## Оглавление

## Ведение

С развитием технологий и распространением цифровых материалов, защита авторских прав стала одной из наиболее актуальных проблем в современном мире. Существующие законы об авторском праве не всегда эффективно решают эту проблему, поэтому появляются новые технические и стеганографические средства защиты, которые позволяют авторам более надежно защитить свои произведения. В данном курсовом проекте мы рассмотрим основные технические и стеганографические средства защиты авторских прав и их применение в современном мире.

## Что такое Авторское Право?

Авторское право — это законодательная защита прав авторов на их интеллектуальную собственность, такую как литературные, музыкальные, художественные и другие произведения. Оно предоставляет создателям право контролировать использование и распространение своих произведений, а также получать вознаграждение за их использование.

Цель авторского права заключается в стимулировании творческой деятельности и обеспечении защиты прав авторов. Без него авторы не имели бы никаких гарантий на защиту своих произведений от копирования и незаконного использования. Это может привести к уменьшению творческой активности и снижению качества произведений. Оно также способствует развитию культуры и образования, поскольку позволяет авторам получать доход от своих произведений и продолжать заниматься творческой деятельностью. Кроме того, авторское право способствует сохранению культурного наследия и его доступности для широкой аудитории.

В понятии «авторское право» различают три определения:

- *Автор*
- *Субъект*
- *Объект права*

*Автор* — это всегда физическое лицо, которое создало произведение.

*Субъектами* прав являются различные операторы, которые приобретают исключительное право на использование произведения, работодатель (если произведение создано работником, право переходит к работодателю), заказчик, если произведение создано по договору заказа, и наследники автора или другого владельца авторского права.

К *объектам*, считающимся интеллектуальной собственностью (ст. 1225 ГК РФ), относятся:

- Текст, фотографии, проекты и рисунки,
- песни и исполнения,
- фильмы и видео,
- подкасты и программы,
- программы,
- базы данных,
- торговые марки: названия, логотипы, слоганы,
- книги, мультфильмы, персонажи фильмов,
- изобретения и коммерческие тайны.

## История появления

История защиты авторских прав начинается в Европе в XVI веке, когда появилась печатная промышленность. В то время книги были редкостью и очень дорогими, поэтому книгопечатники могли легко зарабатывать на продаже копий чужих произведений. Чтобы защитить авторов от незаконного использования их произведений, правительства Европы начали создавать законы об авторском праве.

Первый закон об авторском праве был принят в Англии в 1710 году. Он предоставлял авторам право на эксклюзивное использование своих произведений на 14 лет, с возможностью продления на еще 14 лет. Позже этот закон был усовершенствован и стал известен как Закон об авторском праве 1842 года.

В других странах Европы также были приняты законы об авторском праве. Например, во Франции закон был принят в 1793 году, а в Германии - в 1870 году.

В США первый закон об авторском праве был принят в 1790 году и предоставлял авторам право на эксклюзивное использование своих произведений на 14 лет, с возможностью продления на еще 14 лет. С тех пор закон об авторском праве в США был усовершенствован несколько раз, и сейчас он предоставляет авторам право на использование своих произведений на всю жизнь и 70 лет после смерти.

Сегодня законы об авторском праве существуют в большинстве стран мира и защищают права создателей на их интеллектуальную собственность. Они также регулируют использование произведений в коммерческих целях и в целях научных исследований, обеспечивая баланс между защитой прав авторов и доступностью культурного наследия для широкой аудитории.

## Технические и стеганографические средства защиты авторских прав

Технические средства защиты авторских прав включают в себя различные методы шифрования, цифровую подпись и технологию DRM (Digital Rights Management). Они позволяют авторам защитить свои произведения от несанкционированного копирования и распространения либо позволяют отследить такие действия. На данный момент DRM используется множеством компаний по всему миру, среди которых Amazon, Apple Inc., Microsoft, Electronic Arts, Sony, 1C, Akella и другие. Однако, технические средства защиты авторских прав имеют свои недостатки, такие как возможность обхода или взлома.

Стеганография — это наука о скрытом передаче информации. С помощью стеганографии авторы могут скрыть информацию внутри других файлов, таких как изображения или звуковые файлы. Это позволяет им передавать информацию в тайне, что делает ее более безопасной. Однако, стеганография также имеет свои недостатки, такие как возможность обнаружения и удаления скрытой информации, а также ограничение форматов файлов, поддерживающих стеганографию.

## Современные DRM технологии

### Музыка

Аудио-CD:

Первый метод защиты музыкальных компакт-дисков от копирования использовал нарушения стандарта записи аудио компакт-дисков, которые оставались незамеченными в большинстве проигрывателей компакт-дисков, но не работали в более сложных компьютерных приводах CD-ROM. Компания Philips отказалась наклеивать на такие диски этикетку "Compact Disc Digital Audio". Также было обнаружено, что некоторые проигрыватели не "принимали" такие диски, а некоторые компьютеры, наоборот, могли их "спокойно" копировать.

В 2005 году компания Sony BMG решила использовать новую технологию защиты авторских прав на дисках, прослушивающихся на ПК. Идея была заключена в возможности воспроизведения музыки только через специальное приложение, записанное на диске. Помимо этого, на ПК устанавливалось специальное ПО (причем без согласия пользователя), предотвращающее перехват аудиопотока при воспроизведении.

В январе 2007 года EMI прекратили выпуск аудио-CD с DRM, объявив о нецелесообразности затрат на систему. Крайним творением компании, после которого все закончилось, стал диск с композициями Майкла Джексона, DRM

которого обходилась банальным закрашиванием нужной области диска. Sony, после всех судов и проблем, также отказались от DRM-защиты. На данный момент ни один из четырёх крупнейших лейблов не поддерживает DRM.

Музыка в Интернете:

Защита от авторских прав на стриминговых сервисах основана на использовании технологии DRM. Когда пользователь слушает музыку на стриминговом сервисе, он получает доступ к потоку данных, который передается с сервера сервиса на устройство пользователя. Этот поток данных защищен технологией DRM, которая шифрует данные и предотвращает их несанкционированное копирование или распространение.

Для того чтобы получить доступ к защищенному потоку данных, пользователь должен иметь аккаунт на стриминговом сервисе и оплатить подписку. Когда пользователь оплачивает подписку, он получает право использовать защищенный поток данных только в рамках условий, указанных правообладателем. Например, пользователь может получить доступ к защищенному потоку данных только на определенном устройстве или в определенной программе воспроизведения.

Если пользователь попытается скопировать или распространить защищенный поток данных без разрешения правообладателя, то технология DRM предотвратит это и защитит права авторов. Однако, защита DRM может вызывать проблемы для пользователей, так как она может быть несовместима с некоторыми устройствами или программами воспроизведения. Кроме того, она может ограничивать свободу пользователя в использовании купленной музыки, например, запрещая ее использование в других устройствах или программах.

**Видеоматериалы, фильмы**

YouTube:

Как защитить АП на крупнейшем в мире стриминговом сервисе?

Защита от авторских прав на YouTube основана на использовании технологии Content ID. Когда пользователь загружает видео на YouTube, оно проходит через систему Content ID, которая сравнивает его с базой данных авторских прав. Если система обнаруживает, что в видео используется защищенный авторским правом контент, то она может заблокировать видео или разрешить его использование с определенными ограничениями.

Если автор контента не желает, чтобы его контент использовался на YouTube без его разрешения, он может зарегистрировать свои права в системе Content ID. Таким образом, система будет автоматически обнаруживать и блокировать любое видео, которое использует защищенный авторским правом контент без разрешения правообладателя.

Фильмы:

Так как главная проблема современных стриминговых сервисов – это пиратство, а за ним утечка платящей аудитории, то и тут нашлось применение DRM. У этой технологии три функции: шифрование, расшифровка и управление ключами этого шифрования.

Видео, приходящее в браузер – упаковано с помощью DRM. Без ключа для расшифровки невозможно начать просмотр. Netflix (как и большинство стриминговых сервисов) позволяют сохранять фильмы и сериалы для просмотра позже. Даже так не получиться достать эти файлы из кеша. Ключ шифрования получают только обладатели подписки. Это и есть главный принцип DRM. Казалось бы, очевидным включить запись экрана при помощи сторонних программ, но тут постарались разработчики ОС. Они просто не разрешат Вам использовать запись с подобных приложений в браузерах.

Голливуд тоже не остался в стороне. Там используется технология на уровне железа и невидимых водяных знаков для особо- ценного контента, такого как 4K UHD.

**Тексты, документы, Электронные книги**

Adobe PDF DRM — это формат для понимания того, что такое DRM по отношению к электронным публикациям. После этого в DRM поменялись, в основном, только особенности реализации.

Устройство сначала отправляло запрос на сервер. Он, в свою очередь, осуществлял проверку легитимности доступа к документу. После успешного прохождения проверки сервер генерировал и отправлял устройству файл в формате RMF (Rights Management Format), который представлял собой XML документ. В этом файле хранился криптографический ключ для расшифровки PDF, перечень разрешённых действий и сертификат для проверки лицензии. Кроме того, файл RMF должен содержать хотя бы одно условие, необходимое для успешного доступа к документу. Это может быть учетная запись пользователя (ID), CPUID или ссылка на серийный номер оборудования.

**Компьютерные игры**

DRM в компьютерных играх используется для различных целей, но в целом все схемы направлены на защиту от копирования и распространения пиратских копий игр.

1. Denuvo — это один из самых популярных и эффективных типов DRM, который используется во многих современных играх. Он использует сложные алгоритмы шифрования и защиты от взлома.

2. Steam DRM — это система защиты, которая используется на платформе Steam. Она требует, чтобы игроки запускали игры через Steam и проверяет подлинность игры каждый раз при запуске.

3. Origin DRM — это система защиты, которая используется на платформе Origin от Electronic Arts. Она работает аналогично Steam DRM.

4. SecuROM — это старый тип DRM, который все еще используется в некоторых играх. Он требует, чтобы игроки вводили серийные номера и проверяет подлинность игры при запуске.

5. StarForce — это еще один старый тип DRM, который используется в некоторых играх. Он также требует, чтобы игроки вводили серийные номера и проверяет подлинность игры при запуске.

## Несколько слов о стеганографии

*Стеганография* — это наука о скрытом передаче информации. С помощью стеганографии авторы могут скрыть информацию внутри других файлов, таких как изображения или звуковые файлы. Это позволяет им передавать информацию в тайне, что делает ее более безопасной. В отличие от криптографии, другой области защиты информации, которая скрывает содержание секретных сообщений, стеганография скрывает их существование.

В стеганографии используются следующие основные понятия:

- Стегосистема — это система, которая позволяет скрыть секретную информацию внутри другого файла, чтобы она не была заметна обычным пользователем. При построении такой системы условились о том, что: 1) враг представляет работу стеганографической системы. Неизвестным для противника является ключ, с помощью которого можно узнать о факте существования и содержание тайного сообщения. 2) При обнаружении противником наличия скрытого сообщения он не должен смочь извлечь сообщение до тех пор, пока он не будет владеть ключом. 3) Противник не имеет технических и прочих преимуществ.

- Сообщение — это общее название для конфиденциальной информации, которая передается, например, кусок молока, голова раба или цифровой файл.

- Контейнер — любая информация, используемая для сокрытия тайного сообщения. Есть пустой и заполненный (не содержащий и содержащий секретное послание)

- Стегоканал — канал передачи стегоконтейнера.

- Стегоключ — это пароль или ключ, который используется для доступа к скрытой информации в стегосистеме. Он может быть необходим для извлечения секретного сообщения из файла-носителя. Без знания стегоключа невозможно получить доступ к скрытой информации. Бывает закрытый и открытый. Если стегосистема использует закрытый ключ, то он должен быть создан или до начала обмена сообщениями, или передан по защищённому каналу. Стегосистема, использующая открытый ключ, должна быть устроена таким образом, чтобы было невозможно получить из него закрытый ключ. В этом случае открытый ключ можно передавать по незащищённому каналу.

**Компьютерная стеганография**

Использование компьютерной платформы в качестве основы называется компьютерной стеганографией.

**Цифровая стеганография**

*Цифровая стеганография* — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Можно скрыть информацию в различных типах файлов, в различных онлайн-местах и даже в местах, о которых вы никогда не подозревали, например, изменяя время между пакетами данных, отправляемыми по сетевому протоколу.

Медиафайлы являются одними из самых популярных мест для сокрытия информации, поскольку их большой размер означает, что в них можно поместить больше секретных данных, не вызывая подозрений. Существует три отдельных способа, которыми информация может быть скрыта в файлах:

- Путем добавления его в файл, например, в неиспользуемое пространство заголовка.
- Путем замены части информации в файле.

Один из наиболее распространенных способов сделать это - изменить Младший значащий бит (LSB). В графических, звуковых и других файлах последние биты информации в байте не обязательно так важны, как начальные. Например, 10010010 может быть оттенком синего. Если мы изменим только последние два бита на 10010001, это может быть оттенок синего, который почти точно такой же. Это означает, что мы можем скрыть наши секретные данные в последних двух битах каждого отдельного пикселя изображения, не

изменяя изображение заметно. Если мы изменим первые биты, это значительно изменит его.

- Путем создания нового, казалось бы, доброкачественного файла, который на самом деле является просто прикрытием для стеганографического текста.

**Видеостеганография**

Поскольку видео являются относительно большими файлами, они могут скрывать больше данных, чем другие методы. Наиболее распространенные методы включают различные схемы замены наименее значимых битов (например, полиномиальные уравнения, основанные на хешировании). Также можно встраивать данные в каждый кадр, использовать фильтрацию или маскировку данных. В Интернете можно найти множество программ для стеганографии видео.

**Сетевая стеганография**

В последние годы широкое распространение получили методы передачи секретной информации через компьютерные сети, использующие особенности протоколов передачи данных. Такие методы известны как "сетевая стеганография". Термин был впервые введен Кшиштофом Щипиорски в 2003 году. Типичным методом сетевой стеганографии является изменение одной характеристики сетевого протокола.

Кроме того, связь между двумя или более различными протоколами может быть использована для более надежной маскировки передачи секретных сообщений.

Сетевая стеганография охватывает особенно широкий спектр технологий:

- *WLAN-стеганография* основывается на методах, которые используются для передачи стеганограмм в беспроводных сетях). Практический пример WLAN-стеганографии — система HICCUPS (Hidden Communication System for Corrupted Networks).
- *LACK-стеганография* — скрытие сообщений во время разговоров с использованием IP-телефонии. Например: использование пакетов, которые задерживаются или намеренно повреждаются и игнорируются приемником или сокрытие информации в полях заголовка, которые не используются.

Принцип работы LACK заключается в следующем. Отправитель (Алиса) выбирает один из пакетов речевого потока, полезная нагрузка которого заменяется битами секретного сообщения, встроенным в один из пакетов, бит стеганограммы. Затем выбранный пакет намеренно задерживается. Если пакет с чрезмерной задержкой достигает получателя, не знакомого с процедурой стеганограммы, он отбрасывается. Однако если получатель (Боб) знает о

скрытом сообщении, он извлекает скрытую информацию вместо того, чтобы удалить полученный пакет RTP.

**Стеганография изображений**

Данные могут быть скрыты в изображениях с помощью различных методов.

Для стеганографии изображений существует несколько требований:

1. "*Прозрачность*", или отсутствие различий между исходным изображением и контейнером-результатом при визуальном контроле. Формальных критериев оценки "прозрачности" так как восприятие у всех субъективное.

2. *Робастность*, или устойчивость скрытого сообщения к различным искажениям, в том числе и злонамеренным (случайным возмущениям при передаче информации, изменениям формата файла, сжатием, изменениям его размеров). Робастность обычно вступает в противоречие с прозрачностью скрытого сообщения.

3. *Устойчивость* к попыткам удаления или зашумления. Из-за того, что абсолютной устойчивости достичь невозможно, стараются обеспечить её определённый уровень по отношению к заданному уровню атак.

4. Возможность встраивания *заданного объёма* информации и/или её дублирование для повышения надёжности. Может вступать в противоречие с робастностью и прозрачностью.

5. *Секретность маркировки*. Чаще используются 2 уровня обеспечения секретности: предотвращение доступа к декодированию и защита от извлечения информации в случае её обнаружения.

Цифровые стеганографические техники для защиты графической информации включают технику использования зарезервированных для полей при использовании компьютерных форматов данных и технику избыточности для цифровых фотографий. Использование зарезервированных полей проще в применении, но менее скрытно, в то время как техники избыточности позволяют внедрить больше информации и больше подходят для защиты авторских прав.

Существующие методы:

- *Метод замены наименьших значащих битов (LSB-метод*). Он основан на использовании ошибки дискретизации, которая всегда присутствует в оцифрованном изображении. Эта ошибка соответствует младшему разряду числа, определяющего значение цветовой составляющей элемента изображения (пикселя). Поэтому изменение младших разрядов

в большинстве случаев не приводит к существенному изменению изображения и не является визуально различимым.

- *Метод использования особенностей форматов данных,* использующих сжатие с потерей данных (например, JPEG-формат). Этот метод (в отличие от предыдущего) более стоек к геометрическим преобразованиям и обнаружению канала передачи, так как имеется возможность в широком диапазоне варьировать качество сжатого изображения, что делает невозможным определение происхождения искажения.

- Цифровые изображения в Интернете обычно хранятся в цветовой модели RGB. Графические файлы этой цифровой модели кодируют каждую точку изображения тремя байтами. Каждая такая точка состоит из красного, зеленого и синего аддитивных компонентов; изменение каждого из трех наименее значимых битов изменяет интенсивность данной точки менее чем на 1%.

  В 800 Кбайт стандартной графики могут скрываться около 100 Кбайт информации (незаметной при просмотре человеком). Человеческий глаз воспринимает 7 из 8 битов в канале R (красный), 8 битов в канале G (зеленый) и 4 из 8 битов в канале B (синий). Можно утверждать, что человеческий глаз наименее чувствителен к синему и красному цветам. Это преимущество позволяет встраивать информацию в синюю и красную цветовую гамму.

- *Метод цифровых водяных знаков (ЦВЗ или watermarking)*. Это наиболее востребованный для защиты авторских прав метод. Именно его мы и решили реализовать его в нашей курсовой работе. Он основан на встраивание в мультимедийный файл скрытых маркеров, устойчивых к различным атакам. ЦВЗ должны быть надёжными, устойчивыми к искажениям файла (масштабирование, вращение, компрессия с потерями и др.) и иметь небольшой объём.

  Чтобы восстановить водяной знак из защищенного файла с известными параметрами синтеза (в частности, пространственной несущей), достаточно выполнить двумерное преобразование Фурье.
- *Метод скрытого маркера (метки)* представляют собой узкополосные сигналы в широком частотном диапазоне маркируемого изображения. Такие маркеры создаются путем модификации двух различных алгоритмов: фазовой модуляции информационного сигнала псевдослучайной последовательностью для скрытия информации или разделения доступного частотного диапазона на несколько каналов (передача происходит между этими каналами).

По сравнению с исходным изображением, метки добавляют некоторый дополнительный шум, но поскольку шум всегда присутствует в изображении, его незначительное увеличение за счет добавления меток не вызывает видимых искажений. Более того, поскольку метки распределены по всему исходному изображению более устойчив к обрезке.

**Аудио стеганография**

Аудиостеганография также включает в себя ряд различных методов. Как и в случае с другими видами стеганографии, важно, чтобы методы были надежными, чтобы можно было передать разумное количество секретных данных, а любые изменения должны быть как можно более незаметными. К наиболее распространенным методам относятся:

- Кодирование наименее значимых битов - как и в случае с другими типами наименее значимых битов, упомянутыми ранее, можно изменить наименее значимую часть аудиоданных, не внося очевидных изменений в звучание файла.
- Скрытие эха - также возможно маскировать данные с помощью эха.
- Вставка тона - поскольку низкочастотные тона трудно обнаружить, когда они находятся рядом с очень сильными тонами, эти низкочастотные тона могут быть использованы для скрытия данных.

**Текстовая стеганография**

*Лингвистическая стеганография*: лингвистическая техника, используемая для скрытия сообщения в тексте так, чтобы посторонние не могли обнаружить его присутствие. Ее можно разделить на два типа:

- Семаграммы: информация скрывается с использованием только символов или знаков. Этот метод также делится на два типа:

    1. Визуальные семаграммы: визуальные семаграммы используют повседневные физические объекты для передачи сообщений. Пример: позиционирование продукта на определенном сайте.
    2. Текстовые семаграммы: этот тип используется для сокрытия сообщений путем изменения внешнего вида передаваемого текста, изменения шрифта или размера, добавления дополнительных пробелов между словами или использования различных замен символов в рукописном тексте.

- *Техническая стеганография*: Техническая стеганография использует специальные инструменты, устройства или научные методы для сокрытия сообщений. Этот вид может использовать невидимые чернила, микроточки, компьютерные методы или различные тайники для сохранения сообщения в тайне.

- Обложка: сообщение обложки является носителем сообщения, такого как изображение, видео, аудио, текст или какой-либо другой цифровой носитель. Обложка разделена на блоки и биты сообщений, которые скрыты в каждом блоке. То информация кодируется путем изменения различных свойств изображения обложки. Блоки крышки остаются неизменными, если блок сообщений равен нулю.

Примером лингвистической стеганографии является таблица синонимов, с помощью которой можно доказать свое авторство. Преимуществом является то, что этот метод не зависим от размера, носителя и так далее и является одним из самых надежных.

*Текстовая стеганография*: в этом подходе текст обложки создается путем генерации случайного символа последовательности, изменение слов в тексте, использование контекстно-свободных грамматик или изменение форматирования текста, существующий текст, чтобы скрыть сообщение.

Текст обложки, сгенерированный таким подходом, может претендовать на лингвистический статус стеганография, если текст управляется лингвистически. Хотя эти текстовые методы имеют свои уникальные особенности характеристики для текста обложки, но страдает от различных проблем как с лингвистической точки зрения, так и с точки зрения безопасности.

Когда речь идет о тексте, существуют различные способы скрыть информацию. Однако текстовые файлы очень малы и поэтому не очень подходят для передачи больших объемов данных. Простой способ сделать это - открыть Microsoft Word, напечатать свое секретное сообщение, а затем изменить цвет текста на белый.

Белый фон текстового процессора должен казаться пустым. Затем сообщение сохраняется и отправляется вашему сообщнику. При этом не забудьте проинструктировать его о том, как получить доступ к информации по защищенному каналу.

В противном случае они могут не понять, почему вы продолжаете посылать им пустые документы. Этот метод не очень безопасен. Потому что любой, кто перехватит ваши сообщения, заподозрит, почему вы продолжаете отправлять пустые документы. Просто выделите текст и измените цвет...

## Стеганография в защите авторских прав в изображении

Как уже говорилось, наиболее востребованным для подтверждения АП является метод Цифрового Водяного Знака. К сожалению, методы скрытия данных в пространственной области изображения являются нестойкими к большинству из известных видов искажения, таких как, к примеру, сжатие с потерями. Отличие заключается в наборе изменяемого подмножества и алгоритме смены значений пикселей, в то время как встраивание информации

происходит в первичное изображение. Достойность же таких алгоритмов заключается в отсутствии громоздких линейных вычислений, так как, фактически, ЦВЗ встраиваются путем управления компонентами яркости или цвета.

Наибольший интерес представляет интегрирование информации в изображение, где происходит сжатие с потерями. Для этого используют область изменяемого разрешения или частотную область. Методы, использующие частотную область для сокрытия данных, более устойчивы к различным внешним воздействиям на контейнер-изображении. Такие методы обладают хорошими робастными свойствами.

Эти преобразования можно применять к отдельным частям изображения или ко всему изображению. Для сокрытия данных рекомендуется применять преобразования, с расчетом на изменение изображения со временем. Сжатие. Для алгоритмов встраивания информации в видеоряд используются более простые алгоритмы, чем для цифровых изображений.

*Patchwork* – это перспективный алгоритм встраивания водяных знаков, который имеет высокую устойчивость ко многим популярным атакам, таким, как добавление шума, фильтрация, сжатие, повторное квантование и повторная выборка. Метод состоит из нескольких действий, которые обеспечивают его простую реализацию и в то же время хорошую устойчивость ко многим атакам.

Реализация алгоритма patchwork:

- выбор двух псевдослучайных значений;

- добавление небольшой константы к выборке одного значения и вычитание этой же константы из выборки другого значения;

- процесс обнаружения начинается с нахождения остатка от вычитания этих значений.

В нашей курсовой работе мы использовали *метод замены наименее значащих битов.*

Зачастую длина бит внедряемой информации меньше количества бит изображения, поэтому после внедрения появляются две области с различными статистическими свойствами, что легко распознается статистическими тестами. Поэтому внедряемую информацию дополняют информационным мусором – случайными битами, чтобы ее битовая длина была равна количеству пикселей в изображении, используемом для внедрения.

Как уже говорилось выше, в этом методе, при любом искажении контейнера встроенная информация также искажается. Чтобы определить полезную емкость контейнера используем формулу:

$$Q = H * W * V * D$$

Где $H$ – это высота изображения в пикселях, $W$ – это ширина изображения в пикселях, $V$ – это число компонент цвета, $D$ – это количество наименее значащих бит в каждой компоненте, $Q$ – это емкость контейнера, измеряемая в битах.

## Описание работы программы и результаты

Программа имеет два режима ручное тестирование и автоматическое. В режиме ручного тестирования параметры для подписи задаются вводом в консоль, в автоматическом программа использует заданные тестовые параметры.

Первый этап работы – генерация открытых ключей, для этого используется алгоритм Эль-Гамаля. Далее сгенерированные ключи y, r, и s записываются в изображение. Также создается файл с координатами измененных пикселей, для получения информации о ключах и проверки подписи.

Запись в изображение происходит следующим образом. Исходное изображение разбивается на пиксели, из которых выделяются цветовые компоненты Red, Green, Blue. Каждая из компонент представляет собой число в диапазоне от 0 до 255, мы используем младший бит двоичного представления для побитовой записи открытых ключей Red – y, Green – r, Blue – s.

В результате мы получаем новое изображение с закодированными открытыми ключами и координатный список измененных пикселей.

Для проверки подписи мы выделяем закодированные ключи и вновь пользуемся алгоритмом Эль-Гамаля.

Пример работы в автоматическом режиме:

Исходное изображение:

Изображение после кодирования:

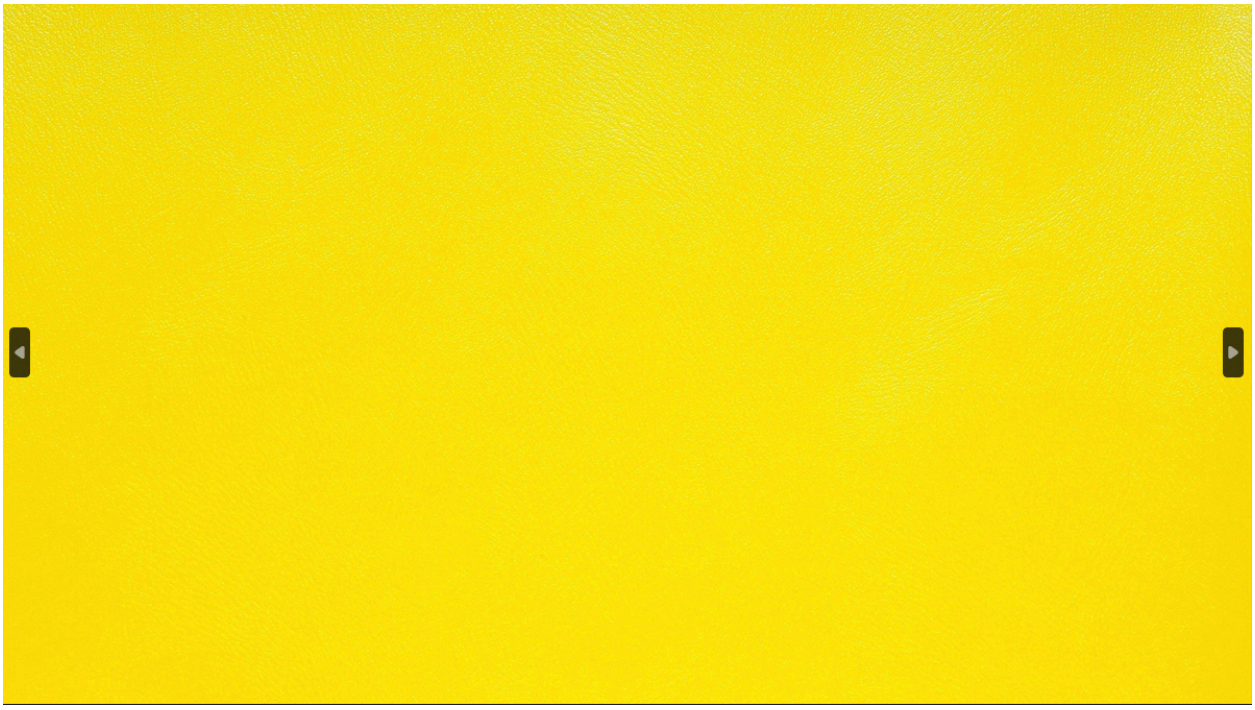
```
Возможные g: [4294967243, 4294967256, 4294967271, 4294967283, 4294967291]
Выбраное g: 4294967271
Полученое p: 8589934543
Закрытый ключ x: 6143955024
Открытый ключ y: 6870474185
Случайное k: 7750327757
Первый ключ подписи r: 6976940681
Второй ключ подписи s: 4106029248
keys were written to the keys.txt file
Раскодированые ключи:
 s: 4106029248
 r: 6976940681
 y: 6870474185
Подпись подтверждена
```

Исходное изображение:

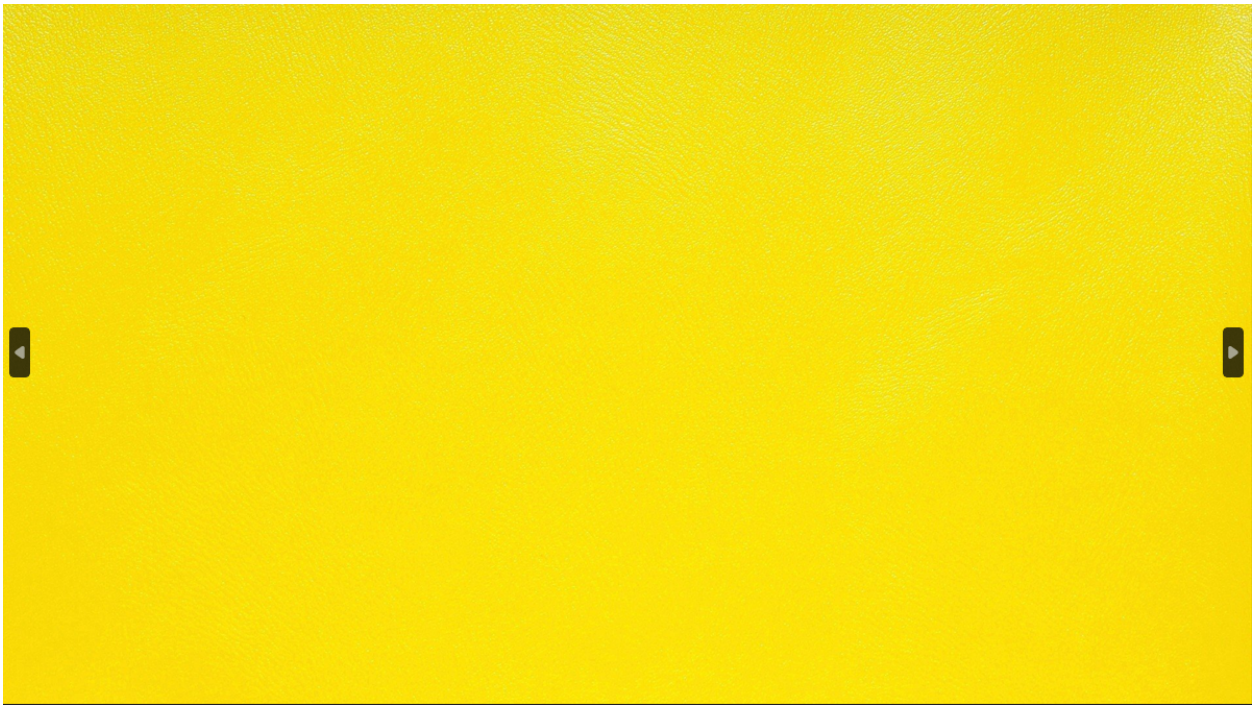
Изображение после кодирования:

```
Возможные g: [4294967243, 4294967256, 4294967271, 4294967283, 4294967291]
Выбраное g: 4294967271
Полученое p: 8589934543
Закрытый ключ x: 396274159
Открытый ключ y: 7055389706
Случайное k: 7138465787
Первый ключ подписи r: 1105506269
Второй ключ подписи s: 4032179285
keys were written to the keys.txt file
Раскодированые ключи:
 s: 4032179285
 r: 1105506269
 y: 7055389706
Подпись подтверждена
```

Исходное изображение:



Изображение после кодирования:



```
Возможные g: [4294967243, 4294967256, 4294967271, 4294967283, 4294967291]
Выбраное g: 4294967283
Полученое p: 8589934567
Закрытый ключ x: 6186729890
Открытый ключ y: 701326884
Случайное k: 874490311
Первый ключ подписи r: 2146726179
Второй ключ подписи s: 1582818504
keys were written to the keys.txt file
Раскодированые ключи:
 s: 1582818504
 r: 2146726179
 y: 701326884
Подпись подтверждена
```

## Выводы

Современный мир стал свидетелем взрывного роста цифровых технологий и распространения цифровых материалов. Книги, фильмы, музыка и другие произведения искусства стали доступными в электронном виде, что позволяет быстро и удобно получать доступ к ним. Однако это также привело к появлению проблемы защиты авторских прав.

Существующие законы об авторском праве не всегда способны эффективно защитить права авторов, поэтому появляются новые технические и стеганографические средства защиты. Технические средства защиты включают в себя различные методы шифрования, цифровую подпись и технологию DRM (Digital Rights Management). С помощью этих средств авторы могут защитить свои произведения от несанкционированного копирования и распространения.

Однако, технические средства защиты имеют свои недостатки. Например, они могут быть обойдены или взломаны, что делает их менее эффективными. Кроме того, некоторые потребители не любят ограничения, которые вводятся с помощью технических средств защиты.

В этой ситуации стеганография может стать более эффективным решением для защиты авторских прав. С ее помощью авторы могут скрыть информацию внутри других файлов, таких как изображения или звуковые файлы. Это позволяет им передавать информацию в тайне, что делает ее более безопасной.

Однако, стеганография также имеет свои недостатки. Например, скрытая информация может быть обнаружена и удалена, а некоторые форматы файлов не поддерживают такого рода преобразования.

В целом, защита авторских прав является сложной проблемой, которая требует комплексного подхода. У всего есть свои достоинства и недостатки. Технические и стеганографические средства защиты могут помочь авторам защитить свои произведения, но они не являются универсальным решением.

## Список литературы


- https://suvorov.legal/avtorskoe-pravo/?ysclid=li9fbdxh6r833870199#Что_такое_авторское_право
- https://masters.donntu.ru/2020/fknt/poludennyi/diss/index.htm?ysclid=li9dnrjjw606913850
- https://ru.wikipedia.org/wiki/Технические_средства_защиты_авторских_прав#Текст,_документы,_электронные_книги
- https://habr.com/ru/companies/ruvds/articles/565432/
- https://dzen.ru/a/XGwZ7NhnzgCuclIK
- https://ru.wikipedia.org/wiki/Стеганография#Сетевая_стеганография
- https://dzen.ru/a/Yv_fjyJwahv8JvQM
- https://masters.donntu.ru/2019/fknt/sidorchuk/library/transarticle.htm?ysclid=licaa8p3ma776315827
- https://elib.bsu.by/bitstream/123456789/261617/1/329-331.pdf?ysclid=li9d9eyr98222622357
- http://repo.ssau.ru/bitstream/Chelovek-Znak-Tehnika/ZAShITA-AVTORSKIH-PRAV-NA-IZOBRAZhENIE-I-AUDIOFAILY-NA-OSNOVE-VSTRAIVANIYa-CIFROVOGO-VODYaNOGO-ZNAKA-87910/1/06.%20Габутдинова%20К.С.%2C%20Тихонова%20В.В.%2C%20Усманов%20Р.И.%2032-38.pdf?ysclid=licebce9a9516301321