**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.** Диссертационная работа посвящена разработке эффективных методов внедрения и обнаружения скрытых данных в изображениях.

Разработка стеганографических алгоритмов – это процесс создания методов, позволяющих организовывать тайный канал связи. В качестве среды передачи используют, например, файлы, передаваемые по сети Интернет. Требуется, чтобы сам факт существования такого канала был трудно обнаружим. Одним из требований к подобным алгоритмам часто выдвигают обеспечение устойчивости к искажению обрабатываемого третьим лицом сетевого трафика, например, для изображения это масштабирование, добавление шумов и другие формы обработки изображения.

Существует множество методов и алгоритмов, используемых в стеганографии, которые основаны на различных подходах и принципах. Некоторые из них ориентированы на скрытие информации в определенных типах изображений, например, в изображениях с высоким разрешением или в видеопоследовательностях. 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 тестирование. Для этого используются различные критерии качества, такие как устойчивость, емкость, незаметность (скрытность) и трудоемкость внедрения. Оценка и тестирование позволяют определить эффективность алгоритма и убедиться в том, что он может быть использован для скрытия информации в конкретных практических условиях.

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.

**Актуальность темы.**

Развитие инфокоммуникационных технологий, процессы внедрения новейших телекоммуникационных систем, формирование и развитие современного информационного сообщества определяет важность понятии стеганографии.

Тема разработки и исследования стеганографических алгоритмов, ориентированных на внедрение скрытой информации в изображения, остается актуальной и востребованной в современном информационном мире. С каждым годом объем данных, которые мы создаем и обрабатываем, становится все больше, и возрастает необходимость в защите информации от несанкционированного доступа. Стеганография является одним из инструментов для обеспечения безопасности данных, позволяя скрыть секретную информацию в ненавязчивой форме, такой как изображение.

Существующие стеганографические алгоритмы имеют свои преимущества и недостатки, и постоянно требуют доработок и совершенствований, чтобы сохранять свою эффективность и защищенность от атак. Кроме того, с развитием технологий и появлением новых методов анализа данных необходимо постоянно адаптировать стеганографические алгоритмы к новым условиям и требованиям.

Таким образом, разработка и исследование новых стеганографических алгоритмов, способных эффективно и безопасно встраивать секретную информацию в изображения, является актуальной задачей, которая имеет практическое применение в различных областях, таких как защита данных, криптография, медицина, телекоммуникации и другие.

«Стеганография» – это слово греческого происхождения, которое означает «скрытое письмо», способ передачи или хранения [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) с учётом сохранения в тайне самого факта такой передачи. Слово стеганография делится на две части: стеганография, что означает «секретный или скрытый» (где вы хотите скрыть секретные сообщения), и графика, которая означает “написание” (текст).

Главная цель стеганографии заключается в том, чтобы скрыть сам факт наличия связи с помощью встраивания сообщений в безобидные на вид объекты, которые называют контейнерами. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, звук, текст. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

Для обеспечения безопасности канала связи, передаваемые между двумя абонентами сообщения, преобразуют так, чтобы их перехват третьим лицом был бесполезным. Обычно такие задачи решаются при помощи методов криптографии. В общем случае криптографическое преобразование сообщения происходит с участием некоторого секретного ключа, доступного только отправителю и получателю. Получение исходного сообщения из преобразованного практически невозможна без знания секретного ключа. Соответственно анализ данных, передаваемых по открытому каналу связи, не позволяет третьему лицу свободно прочитать исходное сообщение.

Когда сообщение получено, то проблема его дальнейшей защиты также является актуальной. Так, графический файл, созданный одним лицом, может быть скопирован другим лицом или незначительно изменен и далее неправомерно выдаваться как авторская собственность. Тогда возникает необходимость создавать средства, позволяющие однозначно идентифицировать автора, когда речь идет об авторском праве, или идентифицировать конечного пользователя, когда речь идет о поиске источника нелицензионных копий файла. Подобные средства разрабатываются и исследуются в рамках науки стеганографии. Стеганография изучает методы создания тайного канала связи, посредством встраивания секретных сообщений в цифровые объекты данных, называемые контейнеры. В криптографии доступ к сообщению ограничивается, если неизвестен секретный ключ, а в стеганографии скрывается сам факт существования секретного сообщения.

В сети Интернет передается огромное количество медиа контента. Большая часть этих данных является источником дохода его создателя и рассматривается как объект защиты авторского права. Учитывая легкость и нулевую стоимость воспроизводства (создания копии) любого файла, возникает потребность отслеживать траекторию его пути (от создателя до конечного потребителя, в том числе нелицензионного). Одним из самых эффективных решений данной проблемы является применение методов стеганографии, которые используют секретные сообщения, встраиваемые в файл. Такие сообщения могут либо идентифицировать автора (цифровые водяные знаки), либо конечного потребителя (цифровой отпечаток пальца).

В научных публикациях встречаются работы, направленные на создание новых методов внедрения и на создание новых методов обнаружения (стегоанализа). Последние используются для выявления фактов утечки информации, например, через служебную переписку. Таким образом, возникает острая необходимость анализа существующих методов внедрения и создания новых и эффективных методов внедрения скрытых сообщений.

Учитывая, то наиболее распространенным типом файлов, передаваемом в сети Интернет, является картинки, то в настоящее исследование ориентированного на внедрение скрытой информации в изображения. Так один из современных подходов стеганографии базируется на методах интерполяции. В частности, исследуется применение методов интерполяции для внедрения сообщения, которая, в некотором смысле, является дискретным аналогом голограммы, и обычно применяется для восстановления сигналов и изображений, подвергшихся воздействиям и приведшим к большой потере информации.

В настоящее время проводится множество исследований, по проблемам информационной безопасности. С каждым годом растет число публикаций, посвященных методам стеганографии и стегоанализа. В этом направлении науки работают многие российские и зарубежные ученые: И.Н. Оков, Б.Я. Рябко, И.В. Туринцев, А.Н. Фионов, И.В. Нечта, 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 разработанных 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 разработанных 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 таким критериям, как скорость внедрения, скрытность информации, устойчивость к атакам и другие.
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.
6. Проведение экспериментальных исследований и анализ полученных результатов

**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.

**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 представлен…

**Во второй главе** диссертации….

**В третьей главе** диссертации…

**В четвертой главе** диссертации …

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