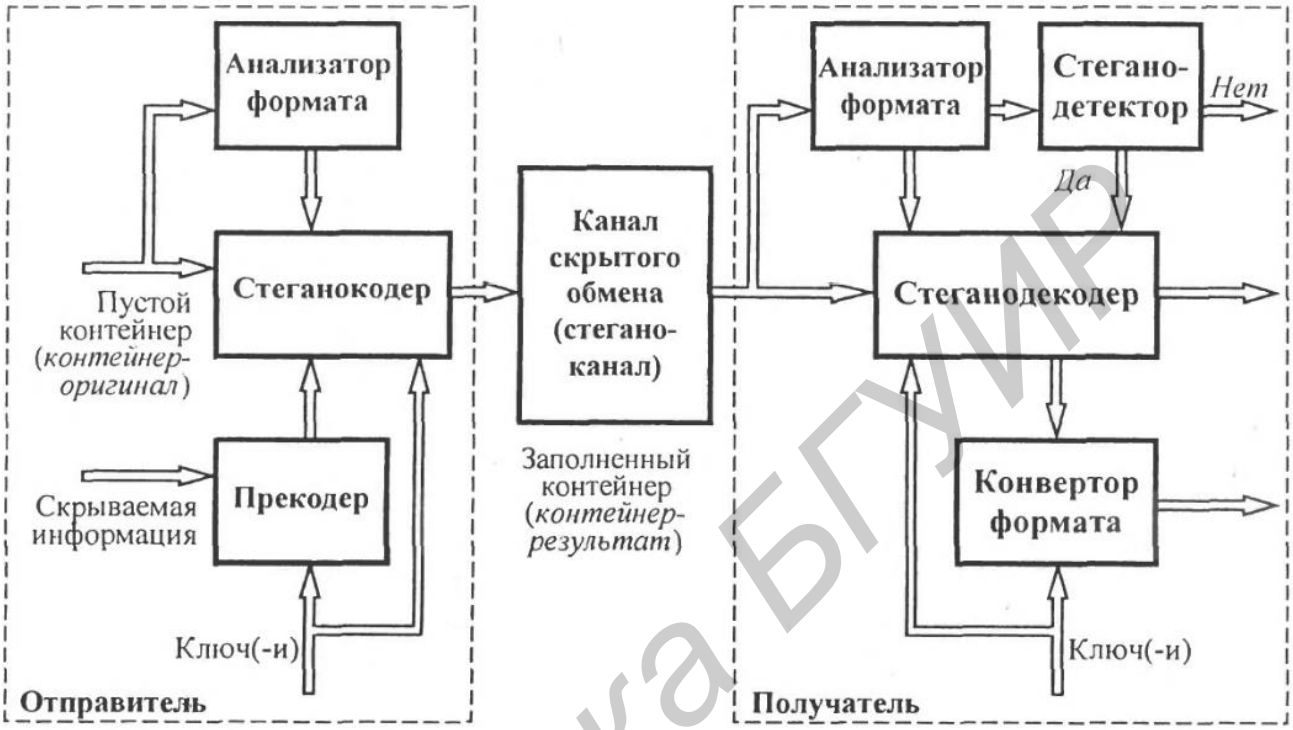
Общий объем работы составляет 57 страниц, из которых основного текста – 44 страницы, 23 рисунка на 19 страницах, 4 таблицы на 6 страницах, список использованных источников из 17 наименований на 2 страницах и 1 приложение на 3 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

В **первой главе** описаны основные потяния и определения, используемые в стеганографии и определена роль использования стеганографии в области защиты информации. Проведен исторический обзор развития стеганографии. Дано понятие стеганосистемы и основных, состовляющих ее, компонентов.

Так, стеганосистема представляет собой совокупность средств и методов, которые используются с целью формирования скрытого канала передачи информации. Причем процесс скрытия данных отличается от операции шифрования. Его целью является не ограничивать или регламинтировать доступ к фай-



лу-контейнеру, а гарантировать, что встроенные данные останутся неповрежденными и подлежащими восстановлению. Обобщенная структурная схема стеганосистемы представлена на рисунке 1.

Рисунок 1 – Обобщенная структурная схема стеганосистемы

Одним из наиболее эффективных методов стеганографии в области защиты мультимедийной информации является встраивание в защищаемый объект специальной информации, называемой цифровыми водяными знаками (ЦВЗ). В данной главе дано определение и классификация ЦВЗ, и описаны требования, предъявляемые к ЦВЗ.

Вторая глава посвящена анализу существующих алгоритмов стеганографии в графических медиаданных. Проведена классификация алгоритмов по различным критериям, дано сравнительно описание некоторых алгоритмов.

Для дальнейшей доработки и улучшения был выбран алгоритм Коха-Жао, основанный на применении дискретного косинусного преобразования (ДКП). Выбор алгоритма обсуловлен сравнительно простой реализацией и небольшой ресурсозатратностью. Так же, использование ДКП увеличивает устойчивость к сжатию JPEG, поскольку этот алгоритм сжатия также использует ДКП.

Для алгоритма Коха-Жао была определена зависимость коэффициента ошибочных бит (BER) от коэффициента качества jpeg при различных коэффициентах силы встраивания, которая представлена на рисунке 2.

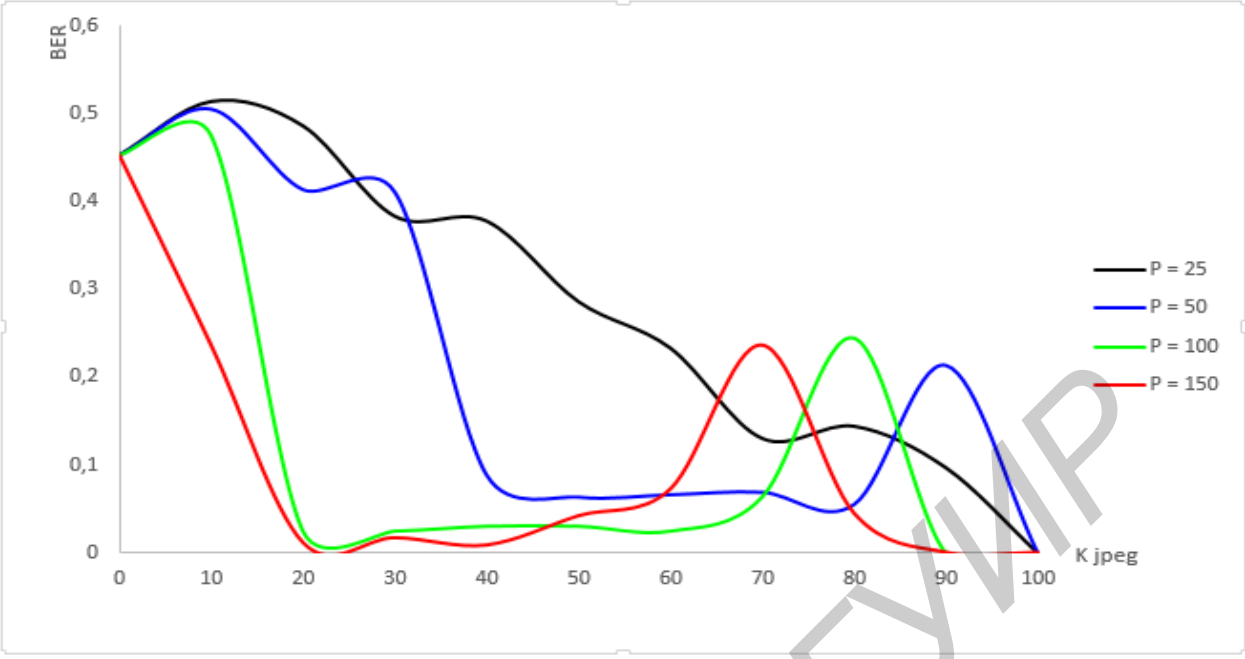


Рисунок 2 – Зависимость BER от коэффициента качества JPEG при различных коэффициентах силы встраивания

BER определяет усточивость стеганоалгоритмов и представляет собой соотношение:

$$BER(S, S'') = \frac{\sum p_i}{N}. \quad (1.1)$$

где N – общее количество бит;

$$p_i = \begin{cases} 1 & если \quad s_i \neq s_i'' \\ 0 & если \quad s_i = s_i'' \end{cases}$$

s_i – j-й бит оригинала встраиваемой строки;

s_i'' – j-й бит извлеченной строки.

В **третьей главе** проведен анализ внешних воздействий на встроенное сообщение. Было изучено деградирующее воздействие сжатия и масштабирования на встроенно сообщение.

В ходе анализа алгоритма сжатия JPEG было выявлено три основные операции, приводящие к потере ифнормации изображения: прямое ДКП, обратное ДКП и квантование.

Потери на этапах прямого и обратного ДКП связаны с погрешностью самих преобразований. Величина погрешности не велика и при грамотном использовании стеганоалгоритмов встраивания не должна оказывать влияния на встроенную в область матрицы ДКП информацию. Под грамотным использованием стеганоалгоритмов, понимается выбор такого значения коэффициента силы встраивания P, которое создаст разницу между кодирующими коэффициентами превышающую максимальную погрешность прямого и обратного ДКП.

Таким образом, единственным деградирующим воздействием на ДКП матрицу, приводящим к потере встроенной информации при JPEG сжатии является квантование. Этап квантования выполняется при выборе пользователем режима сжатия «с потерями» так называемый «lossy mode». Уровень потерь в этом режиме задается Kjpeg, который имеет диапазон изменения от 0 до 100. Чем меньше значение этого коэффициента, тем больше сжатие изображения, а, следовательно, и больше уровень потерь.

Квантование коэффициентов матрицы ДКП осуществляется посредством квантующей матрицы. Коэффициенты квантующей матрицы рассчитываются по формуле

$$\begin{cases} q' = (100 - K_{jpeg})/50, & при \quad K_{jpeg} \geq 50 \\ q' = 50/K_{jpeg}, & при \quad K_{jpeg} < 50 \end{cases} \qquad (1.2)$$

где q – коэффициент, на который производится умножение коэффициентов матрицы квантования JPEG, см. рисунок 3.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

- НЧ компоненты;
- СЧ компоненты;
- ВЧ компоненты;

Рисунок 3 – Матрица квантования стандарта JPEG

В **четвертой главе** рассмотрены методы повышения устойчивости скрываемых данных к JPEG сжатию. К методам повышения устойчивости скрываемой информации можно отнести два следующих метода: перевод пикселей из цветовой модели RGB в цветовую модель YCbCr, поскольку в JPEG используется именно эта модель; встраивание информации в низкочастотные компоненты изображения.

При выполнении JPEG сжатия цветовая модель RGB должна быть преобразована в цветовую модель YCbCr [17]. Для преобразования из цветовой модели RGB в YCbCr используются следующие формулы:

Y = 0.299 * R + 0.587 * G + 0.114 * B;

Cb = -0.1687 * R - 0.3313 * G + 0.5 * B + 128;
Cr = 0.5 * R - 0.4187 * G - 0.0813 * B + 128;

Для обратного преобразования используются следующие формулы:

R = Y + 1.402 * (Cr - 128);
G = Y - 0.34414 * (Cb - 128) - 0.71414 * (Cr - 128);
B = Y + 1.772 * (Cb - 128);

Проанализировав матрицу квантования стандарта JPEG (см. рис. 3.1.2) можно убедиться, что квантующие коэффициенты уменьшаются в сторону низкочастотных компонент. То есть, при квантовании коэффициенты матрицы ДКП из низкочастотных областей подвергаются меньшему изменению относительно своих оригинальных значений. Особенность, позволяющая алгоритму JPEG многократно уменьшать размер файла сжимаемого изображения, как раз и заключается в обнулении большого числа коэффициентов матрицы ДКП. Чем меньше Kjpeg выбран пользователем, тем больше значения коэффициентов квантующей матрицы и тем больше коэффициентов матрицы ДКП будут обнуляться.

Был проведен опыт, из результатов которого было определено, что низкочастотные коэффициенты матрицы ДКП начинают обнуляться при достаточно низких значениях коээфициента качества JPEG. Однако, выбор для встраивания информации коэффициентов среднечастотных компонент большинством авторов стеганоалгоритмов далеко не случаен. Коэффициенты низкочастотных компонент содержат основную информацию о блоке и их модификация может серьезно повлиять на такой важный параметр - как скрытность внедрения. Следовательно, при использовании коэффициентов НЧ компонент, для обеспечения приемлемого для СЧЗ уровня искажений, придется уменьшать величину изменения коэффициентов НЧ компонентов по сравнению с аналогичными изменениями коэффициентов СЧ компонент.

В **пятой главе** был разработан алгоритм встраивания данных в графические изображения. По результатам работы алгоритма и сравнения этих результатов с результатами работы алгоритма Коха-Жао были выявлены недостатки и достоинства разработанного алгоритма.

По результатам работы алгоритма можно выделить следующие его достоинства:

1. Относительно высокая устойчивость к сжатию JPEG.
2. Внедренное сообщение вносит незначительные искажения в изображения, которые трудноразличимы СЧЗ.
3. Отсутсвтует возможность извлечь сообщение, не зная ключа встраивания.
4. Встраивание сообщения начиная от центра позволяет извлечь его при кадрировании, выполненном в определенном порядке.

5. За счет незначительно вносимых искажений существует возможность использовать алгоритм встраивания как трехкоэффициентный, что значительно повысит пропкускную способность стеганоканала.

Из недостатков можно выделить:

1. За счет встраивания сообщения по заданному ключу увеличивается время выполнения алгоритма и требуется больше вычислительных ресурсов.
2. Блоки с резкими перепадами яркости содержат большие абсолютные значения в ВЧ области, что может привести к очень большим искажениям при встраивании информации.
3. Монотонные изображения содержат в НЧ и СЧ области, как правило, нулевые компоненты. Модификация СЧ и НЧ области приведет к внесению видимых искажений.

Для больших изображений требуется значительное количество памяти, используемой при переводе из одной цветовой модели в другую и обратно. Динамическое выделение памяти может привести к небольшим «зависаниям» программы, выполняющей алгоритм.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Подводя итоги результатов, полученных в отдельных разделах работы, можно сказать, что цель диссертации, сформулированная во введении, достигнута, а именно, проведен сравнительный анализ средств и методов стеганографии в гарфических медиаданных, был выбран алгоритм для дальнейшего улучшения, а так же был доработан алгоритм Коха-Жао таким образом, что полученные характеристики отличаются, в лучшую сторону, от аналогичных характеристик оригинального алгоритма.

В процессе исследовательской деятельности по разработке алгоритма стеганографии; изучению воздейтсвия JPEG сжатия на изображение, а так же других возможных внешних воздействий, были получены следующие результаты:

1. Разработана методика сравнительного анализа устойчивости к JPEG сжатию различных стеганоалгоритмов.
2. Исследовано диградирующее воздействие JPEG сжатия на сообщение, встроенное в коэффициенты матрицы ДКП.
3. Проанализированы методы повышения устойчивости стеганоалгоритма к JPEG сжатию, а так же методы, повышающие надежность встраивания сообщения при незначительных искажениях изображения.
4. Разработан алгоритм встраивания сообщения в изображения;
5. Проведен сравнительный анализ результатов разработанного алгоритма с алгоритмом, лежащим в основе разработанного – Коха-Жао.

Использование разработанного алгоритма в области защиты информации позволит создать стеганографичесике системы, устойчивые к JPEG сжатию с

достаточно низким коэффициентом качества и к, существующему на сегодняшний день, статистическому стеганоанализу