**АННОТАЦИЯ**

диссертационной работы **Дайырбаевой Эльмиры Нурбеккызы**

на тему: «Разработка и исследование стеганографических алгоритмов, ориентированных на внедрение скрытой информации в изображения», представленной на соискание степени

доктора философии PhD по образовательной программе 8D06254 –«Радиотехника, электроника и телекоммуникации»

**Общая характеристика работы.**

Настоящая работа направлена на обеспечение безопасности пользователей телекоммуникационных сети и, в частности, заключается в создании новых и совершенствовании существующих средств защиты информации в глобальной сети Интернет. В диссертации исследуются методы организации тайного канала связи методами стеганографии.

Так в обычный файл, например, фотографию, может быть встроена скрытая информация, которая будет доступна только получателю. Посторонний не только не сможет получить доступ к сообщению, но даже и заподозрить его существование. В качестве такого файла (контейнера) могут выступать изображения, видео-, аудио- и текстовые файлы.

В отличие от криптографии, где необходима устойчивость шифра к взлому, в стеганографии главным требованием является «скрытность» - низкая вероятность обнаружения факта существования тайного канала связи. Дополнительным требованием может быть устойчивость к искажению контейнера третьим лицом, например, для изображения – это масштабирование, добавление шумов и др.

Существует множество методов и алгоритмов, используемых в стеганографии, большинство из них базируются на методах теории вероятности, математической статистики и статистических свойствах контейнера. Основной принцип внедрения – это внесение малых изменений контейнера так, чтобы они были незаметны для третьих лиц. В то же время любое изменение выполняется в соответствии со скрываемым сообщением.

Некоторые из них ориентированы на скрытие информации в определенных типах изображений, например, в изображениях с высоким разрешением или в видео. Другие методы используют разные способы внедрения информации в изображения, например, изменение цветовых компонентов пикселей или использование маскировки.

Одним из ключевых аспектов в разработке стеганографических алгоритмов является их оценка и анализ. Для этого используются различные критерии качества, такие как устойчивость, объём, незаметность (скрытность) и трудоемкость внедрения. Оценка и анализ позволяют определить эффективность алгоритма и убедиться в том, что он может быть использован для скрытия информации в конкретных практических условиях.

Настоящая диссертационная работа посвящена разработке новых и эффективных методов внедрения и обнаружения скрытых данных в изображениях. Так для внедрения успешно используются методы интерполяции, базирующиеся на кривой Безье. Также был проведен анализ существующих методов внедрения и была показана их уязвимость, что является основанием для их дальнейшего совершенствования.

**Актуальность темы.**

В связи с бурным развитием компьютерной техники резко возрос объем передаваемых данных в сети Интернет. Наиболее популярным контентом интернет-сайтов являются: аудио- и видео файлы, изображения и текст. Особенностью цифрового контента является его почти нулевая стоимость воспроизводства. Действительно скопировать файл не составляет большого труда.

В этой связи возникает ряд проблем. Во-первых, должностные лица, имеющие доступ к персональным данным клиентов (паспорта, номера банковских счетов и телефонов, и др.) способны тайно отправлять по электронной почте за пределы организации посторонним лицам. На черном рынке такая информация ценится и используется как для рассылки рекламы, так и для совершения противоправных действий. Во-вторых, разработанная программа или созданная фотография может использоваться третьим лицом, которое выдает эти объекты интеллектуальной деятельности под своим авторством. В-третьих, файл, проданный конкретному пользователю, может быть нелегально скопирован и продаваться как пиратский контент, нанося прямой финансовый урон изготовителю.

Указанные проблемы имеют решения в области стеганографии. Так современные требования по информационной безопасности предприятия вынуждают создавать системы анализа передаваемого трафика. В дополнение анализируется отправляемая почта. Очевидно, что объем трафика огромный и не может быть проанализирован человеком, но может проводиться автоматическом режиме. Так при обнаружении утечек персональных данных выполняется стегоанализ всей отправлявшейся почты организации для установления нарушителя.

Для подтверждения своего права владения над цифровым контентом производитель встраивает в изображение или программу специальное сообщение – цифровой водяной знак, который содержит, например его ФИО. При необходимости этот ЦВЗ может быть извлечен и продемонстрирован в суде, что позволит установить истинное авторство.

Для противодействия пиратскому копированию стеганография предлагает методы цифровых отпечатков пальцев, которые в отличие от ЦВЗ содержат информацию о конечном потребителе. То есть в каждую продаваемую копию встраивается ЦОП, содержащий ФИО потребителя. Если будет перехвачена пиратская версия файла, то достаточно извлечь прочитать ЦОП, что является во многих западных странах основанием для возбуждения следственных действий в отношении нарушителя.

Очевидно, что злоумышленник знает о всех особенностях и возможностях стеганографии. Естественным образом он будет стараться противодействовать им. Например, он может начать преобразовывать изображение (масштабировать, добавлять шум и др.) в надежде на то, что внедренный ЦВЗ или ЦОП будет искажен или полностью уничтожен. Именно по этой причине возникает острая необходимость создания новых и совершенствование и известных методов внедрения. Анализ существующих алгоритмов позволит выявить потенциальную уязвимость стегосистемы и посодействовать дальнейшей эволюции стеганографических методов.

Основными характеристиками методов внедрения в изображение являются: вероятность обнаружения факта внедрения, объем внедрения (вычисляемый от максимально допустимого объема контейнера). Для стегоанализа применяются классические ошибки первого и второго рода: пропуска внедрения и ложного срабатывания.

Исследование стеганографических алгоритмов является важным направлением в области информационной безопасности телекоммуникационных систем. Разработка новых алгоритмов и их исследование позволяют улучшить качество стеганографических методов, сделать их более надежными и защищенными от различных атак.

В настоящее время проводится множество исследований, по проблемам информационной безопасности. Проводятся ежегодные конференции, с каждым годом растет число публикаций, посвященных данной проблеме. В этом направлении науки работают многие казахстанские, российские, и зарубежные ученые: Г.Б. Абдыкеримова, С.Е. Нысанбаева, Н.А. Капалова, И.В. Нечта, И.Н. Оков, Б.Я. Рябко, И.В. Туринцев, А.Н. Фионов,, Р. Бергмар (R. Bergmar), К. Кашен (C. Cachin), М. Чапман (M. Chapman), Ц. Чень (J. Chen), Дж. Фридрич (J. Fridrich), и др. Автором диссертации был проведен анализ основных отечественных и зарубежных источников за более чем 10 последних лет. Список этих источников отражен в тексте диссертации. Основные работы, с которыми производилось сопоставление результатов диссертации, принадлежат таким специалистам как Ц. Чень (J. Chen), Дж. Ю (Z. Yu), Мерзлякова Е.Ю., Евсютин О.

**Данная диссертационная работа** **направлена** на создание научно-технического задела в области информационно-коммуникационных технологий и на получение новых знаний, позволяющих осуществлять анализ и эффективно работать в области стеганографии с применением интерполяции.

**Целью диссертационной работы** является создание новых и эффективных методов внедрения и обнаружения скрытых данных в изображении. Для достижения этой цели необходимо решить следующие **задачи**:

1. Изучение существующих методов стеганографии и анализ их преимуществ и недостатков. Эта задача включает в себя обзор литературы по теме, изучение основных методов стеганографии и оценку их преимуществ и недостатков.
2. Разработка новых стеганографических алгоритмов, ориентированных на внедрение секретной информации в изображения, с учетом современных требований к безопасности и эффективности. Для решения этой задачи необходимо провести теоретический анализ и выбрать оптимальный подход к разработке новых стеганографических алгоритмов, затем реализовать эти алгоритмы и провести их тестирование.
3. Исследование известных алгоритмов на устойчивость к атакам, а также на возможность обнаружения скрытой информации. Для решения этой задачи необходимо провести тестирование разработанных алгоритмов на различных датасетах и оценить их устойчивость к атакам, таким как изменение размера изображения, сжатие, фильтрация и другие. Также необходимо провести анализ возможности обнаружения скрытой информации с помощью стеганализа.
4. Оценка эффективности реализованных алгоритмов по сравнению с существующими методами стеганографии. Для решения этой задачи необходимо провести сравнительный анализ разработанных алгоритмов с существующими методами стеганографии и оценить их эффективность по устойчивости к атакам.
5. Разработка программной реализации новых стеганографических алгоритмов и создание пользовательского интерфейса. Для решения этой задачи необходимо разработать программную реализацию разработанных алгоритмов, которая будет позволять пользователям внедрять секретную информацию в изображения. Также необходимо разработать удобный и интуитивно понятный пользовательский интерфейс для работы с программой.

**Объектом исследования** являются методы сокрытия информации в контейнерах, представляющие собой цифровые изображения, а также методы выявления наличия скрытой в таких контейнерах информации.

**Предмет исследования** являются методы оценки стойкости стеганографических систем, основанные на перестановках элементов пространства сокрытия, различные характеристики стегоконтейнеров.

**Методы исследования** – в процессе проведения исследований были использованы методы стеганографии и алгоритмы сжатия.

**Новизна работы**. Новизна и оригинальность работы заключается в том, что в ней впервые:

* Проведен обзор существующих, актуальных методов встраивания и обнаружения скрытых данных в изображения. В настоящее время нет исследований, анализирующих устойчивость подобных алгоритмов к анализу;
* Проведен стегоанализ методов INMI и базирующихся на кривой Безье, и выявлены их уязвимости.
* Разработан новый метод встраивания секретных сообщении в изображения используя кривую Безье – LIBC5 (по пяти точкам), являющийся устойчивым к лучшим современным алгоритмам стегоанализа;
* Впервые проведен сравнительный анализ алгоритмов внедрения NMI и INMI, в котором выявлена уязвимость обоих алгоритмов к RS анализу.

**Положения, выносимые на защиту**

1. Метод на основе кривой Безье является устойчивым к анализу RS и сопоставим по стойкости и ёмкости со стегосистемой способа перестановок для растровых изображений;
2. Метод INMI и базирующийся на кривой Безье являются уязвимыми к RS и SPAM анализу.
3. Метода внедрения LIBC5 является устойчивым к RS анализу.
4. Для рассматриваемых INMI и базирующийся на кривой увеличение объема встроенной информации повышает вероятность успешного стегоанализа.
5. Методы NMI и INMI уязвимы к RS анализу.

**Научно-практическая значимость работы.**

Принимая во внимание то, что наиболее распространенным типом файлов, передаваемых в сети Интернет, являются картинки, то настоящее исследование ориентировано на внедрение скрытой информации в изображения. Полученные результаты могут быть использованы в системах скрытой передачи данных по каналам связи. Предложенные алгоритмы стегоанализа могут быть реализованы на аппаратном уровне в телекоммуникационном оборудовании. Предложенные методы внедрения сообщений не увеличивают объем передаваемого трафика в сети.

Результаты исследований диссертационной работы включены в учебно -методический комплекс дисциплины «Организация дорожного движения» для студентов специальности 6В11367–«Организация дорожного движения» КазАТК имени М.Тынышпаева и используются при проведении лабораторных занятий.

Имеется акт о внедрении полученных научных результатов диссертационной работы в ТОО «Алматыэлектротранс» (г.Алматы, Казахстан).

**Личный вклад автора** заключается в том, что основные результаты экспериментов были получены соискателем. Постановка задач и обсуждение результатов проводились совместно с научными консультантами.

**В публикациях, выполненных в соавторстве,** вклад автора состоит в анализе источников, постановке эксперимента и представлению результатов.

**Соответствие паспорту образовательной программы РЭТ** Проведенное исследование соответствует области профессиональной деятельности: – средства защиты информации в телекоммуникационных системах. Стеганография исследует методы построения тайных каналов связи на базе существующей Интернет сети.

**Достоверность и обоснованность полученных результатов** подтверждаются наличием публикаций в журналах дальнего зарубежья с импакт-фактором и в изданиях, рекомендованных Комитетом по обеспечению качества в сфере образования и науки МНВО РК, и в трудах международных научных конференции ближнего и дальнего зарубежья. Экспериментальные данные, полученные в процессе выполнения работы хорошо согласуется с данными, полученными на основе нового предложенного метода.

**Апробация диссертационной работы.** Результаты, полученные в диссертационной работе опубликованы, докладывались и обсуждались:

**Публикации с импакт-фактором по базе данных Thomson Reuters или в изданиях, входящих в международную научную базу данных Scopus:**

* **Daiyrbayeva E.,** Yerimbetova A., Nechta I., Merzlyakova E, Toigozhinova A., Turganbayev A. A Study of the Information Embedding Method into Raster Image Based on Interpolation. //J. Imaging. – 2022. –№ 8(288).
* **Daiyrbayeva E.,** Yerimbetova A., Toigozhinova A., Maratov Z., Sambetbayeva M. Learning steganography with a strip transform//6th International Conference on Computer Science and Engineering (UBMK). – Ankara, 2021 –P.209-212.

**Публикации в изданиях, рекомендованных КОКСОНВО РК:**

* **Дайырбаева Э.Н.,** Мурзин Ф.А., Липская М.А. Скрытие информации в изображениях // Вестник КазАТК им. М. Тынышпаева. –Алматы, 2020. – №1 (112). –Б.283-290.
* **Дайырбаева Э.Н.,** Липская М.А., Тойгожинова А.Ж. Суреттерді өңдеуде стрип-әдісті пайданалу жолдары мен нәтижелері // Вестник КазНИТУ. –Алматы, 2020. –№5. –Б. 279-284.
* **Дайырбаева Э.Н.,** Липская М.А., Тойгожинова А.Ж, Нугуманов Ш.Е. Сандық және компьютерлік стеганографиялардың сипаттамалары мен мүмкіншіліктеріне шолу // Вестник КазАТК. –Алматы, 2020. – №3 (114). –Б. 246-252.
* **Дайырбаева Э.Н.,** Еримбетова А.С., Тұрғанбаев А.Ж., Тойгожинова А.Ж., Нурланбек А.Д. Интерполяция арқылы ақпараттарды жасыру жолдарына талдау. //ҚазККА хабаршысы. –Алматы, 2022. – №3. – Б. 376-383.
* Yerimbetova A., **Daiyrbayeva E.,** Cherikbayeva L. Embedding hidden information in images based on bicubic interpolation //Известия НАН РК. Серия «Информатика». –Алматы, 2023. –№ (1). –P. 50-63

**Публикации в сборниках тезисов и докладов:**

* **Daiyrbayeva E.,** Yerimbetova A., Toigozhinova A., Maratov Z., Sambetbayeva M. // Learning steganography with a strip transform. 6th International Conference on Computer Science and Engineering (UBMK). – Ankara, 2021. – P.209-212.
* **Дайырбаева Э.Н**., Еримбетова А.С. Роль метрики в обработке изображений // МНСК-2021 Информационные технологии Материалы 59-й Международной научной студенческой конференции. –Новосибирск, 2021. - С.53
* **Дайырбаева Э.Н.** Использование RS анализа в стеганографии // МНСК-2022 Информационные технологии Материалы 60-ой Международной научной студенческой конференции. – Новосибирск, 2022. – С.9
* **Дайырбаева Э.Н.**, Еримбетова А.С. Исследование и внедрение встраивания скрытой информации в изображения на основе интерполяции // Российская конференция с международным участием Распределенные информационно-вычислительные ресурсы (DICR-2022), сборник трудов Россия. – Новосибирск, 2022. – С. 45-48.

Диссертационная работа частично выполнена в соответствии с планами научно-исследовательской работы (НИР): «Разработка методов и алгоритмов для многомерных данных в задачах обработки изображений и компьютерной лингвистике» 2020-2022 гг., ГФ АР 08857179.

**Публикации.** По материалам диссертационной работы опубликовано 10 работ: 5 в журналах из перечня КОКСОНВО РК для опубликования основных результатов диссертации на соискание ученой степени PhD и 1 статья в журнале дальнего зарубежья с импакт-фактором, входящих в международные информационные ресурсы Web of Science (Clarivate Analitycs, США) и Scopus (Elesiver, Нидерланды); 4 работ в материалах Международных научных конференций.

**Свидетельства о внесении записи в Государственный реестр прав на объекты авторского права.**

**-** Еримбетова А.С., Дайырбаева Э.Н., Маратов Ж.С. Программа для передачи срытых данных с помощью объекта изображения. Авторское свидетельство. № 20614 от 30.09.2021 г.

- Дайырбаева Э.Н., Еримбетова А.С., Маратов Ж.С., Турганбаев А.Ж. Программа встраивания информации в цифровые изображения с применением интерполяции. Авторское свидетельство № 25573 от 28.04. 2022 г.

- Дайырбаева Э.Н., Еримбетова А.С., Турганбаев А.Ж. Программа встраивания информации в цифровые изображения с применением кривой Безье. Авторское свидетельство № 34297 от 04.04. 2023 г.

**Объем и структура диссертации.** Диссертационная работа состоит из введения, 4 разделов, заключения и списка использованных источников из ХХХ наименовании, содержит 120 страниц основного компьютерного текста, включая ХХ рисунков, ХХХ формул и ХХ таблиц.

Во введении раскрыты актуальность, конкретизированы проблемы, связанные с исследуемой темой. Приведены цель и задачи исследования, научная новизна и практическая ценность работы, методы исследования.

**В первой главе** диссертации представлены обзор существующих, актуальных методов встраивания и обнаружения скрытых данных в изображения. Было выявлено, что методы стеганографии имеют широкое применение в области защиты авторских прав и отслеживания траектории распространения цифрового объекта. Применение стегоанализа в области обеспечения безопасности объектов критической телекоммуникационной инфраструктуры в части контроля за передачей конфиденциальных данных.

**Во второй главе** диссертации проведен анализ эффективности методов внедрения скрытых сообщений в изображение: INMI и NMI. Представлено программное обеспечение для внедрения скрытой информации в изображения с использованием известных ранее алгоритмов стеганографии. Приведены результаты по оценке устойчивости рассматриваемых алгоритмов к атакам, использующим изменение цветовой палитры. Также отражены сравнение полученных результатов с другими существующими методами стеганографии.

**В третьей главе** диссертации исследованы существующие методы, базирующиеся на кривой Безье. Были проанализированы преимущества и недостатки кривых Безье по их порядкам. Также был дан предложенный новый метод LIBC5, который был использован в сокрытии данных для создания стегоконтейнера, который содержал секретные данные. Были приведены итоговые сравнительные результаты RS анализа методов INMI и LIBC5.

**В четвертой главе** диссертации представлено полное описание разработанного ПО и схемы её работы. Данное описание поможет будущим исследователям при проведении экспериментов и дальнейшем совершенствовании методов стеганографии.

**В заключении** отражены основные результаты и выводы диссертационной работы.