МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

НУКУССКИЙ ФИЛИАЛ ТАШКЕНТСКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРЕЗМИЙ

ФАКУЛЬТЕТ КОМПЬЮТЕРННЫЙ ИНЖИНИРИНГ
КАФЕДРА ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Направления компьютерный инжиниринг

Допустить к защите
Заведующий кафедрой
Туреniязова А.
2019 г. «___»_____

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: «Обеспечение безопасности передачи информации с использованием стенографических методов защиты.»

Выпускник: **Жусипбаев Ж**

Научный руководитель: **Туреniязова А.**

НУКУС 2019

Содержание

Введение

В настоящее время стеганографические системы активно используются для решения следующих основных задач:

- защита авторских прав встраиванием водяных знаков;
- защита конфиденциальной информации от несанкционированного доступа;
- преодоление систем мониторинга и управления сетевыми ресурсами;
- камуфлирование программного обеспечения.

В рамках компьютерной стеганографии рассматриваются вопросы, связанные с сокрытием информации, которая хранится на носителях или передается по сетям телекоммуникаций, с организацией скрытых каналов в компьютерных системах и сетях, а также с технологиями цифровых водяных знаков и отпечатка пальца

Для защиты авторских прав и скрытой передачи используются робастные методы стеганографии, в то время как «хрупкие» - для защиты от несанкционированного доступа к информации или нарушения целостности.

Типичная схема передачи скрытой информации показана на рисунке 1.

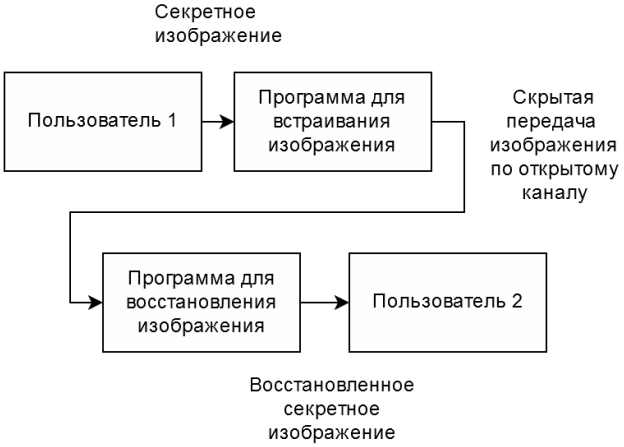

Рис. 1. Схема скрытой передачи информации

Секретное изображение встраивается в открытое,затем передается по

открытому каналу. На принимающей стороне пользователь, используя программу для извлечения скрытой информации, получает из открытого изображения – секретное.

Иногда данную схему дополняют криптографическими методами для шифрования передаваемой секретной информации.

Целью данной работы заключается в безопасной передачи информации путем стенографическим методом защиты а именно скрытие информации (файла) в изображении

Для достижения этой цели были сформулированы следующие задачи:

* Обзор и анализ существующих решений.

* Выбор методов разработки программных (программных) приложений.

* Выберите инструменты и программное обеспечение.

* Разработка структуры приложения.

* Разработка прикладного программного обеспечения.

* Протестируйте приложение.

Объектом исследования является обеспечения безопасной передачи информации

Предметом исследования является стенографический метод защиты информации

В дипломной работе использованы такие методы исследования, как: анализ литературы (с целью поиска необходимого материала для выявление преимуществ и недостатков стенографической метода)

В процессе написания дипломной работы были рассмотрены существующие онлайн-курсы по безопасной передачи информации

Структура дипломной работы обусловлена предметом, целью и задачами исследования. Работа состоит из введения, четырёх глав и заключения.

Глава 1. Существующие решения

1.1 Общая характеристика объектов защиты информационной деятельности и обеспечения ИБ

К объектам ИБ относятся:

информационные ресурсы, независимо от форм хранения, содержащие данные, составляющие государственную тайну и другие конфиденциальные сведения;

информационные системы различных классов и разного назначения (библиотеки, архивы, базы и банки данных, средства теледоступа, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации);

информационная инфраструктура и ее элементы; центры обработки и анализа информации; каналы информационного обмена и телекоммуникации; механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе сами системы и средства защиты процессов переработки информации.

Из перечисленного видно, что многие, если не все информационные системы, являющиеся объектами ИБ, одновременно являются организационными, организационно-техническими или техническими системами.

Объектом защиты процессов переработки информации является компьютерная система или автоматизированная система обработки данных (АСОД), функционирующая на предприятии. В работах, посвященных защите процессов переработки информации в автоматизированных системах, используется термин «автоматизированная система обработки данных», который обычно заменяется термином «компьютерная система».

Компьютерная система — это комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.

Понятие «компьютерная система» охватывает следующие системы:

- ЭВМ всех классов и назначений;
- вычислительные комплексы и системы;
- вычислительные сети (локальные, региональные и глобальные).

Предметом защиты в КС являются процессы переработки информации. Материальной основой существования информации в КС являются электронные и электромеханические устройства (подсистемы), а также машинные носители. С помощью устройств ввода или систем передачи данных (СПД) информация попадает в КС. В системе информация хранится в запоминающих устройствах (ЗУ) различных уровней, преобразуется (обрабатывается) процессорами (ПЦ) и выводится из системы с помощью устройств вывода или СПД. В качестве машинных носителей используются бумага, магнитные ленты, диски различных типов. Большинство типов машинных носителей информации являются съемными, т.е. могут сниматься с устройств и использоваться (бумага) или храниться (ленты, диски, бумага) отдельно от устройств.

При решении проблемы защиты процессов переработки информации в КС необходимо учитывать также человеческий фактор системы. Обслуживающий персонал и пользователи могут быть как объектом, так и источником несанкционированного воздействия на информацию.

Понятие «объект защиты» чаще трактуется в более широком смысле. Для сосредоточенных КС или элементов распределенных систем понятие «объект» включает в себя не только информационные ресурсы, аппаратные и программные средства, обслуживающий персонал, пользователей, но и

инженерно-технические сооружения: помещения, здания и даже прилегающую к зданиям территорию.

В основу системы классификации АС положены следующие характеристики объектов и субъектов защиты, а также способов их взаимодействия:

- информационные, определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможные последствия неправильного функционирования АС из-за искажения (потери) информации;
- организационные, определяющие полномочия пользователей;
- технологические, определяющие условия обработки информации, например, способ обработки (автономный, мультипрограммный и т.д.), время циркуляции (транзит, хранение и т.д.), вид АС (автономная, сеть, стационарная, подвижная и т.д.).

Одними из основных понятий теории защиты информации являются понятия «безопасность процессов переработки информации в КС» и «защищенные КС».

Безопасность процессов переработки информации в КС — это такое состояние всех компонентов КС, при котором обеспечивается защита процессов переработки информации от возможных угроз на требуемом уровне. Компьютерные системы, в которых обеспечивается безопасность процессов переработки информации, называются защищенными.

ИБ достигается проведением руководством соответствующего уровня политики информационной безопасности. Основным документом, на основе которого проводится такая политика, является программа ИБ. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомством, организацией. В

документе приводятся цели политики ИБ и основные направления решения задач защиты информации в КС. Так же в программах информационной безопасности содержатся общие требования и принципы построения систем защиты информации в КС.

Под системой защиты процессов переработки информации в КС понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность этих процессов в КС от несанкционированного доступа в соответствии с принятой политикой безопасности.

Несанкционированный доступ к информации это преднамеренное, противоправное овладение конфиденциальной информацией лицами, не имеющих права доступа к охраняемым сведениям.

Современные автоматизированные информационные технологии, применяемые при управлении различных сфер деятельности предприятий и организаций, базируются на применении КС широкого спектра назначений — от локальных до глобальных, но все они, с точки зрения обеспечения информационных взаимодействий различных объектов и субъектов, обладают следующими основными признаками ИБ:

- наличие информации различной степени конфиденциальности;
- необходимость криптографической защиты процессов пользования информацией различной степени конфиденциальности при передаче данных;
- иерархичность полномочий субъектов доступа и программ к автоматизированному рабочему месту (АРМ), файл-серверам, каналам связи и информации системы; необходимость оперативного изменения этих полномочий;

- организация обработки информации в диалоговом режиме, режиме разделения времени между пользователями и режиме реального времени;
- обязательное управление потоками информации, как в локальных сетях, так и при их передаче по каналам связи на далекие расстояния;
- необходимость регистрации и учета попыток несанкционированного доступа, событий в системе и документов, выводимых на печать;
- обязательное обеспечение целостности программного обеспечения и информации в АИТ;
- наличие средств восстановления системы защиты процессов переработки информации;
- обязательный учет магнитных носителей;
- наличие физической охраны средств вычислительной техники и магнитных носителей.

Первой удачной попыткой стандартизации практических аспектов безопасности стал британский стандарт BS 7799 “Практические правила управления информационной безопасностью”, изданный в 1995 году, в котором обобщен опыт обеспечения режима информационной безопасности в информационных системах разного профиля. Впоследствии было опубликовано несколько аналогичных документов: стандарты различных организаций и ведомств, например, германский стандарт BSI. Содержание этих документов в основном относится к этапу анализа рисков, на котором определяются угрозы безопасности и уязвимости информационных ресурсов, уточняются требования к режиму ИБ.

Несмотря на существенную разницу в методологии обеспечения базового и повышенного уровней безопасности, можно говорить о единой концепции ИБ

1.2 Механизм выработки детальных предложений по формированию политики и построению системы информационной безопасности. Обобщенная модель способов несанкционированного доступа к источникам конфиденциальной информации

Организационные мероприятия и процедуры, используемые для решения проблемы безопасности переработки информации, решаются на всех этапах проектирования и в процессе эксплуатации АИТ.

Существенное значение при проектировании придается анализу риска и потерь. Анализ риска и потерь производится исходя из непосредственных целей и задач по защите информации.

Задачами защиты информации являются определение того, что следует защищать, от чего/кого защищать и как это делать. Необходимо рассмотреть все возможные риски и ранжировать их в зависимости от потенциального размера ущерба. Ранги меняются в зависимости от складывающейся ситуации.

Для построения надежной системы защиты необходимо:

- выявить все возможные угрозы безопасности информации;
- оценить последствия их проявления;
- определить необходимые меры и средства защиты с учетом:

- требований нормативных документов;
- экономической целесообразности;
- совместимости и бесконфликтности с используемым ПО;

- оценить эффективность выбранных мер и средств защиты.

Под угрозой (риском) следует понимать реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации в информационной

системе, а также к прямым материальным убыткам за счет воздействия на материальные ресурсы.

Непосредственными целями защиты информации являются обеспечение:

- конфиденциальности (засекреченная информация должна быть доступна только тому, кому она предназначена);
- целостности (информация, на основе которой принимаются решения, должна быть достоверной и полной, защищенной от возможных непреднамеренных и злоумышленных искажений);
- готовности (информация и соответствующие службы автоматизации должны быть доступны и в случае необходимости готовы к обслуживанию).

Одной из важнейших задач в рамках защиты информации наряду с обеспечением конфиденциальности является обеспечение ее целостности. Часто забывается, что нарушение целостности может произойти не только вследствие преднамеренных действий, но и следующих причин:

- сбоев оборудования, ведущих к потере или искажению информации;
- физических воздействий, в том числе в результате стихийных бедствий;
- ошибок в программном обеспечении (системном или прикладном).

Среди организационных мероприятий по обеспечению безопасности переработки информации важное место занимает охрана объекта, на котором расположена защищаемая АИТ (территория здания, помещения, хранилища информационных носителей). При этом устанавливаются соответствующие посты охраны, технические средства, предотвращающие или существенно затрудняющие хищение средств вычислительной техники, информационных носителей, а также исключающие несанкционированный доступ к АИТ и линиям связи.

Функционирование системы защиты переработки информации от несанкционированного доступа как комплекса программно-технических средств и организационных (процедурных) решений предусматривает:

- учет, хранение и выдачу пользователям информационных носителей, паролей, ключей;
- ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа);
- оперативный контроль за функционированием систем защиты секретной информации;
- контроль соответствия общесистемной программной среды эталону;
- приемку включаемых в АИТ новых программных средств;
- контроль за ходом технологического процесса обработки финансово-кредитной информации путем регистрации анализа действий пользователей;
- сигнализацию опасных событий и т.д.

Системы защиты процессов переработки информации в АИТ основываются на следующих принципах:

- комплексный подход к построению системы защиты при ведущей роли организационных мероприятий, означающий оптимальное сочетание программно-аппаратных средств и организационных мер защиты и подтвержденный практикой создания отечественных и зарубежных систем защиты;
- разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки, т.е. предоставление пользователям минимума строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автоматизированной обработки доступной им конфиденциальной информации;

- полнота контроля и регистрации попыток несанкционированного доступа, т. е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в АИТ без ее предварительной регистрации;
- обеспечение надежности системы защиты, т.е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала;
- обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты;
- «прозрачность» системы защиты процессов переработки информации для общего, прикладного программного обеспечения и пользователей АИТ;
- экономическая целесообразность использования системы защиты, выражающаяся в том, что стоимость разработки и эксплуатации систем защиты обработки информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации АИТ без системы защиты.

Методы и средства обеспечения безопасности процессов переработки информации могут быть формальными и неформальными.

Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом — метод защиты процессов переработки информации регулированием использования всех ресурсов компьютерной

информационной системы.

Мероприятия по защите информации должны исключать:

- выход излучений электромагнитного и акустического полей, а также наводок в сетях питания, кабельных линиях, заземлении, радио- и телефонных сетях за пределы контролируемой зоны;
- доступ в помещение, где осуществляется обработка информации, а также визуально-оптические возможности съема информации;
- работу специальных устройств ведения разведки, которые могут находиться в строительных конструкциях помещений и предметах их интерьера, а также внутри самого помещения или непосредственно в средствах обработки и передачи информации;
- перехват информации из каналов передачи данных;
- несанкционированный доступ к информационным ресурсам;
- воздействие излучений, приводящих к разрушению информации.

Дальнейшими этапами, вне зависимости от размеров организации и специфики ее информационной системы, в том или ином виде должны быть:

- определение границ управления информационной безопасностью объекта;
- разработка сценария действий по нарушению информационной безопасности
- ранжирование угроз и выбор контрмер, обеспечивающих информационную безопасность;
- проверка системы защиты информации.

Исходя из того, что речь идет о безопасности информационных систем, именно с их анализа необходимо начинать разработку системы защиты информации.

Информационная система — это организационно - упорядоченная совокупность информационных ресурсов, технических средств, технологий, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователей. Важнейшим компонентом информационных систем являются люди – основной источник компьютерных нарушений.

С точки зрения степени участия предприятия и конкурентов в информационном процессе с противоположными интересами можно рассматривать внутренние и внешние факторы, которые могут привести к утрате охраняемых сведений.

Внутренние факторы или действия по тем или иным причинам или условиям инициируются персоналом предприятия, внешние — конкурентами, что обусловлено активными действиями, направленными на добывание коммерческих секретов.

К таким действиям относятся:

- разглашение конфиденциальной информации ее обладателем;
- утечка информации по различным, главным образом техническим, каналам;
- несанкционированный доступ к конфиденциальной информации различными способами.

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена по службе или стала известна в процессе работы.

Несанкционированный доступ — совокупность приемов и порядок действий с целью получения (добывания) охраняемых сведений незаконным, противоправным путем.

Злоумышленник преследует три цели, осуществляя несанкционированный доступ к источникам конфиденциальной информации:

— получить необходимую информацию в требуемом для конкурентной борьбы объеме и ассортименте;

— иметь возможность вносить изменения в информационные потоки конкурента в соответствии со своими интересами;

— нанести ущерб конкуренту путем уничтожения материальных и информационных ценностей.

От целей зависит как выбор способов действий, так и количественный и качественный состав привлекаемых сил и средств посягательства на чужие секреты.

Полный объем сведений о деятельности конкурента не может быть получен только каким-нибудь одним из возможных способов доступа к информации.

Даже беглый обзор позволяет заключить, что к определенным источникам применяются и определенные способы. Как разнообразны источники, так и разнообразны способы несанкционированного доступа к ним. Имея формальный набор источников и способов НСД к ним можно построить формальную модель взаимосвязи источников и способов на качественном уровне с определенной степенью условности. Такую модель можно было бы назвать обобщенной моделью способов несанкционированного доступа к источникам конфиденциальной информации.

Статистика утверждает, что в криминальной практике несанкционированный доступ осуществляется посредством использования

тех или иных технических средств, которые составляют 47% от общего их числа. Это лишний раз подтверждает опасность технических каналов утечки информации в практике ведения предпринимательской деятельности. Однако не отстает и человеческий фактор – 43%. Такая статистика приводит к необходимости рассмотрения социально-психологических факторов при построении модели нарушителя.

Целью определения границ управления информационной безопасностью объекта является определение всех возможных «болевых точек» объекта, которые могут доставить неприятности с точки зрения безопасности информационных ресурсов, представляющих для организации определенную ценность.

На этом этапе происходит инвентаризация информационных ресурсов, сбор данных об объекте в целом, информационных потоках, структуре автоматизированной системы автоматизированных рабочих местах, серверах, носителях информации, способах обработки и хранения данных. Определяется система критериев и методология получения оценок по этим критериям. Все это необходимо для последующего анализа уязвимости информационных ресурсов.

Для работ на данном этапе должны быть собраны следующие сведения:

- перечень сведений, составляющих коммерческую или служебную тайну;
- организационно-штатная структура предприятия или организации;
- характеристика и план объекта, размещение средств вычислительной техники и поддерживающей инфраструктуры. На плане объекта указывается порядок расположения административных зданий, производственных и вспомогательных помещений, различных строений, площадок, складов, стендов и подъездных путей с учетом

масштаба изображения. Дополнительно на плане указываются структура и состав автоматизированной системы, помещения, в которых имеются технические средства обработки критичной информации с учетом их расположения. Указываются также контуры вероятного установления информационного контакта с источником излучений по видам технических средств наблюдения с учетом условий среды, по времени и месту;

- перечень и характеристика используемых автоматизированных рабочих мест, серверов, носителей информации;
- описание информационных потоков, технология обработки информации и решаемые задачи, порядок хранения информации. Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов;
- используемые средства связи (цифровая, голосовая и т.д.).

Знание элементов системы дает возможность выделить критичные ресурсы и определить степень детализации будущего обследования. Инвентаризация информационных ресурсов должна производиться исходя из последующего анализа их уязвимости. Чем качественнее будут проведены работы на этом этапе, тем выше будет достоверность оценок на следующем.

В результате должен быть составлен документ, в котором зафиксированы границы системы, перечислены ресурсы, подлежащие защите, дана система критериев для оценки их ценности. В идеале такой документ должен включать информационно-логическую модель объекта, иллюстрирующую технологию обработки критичной информации с выделением вероятных точек уязвимости, по каждой из которых необходимо иметь полную характеристику. Такая модель является базой, а ее полнота залогом успеха на следующем этапе построения системы информационной безопасности.

1.3 Типы стеганографических методов

Стеганографические методы можно разделить на 2 типа [1]:

- Частотные (frequency domain)
- Пространственные (spatial domain) Методы также могут специализироваться на встраивании в определенные форматы файлов:
- Изображения
- Текст
- Аудио/Видео
- Протокол

Частотные методы основываются на скрытии информации при помощи преобразований. Они считаются более надежными по сравнению с пространственными.

Симпатические чернила

Одним из наиболее распространённых методов **классической стеганографии** является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определённых условиях (нагрев, освещение, химический проявитель и т. д.) Изобретённые ещё в I веке н. э. Филоном Александрийским они продолжали использоваться как в средневековье, так и в новейшее время, например, в письмах русских революционеров из тюрем. В советское время школьники на уроках литературы изучали рассказ, как Владимир Ленин писал молоком на бумаге между строк (см. «Рассказы о Ленине»). Строки, написанные молоком, становились видимыми при нагреве над пламенем свечи.

Существуют также чернила с химически нестабильным пигментом. Написанное этими чернилами выглядит как написанное обычной ручкой, но через определённое время нестабильный пигмент разлагается, и от текста не

остаётся и следа. Хотя при использовании обычной шариковой ручки текст можно восстановить по деформации бумаги, этот недостаток можно устранить с помощью мягкого пишущего узла, наподобие фломастера.

Другие стеганографические методы

Во время Второй мировой войны активно использовались **микроточки** — микроскопические фотоснимки, вклеиваемые в текст писем.

Также существует ряд альтернативных методов сокрытия информации:[

- запись на боковой стороне колоды карт, расположенных в условленном порядке;
- запись внутри варёного яйца;
- «жаргонные шифры», где слова имеют другое обусловленное значение;
- трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы;
- геометрическая форма — метод, в котором отправитель старается скрыть ценную информацию, поместив ее в сообщение так, чтобы важные слова расположились в нужных местах или в узлах пересечения геометрического рисунка;
- семаграммы — секретные сообщения, в которых в качестве шифра используются различные знаки, за исключением букв и цифр;
- узелки на нитках и т. д.

В настоящее время под **стеганографией** чаще всего понимают скрытие информации в текстовых, графических либо аудиофайлах путём использования специального программного обеспечения.

Компьютерная стеганография

Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры — стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганографияи т. д. Приведём некоторые примеры:

- Использование зарезервированных полей компьютерных форматов файлов — суть метода состоит в том, что часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных. Недостатком этого метода является низкая степень скрытности и малый объём передаваемой информации.
- Метод скрытия информации в неиспользуемых местах гибких дисков — при использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку. Недостатки: маленькая производительность, передача небольших по объёму сообщений.
- Метод использования особых свойств полей форматов, которые не отображаются на экране — этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание чёрным шрифтом на чёрном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.
- Использование особенностей файловых систем — при хранении на жёстком диске файл всегда (не считая некоторых ФС, например, ReiserFS) занимает целое число кластеров (минимальных адресуемых объёмов информации). К примеру, в ранее широко используемой файловой системе FAT32 (использовалась в Windows98/Me/2000) стандартный размер кластера — 4 КБ. Соответственно для хранения 1 КБ информации на диске выделяется 4 КБ памяти, из которых 1 КБ нужен для хранения сохраняемого файла, а остальные 3 ни на что не используются — соответственно их можно

использовать для хранения информации. Недостаток данного метода: лёгкость обнаружения.

1.4 Математические методы преобразования сигналов

Для задачи обработки изображений используются различные двумерные преобразования. В

стеганографии некоторые из них используются для частотных методов.

Преобразование Карунена-Лоэва

Все преобразования, кроме KLT (преобразование Карунена-Лоэва), являются преобразованиями с постоянным базисом. А в KLT вычисляется самый оптимальный базис для нескольких векторов. Он вычисляется таким образом, что первые коэффициенты дадут наименьшую среднеквадратичную погрешность суммарно для всех векторов. Но этот метод имеет свои недостатки - появляется проблема хранения оптимального базиса, операция его вычисления достаточно трудоемкая. Дискретное косинусное преобразование (DCT или ДКП) проигрывает лишь немного, и к тому же у DCT существуют алгоритмы быстрого преобразования.

Дискретное преобразование Фурье

DFT (Discrete Fourier Transform) - дискретное преобразование Фурье. Это ортогональное преобразование с комплексным базисом.

Формула для преобразования в комплексном

виде

$$\mathcal{F}(\omega_x, \omega_y) = \int_{-\infty}^{\infty}\int F(x, y) \exp\{-i(\omega_x x + \omega_y y)\}\, dx\, dy,$$

(1)

Обратное преобразование:

$$F(x,\ y) = (1/4\pi^2) \int_{-\infty}^{\infty}\int \mathcal{F}(\omega_x,\ \omega_y) \exp\{i(\omega_x x + \omega_y y)\}\, d\omega_x\, d\omega_y.$$

(2)

Дискретное синусное преобразование

Дискретное синусное преобразование - Discrete Sine Transform (DST) - это преобразование с базисом синус, в отличии от DCT. Данные преобразования не представляют интереса, так как и целые, и половинки периодов синусов близки к нулю на границах.

Дискретное косинусное преобразование

Дискретное косинусное преобразование - одно из ортогональных преобразований. Вариант косинусного преобразования для вектора действительных чисел. Применяется в алгоритмах сжатия информации с потерями, например, MPEG и JPEG. Также широко применяется в стеганографических методах. Это преобразование тесно связано с дискретным преобразованием Фурье и является гомоморфизмом его векторного пространства.

Математически преобразование можно осуществить умножением вектора на матрицу преобразования. При этом матрица обратного преобразования с точностью до множителя равна транспонированной матрице. В математике матрицы выбирают так, чтобы преобразование было ортонормированным, а постоянный множитель равен единице. В компьютерных приложениях это не всегда так.

$$F(u,v)=C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y)\cos[\frac{\pi(2x+1)u}{2N}]\cos[\frac{\pi(2y+1)v}{2N}] \quad (3)$$

$$where\ u=0,1,\dots N-1 \quad v=0,1,\dots M-1 \quad (4)$$

$$C(u),C(v)=\sqrt{\frac{1}{N}}\ when\ u,v=0 \quad C(u),C(v)=\sqrt{\frac{2}{N}}\ when\ u,v\neq 0 \quad (5)$$

Преобразование Хаара

В традиционной постановке вейвлет - преобразование в

базисе Хаара заключается в линейном преобразовании вектора a четной размерности 2M в другой вектор b такой же размерности согласно следующим соотношениям [2]

$$b_k = (a_{2k} + a_{2k+1})/2,\ b_{k+M} = (a_{2k} - a_{2k+1})/2,\ k = 0, M-1.$$

(6)

Для обратного преобразования:

$$a_{2k} = b_k + b_{k+M},\ a_{2k+1} = b_k - b_{k+M},\ k = 0,\ M-1.$$

(7)

Преобразование широко известно по методу сжатия Jpeg 2000 и до сих пор обширно используется в различных задачах обработки изображений и сигналов, в том числе в задачах стеганографии.

Преобразование Адамара

Данное преобразование также было использовано в методе, описанном в статье Бхаттачариа С., Мондал С., Саньйал Г. A Robust Image Steganography using Hadamard Transform [3] и в статье В.А. Батура, А.Ю. Тропченко Эффективность алгоритмов маркирования цифровых изображений в частотной области на основе дискретного преобразования Адамара [4]. Преобразование Адамара более точное, высокочастотные коэффициенты менее чувствительны к искажениям за счет прямоугольного базиса (функция Уолша). Базис дискретного косинусного преобразования – вещественная функция, он дает ошибку округления. За счет округления базис получается не ортогональным. По результатам проверки приведенные особенности ДКП сильно повлияли на качество восстановления информации.

1.5 Стеганографические методы

Простейший метод наименьшего значащего бита (Least Significant Bit - LSB), описанный в статье Чампакмала Б., Падмини К. и Радхика Д.[6], основан

на подмене младших незначащих бит изображения. Метод был успешно атакован статистически, в соответствии с изложенным в работе Фридриха Д., Гольян М., и Ду Р. [7].

Также существуют его модификации, где встраивание происходит в коэффициенты дискретного косинусного преобразования (ДКП) [9; 10]. Один из

таких алгоритмов Jsteg (улучшения данного алгоритма

— f3, f4 и f5) был изложен в работе Вестфолда А. [11]. Здесь встраивание происходит в DC коэффициент преобразования методом LSB. Метод используется только для формата Jpeg.

Метод подмены коэффициентов ДКП, описанный в работе Шейзи Х., Месгариан Д., Рахмани М. «Steganography: Dct Coefficient Replacement Method and Compare With Jsteg Algorithm»[9], для встраивания использует средние частоты в отличие от Jsteg.

Метод Куттера – Джордана – Боссена, поясненный в работе Фомина Д.В. [12], состоит в том, что бит сообщения, закодированного данным методом, встраивается в канал синего цвета путем модификации яркости выбранного пикселя в соответствии с формулой ниже.

$$B^*_{x,y} = \begin{cases} B_{x,y} + \lambda Y_{x,y}, \text{при } m_i = 1 \\ B_{x,y} - \lambda Y_{x,y}, \text{при } m_i = 0 \end{cases}, \quad (8)$$

где $\lambda = 0.1$, $Y_{x,y} = 0.3*R_{x,y}+0.59*G_{x,y}+0.11*B_{x,y}$.

Извлечение происходит по следующей формуле:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma}(B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma} \quad (9)$$

Главная проблема данного метода – вероятностный характер извлечения яркости цвета.

Алгоритм Коха-Жао для встраивания информации использует частотную область контейнера и заключается в относительной замене величин коэффициентов ДКП. Каждый блок пригоден для записи одного бита информации. Выбирается 2 коэффициента ДКП, и бит информации кодируется знаками этих коэффициентов [8].

Также существует метод, построенный на базе преобразования Адамара, который представлен в статье Бхаттачариа С., Мондал С., Саньйал Г. A Robust Image Steganography using Hadamard Transform [3]. Данный метод для встраивания использует Pixel Mapping Method (PMM), который изменяет порядок встраивания бит секретного сообщения . Встраивание происходит изменением свойств исходного пикселя, таких как количество единиц и четность.

На рисунке 3 приведена таблица встраивания 2-х

PAIR OF MSG BIT	PIXEL INTENSITY VALUE	NO OF ONES (BIN)
01	EVEN	ODD
10	ODD	EVEN
00	EVEN	EVEN
11	ODD	ODD

Рис. 3. Таблица встраивания методом PMM

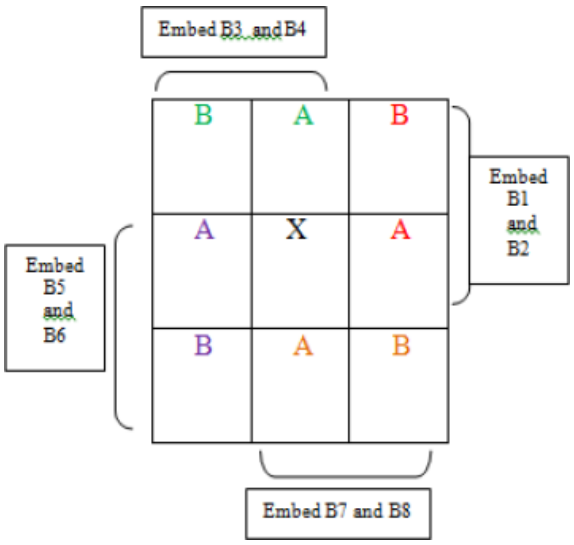

Рис.4. Порядок встраивания методом PMM

Один бит встраивается в четность количества единиц в числе, другой бит встраивается в четность числа. Т.е. один из битов встраивается в наименьший значащий бит, который отвечает за четность.

На рисунке 4 показан порядок встраивания битов сообщения в окно 3x3.

Другая идея данного метода – использование преобразования Адамара – перспективная, она позволяет обойти большинство методов распознавания встроенной информации.

В статье В.А. Батура и А.Ю. Тропченко «Эффективность алгоритмов маркирования цифровых изображений в частотной области на основе дискретного преобразования Адамара» [4] также было подмечено, что преобразование Адамара уменьшает ошибку встраивания.

В последнее время получили методы, основанные на Exploiting Modification Direction (EMD) [9]. Один из новейших методов – Diamond Encoding (DEMD) и его модификации были описаны в статье Вэн-Чунг Куо A Formula Diamond Encoding Data Hiding Scheme . Секретное сообщение данным методом встраивается в остаток от деления на некоторое число, зависящее от параметра встраивания.

Существуют решения и на основе Wavelet преобразований. К примеру,

совместного использования с преобразованием таких методов, как LSB, Wavelet Fusion Metod (комбинирование высокочастотных коэффициентов веевлет преобразования секретного сообщения и контейнера), описанных в статье С. Кумара И С.К. Мутто A Comparative Study of Image Steganography In Wawelet Domain .

1.6 Методы оценки качества изображений

В данной главе приведены некоторые критерии оценки качества изображений, использованные в данной работе.

Абсолютное отклонение от медианы

Медианное абсолютное отклонение используется вместо среднего отклонения, когда крайние значения из области отклонений должны оказывать меньшее влияние на величину отклонения. Используется оно в силу того, что медиана затрагивается крайними значениями области отклонений в меньшей степени, чем среднее.

(10) $$\mathrm{MAD} = \mathrm{median}(\ |X_i - \mathrm{median}(X)|\ ),$$

Среднее квадратичное отклонение

Данный показатель (RMSE – root-mean-squared- error) вычисляется по формуле ниже.

$$RMSE = \sqrt{\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}|I(i,j) - K(i,j)|^2}$$

(11)

По этому показателю качества можно определить разброс ошибки в изображении.

Также распространен критерий (MSE – mean- squared-error). Разница

лишь в отсутствии корня в формуле.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

(12)

Пиковое отношение сигнала к шуму

Пиковое отношение сигнала к шуму (Peak signal- to-noise ratio) может быть определено через среднее квадратичное отклонение - MSE:

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

(13)

Или через RMSE

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{RMSE^2}\right) = 20\log_{10}\left(\frac{MAX_I}{RMSE}\right)$$

(14)

По этому параметру можно определить уровень искажения изображения.

1.7 Коэффициент корреляции (Пирсона)

Данный критерий позволяет определить схожесть двух изображений и вычисляется по следующей формуле:

$$\mathbf{r}_{XY} = \frac{\mathbf{cov}_{XY}}{\sigma_X \sigma_Y} = \frac{\sum(X - \bar{X})(Y - \bar{Y})}{\sqrt{\sum(X - \bar{X})^2}\sqrt{\sum(Y - \bar{Y})^2}}.$$

(15)

Для оценки качества можно воспользоваться таблицей Чеддока, которая позволяет классифицировать силу связи.

Таблица 1. Таблица Чеддока

Величина коэффициента корреляции	Оценка силы связи
0,1 – 0,3	Слабая
0,3 – 0,5	Умеренная
0,5 – 0,7	Заметная
0,7 – 0,9	Высокая
0,9 – 0,99	Весьма высокая

1.8 Выводы по главе

В главе были освещены основные преобразования и стеганографические методы, а также основные частотные преобразования. Некоторые из них используются в стеганографии. В нескольких статьях было подмечено, что преобразование Адамара имеет хороший потенциал для стеганографии в виду помехоустойчивости.

Один из новейших стеганографических методов

– DEMD, на котором построена серия модификаций, показался интересным. Он гибкий, устойчив к статистическим атакам и имеет хорошую устойчивость к помехам.

Глава 2. Аналитическая часть

2.1Выбор основного инструментария

Выбором языка реализации пал на Python. Он был обусловлен большим количеством научных библиотек, которые позволяют работать с изображениями, сигналами, частотной областью, графиками.

В качестве основных библиотек использовались:

- numpy
- scipy
- fht
- matplotlib
- pillow
- PyWavelets

Данный набор библиотек использовался не только для прототипирования и исследования, а также для основной реализации. Все представленные в работе графики и исследования были сделаны при помощи данных инструментов.

NumPy - это библиотека с открытым исходным кодом для языка программирования Python. Она обладает поддержкой многомерных массивов (включая матрицы) и высокоуровневых математических функций, предназначенных для работы с многомерными массивами.

SciPy - библиотека для языка программирования Python с открытым исходным кодом, предназначенная для выполнения научных и инженерных расчётов. Данная библиотека включает в себя обширный функционал для обработки сигналов, изображений. Также в ней содержится библиотека для статистических расчетов.

Fht – библиотека для быстрого преобразования Адамара.

PyWavelets – библиотека, позволяющая использовать wavelet преобразования.

Matplotlib - библиотека на языке программирования Python для визуализации данных двумерной (2D) графикой (3D графика также поддерживается).

Pillow - библиотека языка, предназначенная для работы с растровой графикой. Она позволяет работать с большим количеством форматов изображений.

В качестве IDE была выбрана Pycharm. Этот инструмент имеет сильный синтаксический анализатор, инструменты реорганизации кода, статический анализатор и средство автоматического форматирования кода.

2.2 Исследование ошибок преобразования

При переходе в частотную область происходят ошибки округления. Также добавляется ошибка, вызванная искажениями и сжатием. На графике ниже представлено распределение ошибки после сжатия изображения, представленного на рис. 5 в частотной области преобразования Адамара. Сжатие проводилось кодеком jpeg с 90% качества.

Как мы видим по графику распределения ошибки (рис. 6), их подавляющее число находится в интервале от -3 до 3. По графику, представленному на рис. 7, видно, что ошибки распределены равномерно по всем высокочастотным коэффициентам и наиболее частые находятся в двух первых битах.

Еще один важный параметр – размер коэффициентов. Если искажения коэффициентов при встраивании будут слишком большими, то изменятся статистические

искажение свойства, и станет заметно изображения- контейнера.

Рис. 5. Анализируемое изображение

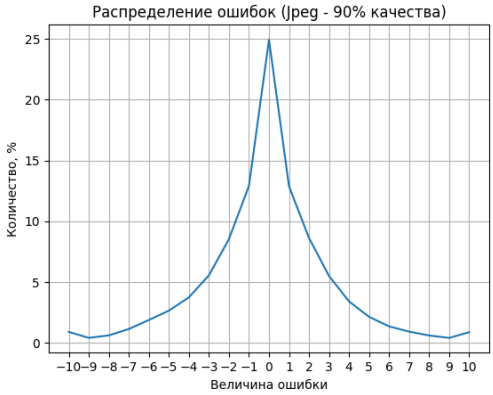

Рис. 6. Распределение ошибки

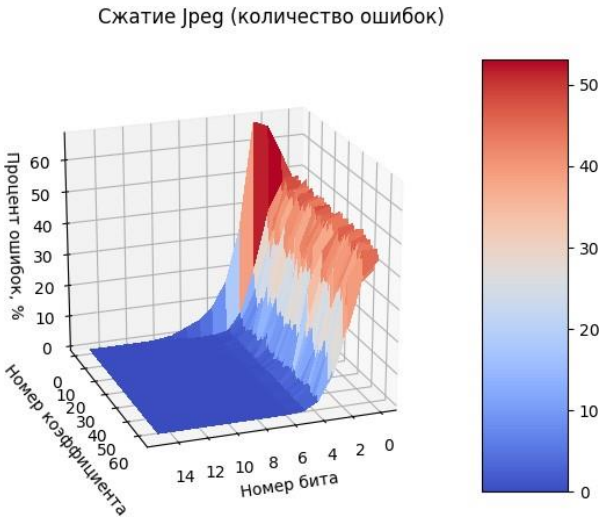

Рис. 7. Распределение ошибок в битах коэффициентов

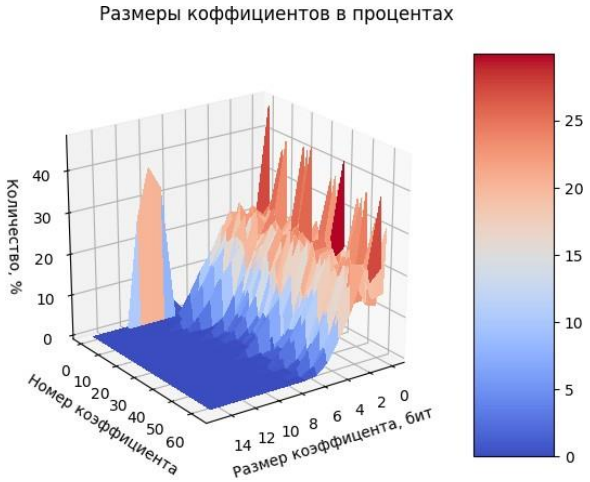

Рис. 8. Распределение размеров коэффициентов

На рис. 8 приведен график распределения размеров коэффициентов. Как мы видим по данному графику, размеры высокочастотных коэффициентов не превышают 4 бита.

2.3 Заключение по главе

В данной главе был произведен выбор основных инструментов и проведен анализ ошибок преобразования.

Анализ ошибок преобразования показал, что ошибки в большинстве своем лежат в интервале от -3 до

3. Данная специфика показывает, что битовые манипуляции в частотной области недопустимы. Если коэффициент преобразования был положительным, а при наложении ошибки он стал отрицательным, то все биты будут ошибочны. Поэтому метод встраивания не должен содержать битовые манипуляции.

Глава 3. Описание предлагаемого метода

Предлагаемый метод является частотным, работающим на основе преобразования Адамара. Встраивание предполагается производить модифицированным методом DEMD для увеличения его помехоустойчивости.

Встраивание коэффициентов предполагается производить в высокочастотной-среднечастотной области контейнера.

3.1 Модификация метода DEMD

Метод DEMD основан на следующей формуле

$$f = ((2k+1)x_1 + x_2) \ mod \ (2k^2 + 2k + 1)$$

(22),

где x1 и x2 – пиксели изображения, k – параметр встраивания.

Данный метод был выбран, поскольку он в достаточной мере устойчив к искажениям, и его сложнее атаковать статистически. На данный момент существует большое число модификаций, которые

направлены на устранение одного недостатка – переполнение пикселей оригинального изображения. В частотной области переполнение коэффициентов не происходит, так как они имеют неограниченный размер, поэтому за базу был выбран оригинальный метод DEMD.

Еще один минус данного метода в том, что при использовании его совместно с преобразованием, возникающие помехи могут превратить встраиваемое максимальное число в минимальное и наоборот. Данный эффект происходит из-за природы оператора взятия остатка от деления.

В частотной области преобразования Адамара данная ситуация будет встречаться часто, что было проверено в предыдущем параграфе.

$$f = (2kx_1 + kx_2 + x_3) mod\left(2^{l+1} - 2\right) - (2^l - 1)$$

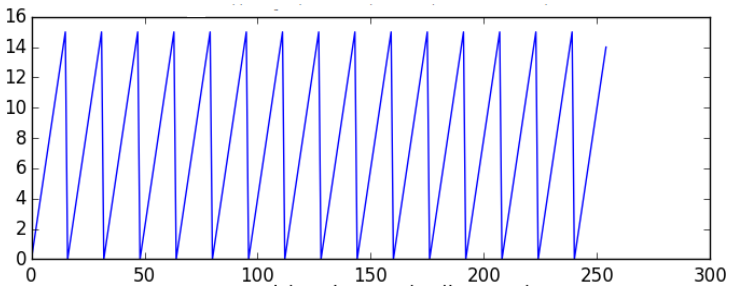

Рис. 9. Функция извлечения DEMD

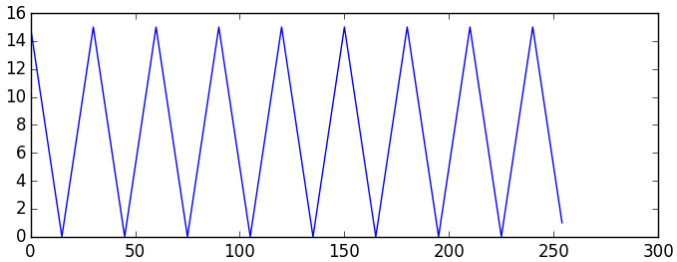

Рис. 10. Предлагаемая функция

По рис.10 видно, что если ту же самую операцию произвести с предлагаемой функцией, то ошибка будет минимальна благодаря симметричности графика.

Данная модификация полезна в случае встраивания изображения и позволяет уменьшить помехи благодаря тому, что при переполнении функция

переходит на симметричный участок графика, близкий по значению.

Также преобразование формулы задело количество коэффициентов, в которые была встроена информация. В частотной области контейнера коэффициенты имеют малую размерность, поэтому встраивание происходит в тройку коэффициентов.

3.2 Исправление ошибок преобразования

Во время встраивания в частотную область периодически происходит переполнение пикселей. Для борьбы с данным эффектом был разработан простой метод, который позволяет устранить небольшие переполнения.

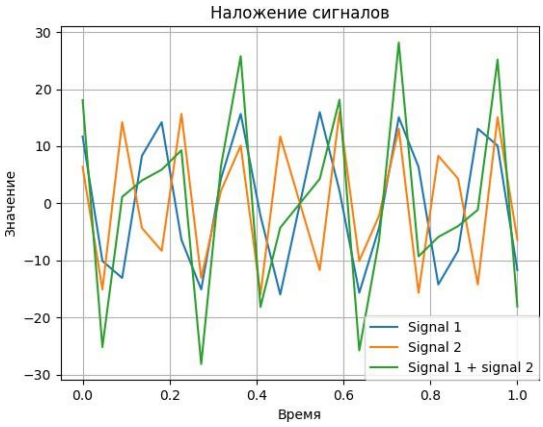

Рис. 11. Наложение сигналов

На рисунке 11 проиллюстрировано влияние наложения сигналов.

Сигналы 1 и 2 на графике не превышают по значению 15. А если сложить их частотные образы, то результирующих сигнал будет большей размерности.

Переполнения встречаются чаще в участках, где яркость близка к максимальной или нулю.

Метод заключается в том, что в исходном блоке в пространственной области вычисляется размер переполнения пикселя и вычитается.

bl[bl < 0] = -bl[bl < 0] + 1

bl[bl > 255] = 254 - (bl[bl > 255] - 255)

Уменьшенная яркость в местах переполнения компенсирует

накладываемый сигнал при встраивании. Таким образом, подавляется большое количество ошибок преобразования.

Однако есть случаи, когда исправление не происходит, к примеру, когда внедряемый сигнал имеет большую амплитуду, когда отсутствует высокочастотная составляющая исходного сигнала, и он находится близко к границам максимального или минимального значения.

Таблица 2. Результаты проверки

	Эксперимент 1	Эксперимент 2
Количество блоков с переполнением	157	63
Исправленных блоков, %	90%	100%
Ошибочных блоков в изображении, %	1,3%	0,5%

Описание компонентов разрабатываемого программного продукта

Разрабатываемый программный продукт имеет архитектуру клиент-клиент, как представлено на рисунке 12.

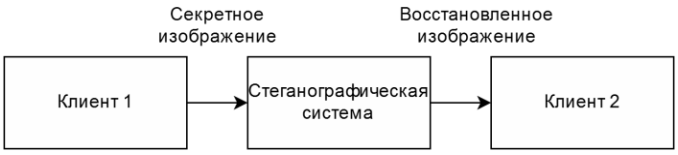

Рис. 12. Системный уровень

Скрытая передача секретного изображения происходит по открытому каналу. Сначала пользователь использует программу для встраивания

информации чтобы скрыть картинку. Дальше передача проходит по открытому каналу. Другой пользователь, получатель информации, использует программу для извлечения скрытой информации, чтобы восстановить секретное изображение.

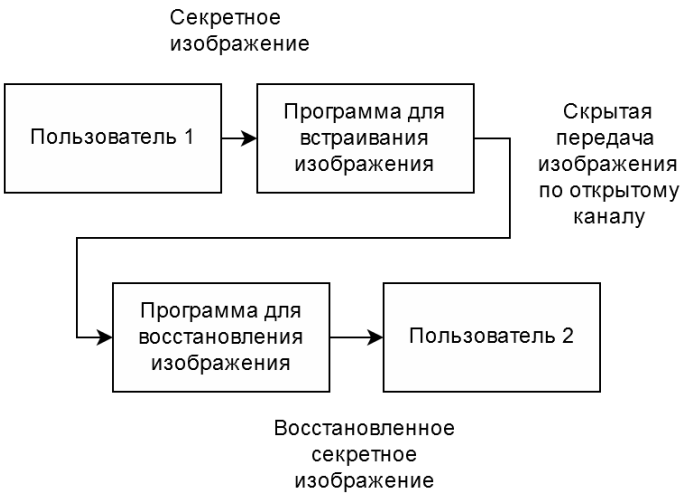

Рис 13. Архитектурный уровень

3.3 Модуль разбиения на блоки

Данный модуль предоставляет интерфейс для поблочной обработки изображения.

Основные методы класса BlockProcessor:

- map
- reduce
- combine
- save

Рассмотрим каждый метод отдельно.

Метод map позволяет применить функцию для каждого блока, а также получить изображение с измененным размером блока, если функция обработки

изменяет размер. Еще предусмотрен параметр new, который позволяет результат обработки записать в новое изображение, и в качестве результата функция выдаст новый класс BlockProcessor.

С помощью метода reduce можно обработать каждый блок, но результатом будет одна результирующая матрица заданного размера. Данная функция применялась при получении статистических данных по блокам.

Метод combine позволяет производить совместную обработку двух изображений поблочно и получить одно изображение. Как и метод map, можно результат записывать в новое изображение. Дополнительно был предусмотрен режим работы с повторением, который является опциональным. Если комбинируемое изображение меньше основного, то при выходе за границу изображение повторится.

Для увеличения скорости работы обработки используются срезы массивов numpy вместо реального разбиения на блоки

3.4 Модуль встраивания

Данный модуль содержит несколько алгоритмов встраивания. Все они были реализованы в стиле ООП и наследуют интерфейс embedder. Данный интерфейс содержит всего 3 метода: embed, extract, measure.

Методы embed и extract предоставляют интерфейс для встраивания и извлечения информации из блока. Метод measure используется для вычисления объема информации, которую можно встроить в блок заданного размера

Реализации интерфейса embedder работают только с одномерными массивами, поэтому перед встраиванием требуется обход зигзагом.

Реализованные стеганографические методы:

- lsb
- demd

- предлагаемый метод

3.5 Модуль преобразований

Данный модуль реализует два вида преобразований: wavelet и преобразование Адамара. На языке Python существует большое множество библиотек, которые работают под разными операционными системами. Не всегда есть возможность использовать преобразования, поскольку определенная библиотека может для некоторых операционных систем не работать. Данный модуль проверяет наличие библиотек для преобразований. Если такие не находятся, то используется написанная в данном модуле реализация преобразования, которая работает медленнее.

Для преобразования Адамара была написана функция генерации матрицы двумерной функции

Уолша. При первом вызове функции преобразования с заданным размером будет произведена генерация матрицы и кэширование, при последующих вызовах будет использоваться матрица из оперативной памяти. Причем матрицы сохраняются для каждого использованного размера блока.

3.6 Модуль обхода зиг-загом

Данный модуль применяется для обхода блоков зиг-загом. Основной принцип действия – перестановка элементов по предварительно сгенерированным по алгоритму матрицам перестановок.

Как и функция преобразования Адамара, генерирует матрицы перестановок для блоков определенного размера и потом хранит в памяти для последующих запусков. Применение кэш памяти позволило существенно сократить время вычислений.

3.7 Модуль качественного анализа изображения

Модуль может быть использован как программа и принимать аргументами командной строки изображения для анализа, так и может подключаться как модуль.

Некоторые функции были использованы из библиотек scipy и numpy.

Данный модуль предоставляет возможности анализа изображений.

- Абсолютное отклонение от медианы
- Отношение сигнала к шуму
- Пиковое отношение сигнала к шуму
- Среднее квадратичное отклонение
- Коэффициент корреляции
- Матожидание
- Геометрическое матожидание
- Гармоническое матожидание

3.8 Программа анализа качества встраивания

Данная программа использует программы для встраивания и извлечения информации для того, чтобы проделать эксперимент. По завершению опыта производится анализ качества изображений с помощью библиотеки для анализа (evaluation.py).

После анализа качества изображений результаты выводятся в командную строку.

Предоставляемые программой данные:

- Статистика ошибочных бит
- Абсолютное отклонение от медианы

- Отношение сигнала к шуму
- Пиковое отношение сигнала к шуму
- Среднее квадратичное отклонение
- Коэффициент корреляции

3.9 Программа анализа ошибок преобразования

Данная программа была написана для того, чтобы получить статистические данные об ошибке преобразования с разными условиями.

В начале происходит открытие изображения и искажение при помощи размытия по Гауссу или симуляцией эффекта потери качества jpeg после квантования. Затем исходное и результирующие изображения проходят преобразование Адамара. После преобразования побитно и арифметически находится разница между коэффициентами.

Данные, предоставляемые программой:

- Распределение размеров коэффициентов
- Распределение ошибки на бит после искажения Гауссовским размытием
- Распределение значений ошибки после искажения Гауссовским размытием

Глава 4. Анализ результатов и тестирование.

Проверки программы, можно подразделить условно на две части:

- Проверка метода
- Тестирование модулей

Проверка метода заключается в анализе результирующих изображений после встраивания. На данном этапе проверяетсякачество стеганографического метода.В процессе разработки для проверки основных модулей были написаны небольшие тесты. Это описано в главе «Тестирование программного продукта».

4.1 Проверка метода

Для проверки изображение встраивалось в другое изображение. На изображениях и в таблицах ниже представлены результаты работы метода.

Метод DEMD использовался совместно с преобразованием Адамара

В таблице 3 приведены критерии качества, по которым оценивался метод. Коэффициент корреляции показал значительную разницу в качестве изображений. Также количество ошибочных бит оказалось значительно меньшим в предлагаемой модификации, чем в оригинальном методе DEMD.

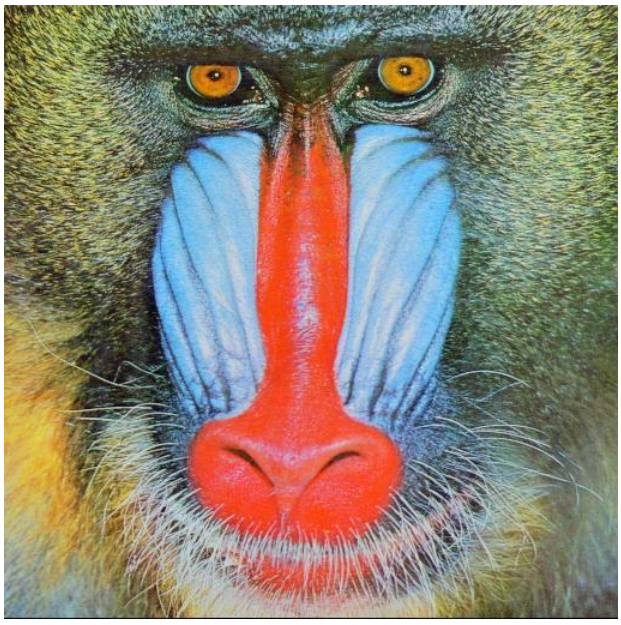

Рис. 22. Изображение для проверки

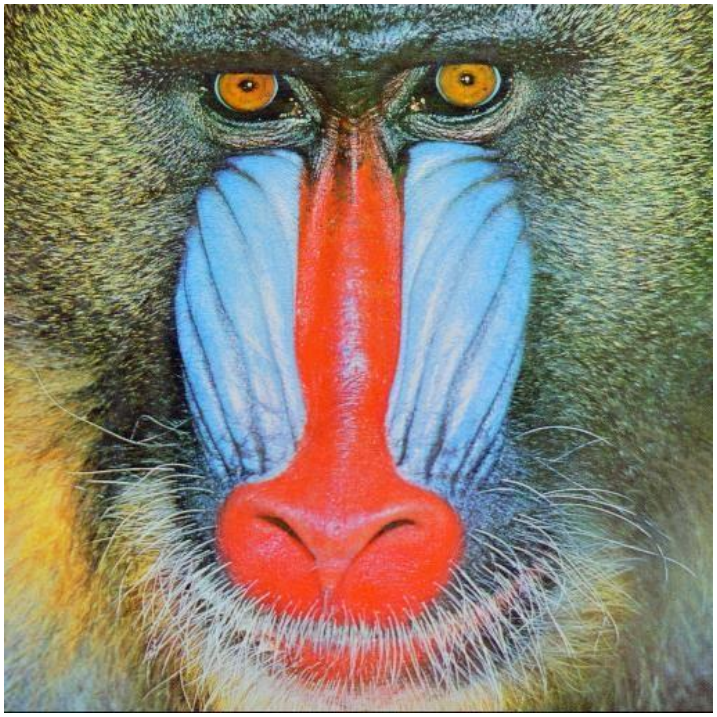

Рис. 23. Изображение со встроенной информацией предлагаемым методом

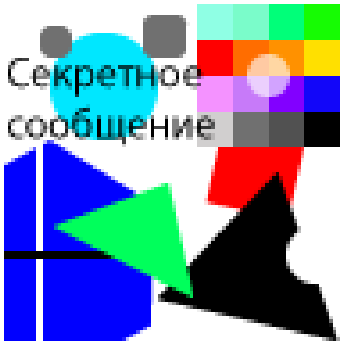

Рис. 24. Секретное изображение

Рис 25. Извлеченное изображение предлагаемым

Методом

4.2 Тестирование программного продукта

Задачей является отправить безопастно и скрытно файл с помощью стенографическим методом защиты информации .

Входных параметра будет 2 файла , первый является скрытый файл для отправки , а вторым является изоброжения или маскировочный файл.

Запускаем программный продукт Рис 26

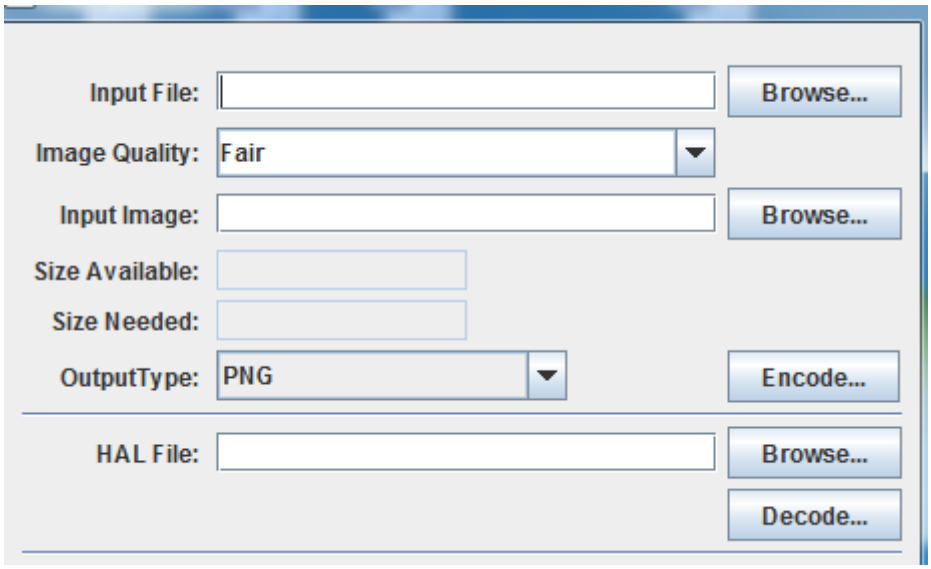

Рис 26 Интерфейс программного продукта

Выбираем файл для скрытой отправки это у нас документ “Жеткер.doc” и картинку для маскировки на Рис 27

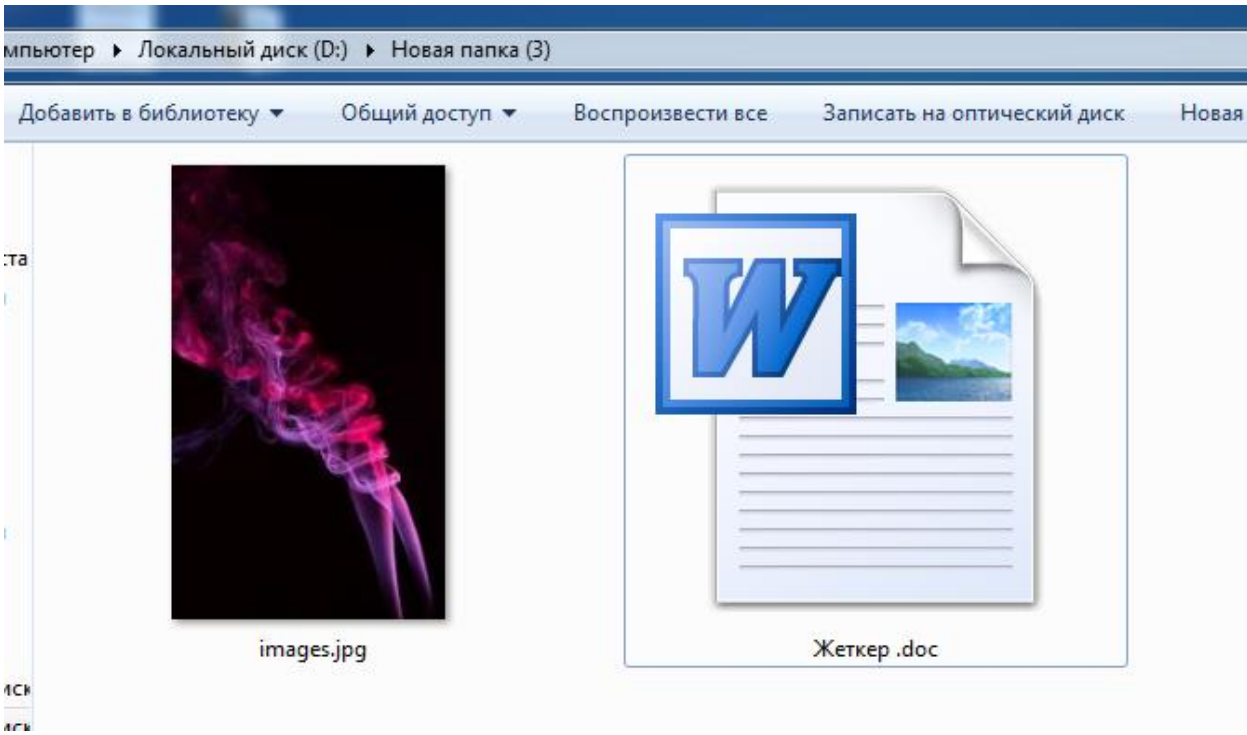

Рис 27 Файлы для тестирования программы

Дальнейшие действии очень просты указываем путь файла для скрытой отправки , указываем качество выходной параметра картинки и путь маскировачной картинки и нажимаем кнопку encode и указываем уже путь маскированного под картинку файла на рис 28

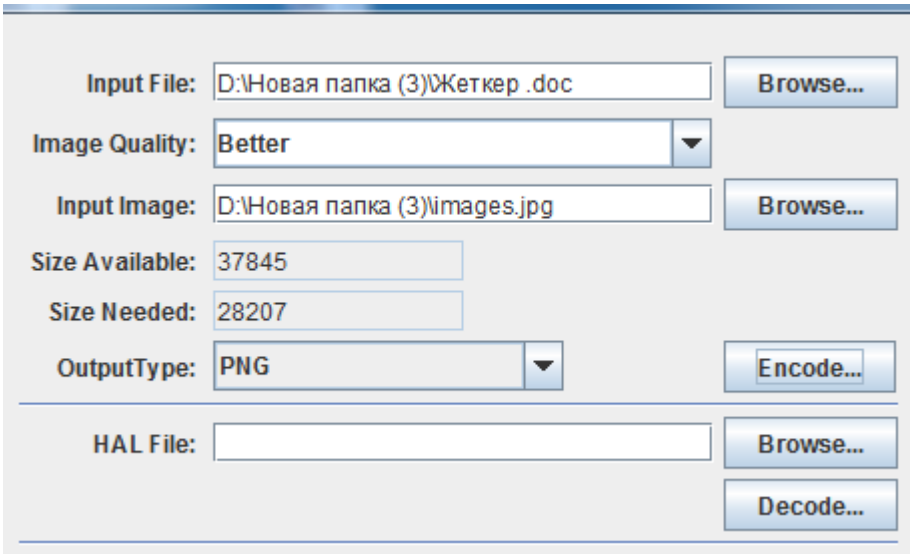

Рис 28 Пример пользования программы

Результат на лицо ни какой разницы после скрытия информации в изображения Рис 29

ДО ПОСЛЕ

Рис 29 Результат маскировки методом стенографии

Различается только в размерах файла и теперь мы можем отравить эту картинку назначенному человеку и никто другой не догадается что внутри имеется скрытый файл

Декодировка файла очень прост выбираем маскированную файл под картинку в программном интерфейсе и нажимаем decode получаем сам скрытый файл .Интерфейс программы очень прост.Рис 30

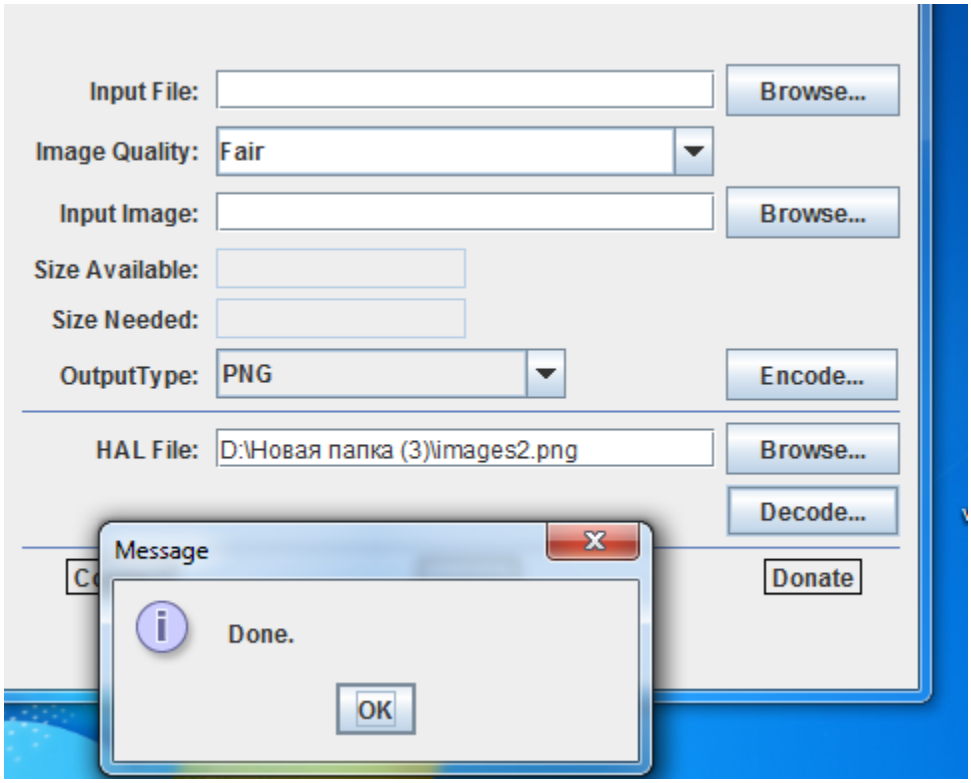

Рис 30 Извлекаем из картинки скрытый файл

Заключение

В данной работе была произведена модификация метода DEMD, для повышения его помехоустойчивости при использовании совместно с частотным преобразованием.

Для встраивания изображения предлагаемым методом не требуется помехоустойчивое кодирование за счет большей устойчивости к шуму. Основные ошибки приходятся на младшие биты встраиваемой информации, которые не являются носителями основной информации и искажают изображение незначительно.

При встраивании текстовой и бинарной информации данный метод стоит использовать совместно с помехоустойчивым кодированием, для исправления ошибок в младших битах.

В заключение можно безопастно и не заметно оправить файл с помощью данного программного продукта и само программа весит 35 килобайт и имеет простой понятный интерфейс

Применяется к

.NET Core

3.0 Preview 5 2.2 2.1 2.0

.NET Framework

4.8 4.7.2 4.7.1 4.7 4.6.2 4.6.1 4.6 4.5.2 4.5.1 4.5 4.0 3.5 3.0 2.0 1.1

.NET Platform Extensions

3.0 Preview 5

.NET Standard

2.1 Preview 2.0

Xamarin.Android

7.1

Xamarin.iOS

10.8

Список литературы