Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Реферат на тему «Метод PVD (Pixel-Value Differencing)»

Студент: Трубач Д. С.

ФИТ 4 курс 5 группа

Преподаватель: Ржеутская Н. В.

Минск 2024

**Содержание**

[Введение 5](#_Toc178713728)

[1 Цифровая стеганография 6](#_Toc178713729)

[1.1 Метод PVD 6](#_Toc178713730)

[1.2 Преимущества и недостатки метода PVD 9](#_Toc178713731)

[1.3 Примеры применения метода PVD 10](#_Toc178713732)

[1.4 Методы улучшения безопасности стегосистем на основе PVD 11](#_Toc178713733)

[1.5 Альтернативы методу PVD 12](#_Toc178713734)

[Заключение 13](#_Toc178713735)

[Список используемых источников 14](#_Toc178713736)

# Введение

Цифровая стеганография является важной областью исследований в условиях современных информационных технологий, где передача и защита данных играют ключевую роль. С развитием интернета и цифровых коммуникаций возникла необходимость не только шифровать информацию, но и скрывать сам факт её существования, что делает стеганографию крайне востребованной. Особую актуальность это приобретает в контексте безопасности данных и конфиденциальности информации.

Метод PVD (Pixel-Value Differencing) представляет собой один из передовых способов цифровой стеганографии, который использует особенности восприятия изображений человеком. Благодаря возможности скрывать данные в разнице значений соседних пикселей, метод PVD позволяет передавать информацию с высокой степенью скрытности, при этом минимально искажая исходное изображение. Это делает его популярным выбором для задач, связанных с безопасной передачей данных и цифровыми водяными знаками.

Целью данного реферата является рассмотрение принципа работы метода PVD, а также анализ его применения в задачах цифровой стеганографии. В работе также будут рассмотрены основные преимущества и недостатки метода PVD, примеры его использования в реальных приложениях, а также возможные альтернативы данному методу. Важной частью исследования станет обзор методов улучшения безопасности стеганографических систем на основе PVD, что особенно актуально в условиях современных вызовов, связанных с использованием машинного обучения и других передовых технологий для анализа и обнаружения скрытой информации. Таким образом, данный реферат предоставляет комплексный анализ метода PVD в контексте его актуальности и эффективности в современных условиях защиты данных.

# 1 Цифровая стеганография

Стеганография — это искусство и наука скрытия информации таким образом, что факт её передачи остаётся незаметным. В отличие от криптографии, которая шифрует данные, стеганография маскирует сам факт существования сообщения. В стеганографии можно скрывать данные в различных носителях, таких как изображения, аудио, видео и текстовые файлы.

Основные виды стеганографии:

* **изображения** — скрытие данных в графических файлах;
* **аудио** — встраивание данных в звуковые файлы;
* **видео** — использование видеофайлов для скрытия информации;
* **текст** — изменение текста таким образом, что в нем скрываются сообщения.

Одной из ключевых особенностей стеганографии является способность сохранять незаметность сообщения, даже если злоумышленник перехватит носитель информации. Важно, чтобы изменения, вносимые в исходные данные, были минимальными и не вызывали подозрений у стороннего наблюдателя. Это особенно критично при работе с визуальными или аудиофайлами, где даже малозаметные изменения могут быть выявлены с помощью специальных инструментов анализа.

Современные методы стеганографии, такие как метод PVD (Pixel-Value Differencing), обеспечивают высокий уровень скрытности благодаря использованию особенностей человеческого восприятия изображений. Скрытие данных в таких файлах требует точных математических расчетов и понимания специфики медианосителей, чтобы встраивание информации не влияло на качество изображения, звука или текста.

Основные задачи стеганографии:

* безопасность — защита информации от несанкционированного доступа;
* скрытность — недопущение обнаружения факта скрытия данных;
* сохранение качества изображения — минимизация искажений оригинальных данных, чтобы стеганографическое сообщение не вызывало подозрений.

Кроме того, стеганография часто используется совместно с криптографией, когда данные сначала шифруются, а затем скрываются в медианосителе. Это позволяет значительно повысить безопасность передачи данных, обеспечивая защиту как от расшифровки сообщения, так и от обнаружения самого факта передачи. Таким образом, стеганография остаётся важным элементом комплексных систем защиты информации в условиях современной цифровой среды.

## 1.1 Метод PVD

Метод PVD (Pixel-Value Differencing) основан на использовании разницы между значениями соседних пикселей изображения. В зависимости от величины этой разницы, данные можно скрыть с минимальными изменениями. Основная идея заключается в том, что большие различия между пикселями позволяют встраивать больше данных, в то время как при малых различиях скрывать информацию нужно осторожно, чтобы избежать заметных искажений.

Изображение разделяется на пары соседних пикселей (или на более крупные блоки), и для каждой такой пары вычисляется разница их значений. Эта разница используется для определения того, сколько бит данных можно встроить в данную пару пикселей. Если разница значений между двумя пикселями достаточно велика, то можно скрыть больше бит информации, так как изменение разницы будет менее заметно.

**Шаги обработки изображения и вставки данных:**

1. Разделить изображение на блоки пикселей (например, пары).
2. Для каждой пары вычислить разницу их значений.
3. В зависимости от разницы, определить количество бит, которые можно встроить.
4. Модифицировать значения пикселей для встраивания данных.
5. Объединить все блоки в новое изображение.

Рассмотрим пример реализации метода PVD на языке программирования Python, код программы, который реализует данный метод, представлен в листинге 1.1.

from PIL import Image  
  
def embed\_message(image\_path, message):  
 image = Image.open(image\_path)  
 pixels = list(image.getdata())  
 message\_bits = ''.join(format(ord(char), '08b') for char in message)  
 bit\_index = 0  
  
 for i in range(0, len(pixels), 2):  
 if bit\_index >= len(message\_bits):  
 break  
  
 pixel1 = pixels[i]  
 pixel2 = pixels[i + 1]  
 brightness1 = sum(pixel1) // len(pixel1)  
 brightness2 = sum(pixel2) // len(pixel2)  
 diff = abs(brightness1 - brightness2)  
 if diff >= 16:  
 num\_bits\_to\_hide = 4  
 elif diff >= 8:  
 num\_bits\_to\_hide = 2  
 else:  
 num\_bits\_to\_hide = 1  
  
 if bit\_index + num\_bits\_to\_hide <= len(message\_bits):  
 data\_to\_hide = message\_bits[bit\_index:bit\_index + num\_bits\_to\_hide]  
 new\_pixel1 = tuple((channel & ~1) | int(data\_to\_hide[j], 2) if j < num\_bits\_to\_hide else channel  
 for j, channel in enumerate(pixel1))  
 new\_pixel2 = pixel2 # minimal adjustment to hide data  
 pixels[i] = new\_pixel1  
 pixels[i + 1] = new\_pixel2  
 bit\_index += num\_bits\_to\_hide  
  
 new\_image = Image.new(image.mode, image.size)  
 new\_image.putdata(pixels) new\_image.save("pikachu\_new.png")  
  
embed\_message("pikachu.png", "Secret text in photo")

Листинг 1.1 – Реализация метода PVD на языке Python

Результат выполнения программы показан на рисунке 1.1.

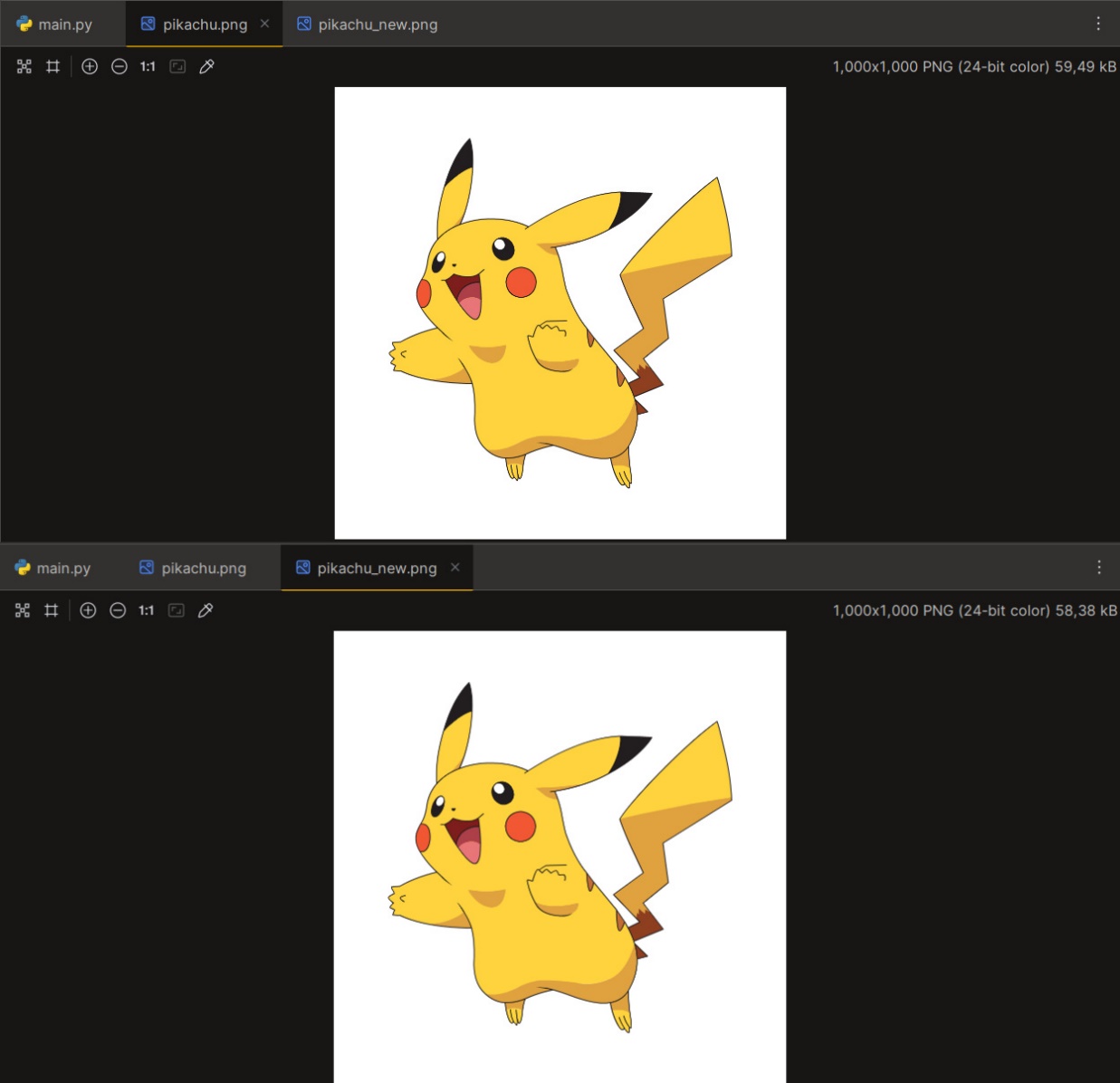


Рисунок 1.1 – Результат выполнения программы

Как можно видеть, размер картинки уменьшился, это связано с тем, что мы изменяем значение некоторых пикселей в изображении для встраивания сообщения. Каждый раз, когда мы модифицируем пиксель, мы потенциально изменяем его цветовые компоненты, и в некоторых случаях это может привести к уменьшению общей цветовой палитры, используемой в изображении.

## 1.2 Преимущества и недостатки метода PVD

Метод PVD (Pixel Value Differencing) представляет собой одну из инновационных техник цифровой стеганографии, направленных на сокрытие данных внутри изображений. Он работает на основе изменения разницы между соседними пикселями в изображении, что позволяет эффективно скрывать информацию, минимально влияя на визуальное восприятие изображения. Основная идея метода заключается в том, что человеческий глаз менее чувствителен к небольшим изменениям в яркости пикселей, особенно в областях с высокой текстурной сложностью, что позволяет незаметно встраивать данные.

К заметным преимущества такого метода можно отнести:

1. **Устойчивость к статистическому анализу:** Благодаря своей гибкости, этот метод обладает стойкостью к основным методам стеганографического анализа, таким как гистограммы, что затрудняет его обнаружение при анализе изображения.
2. **Адаптивность:** Метод адаптируется к местным особенностям изображения, что обеспечивает возможность внедрения большего объема информации в областях с высокой изменчивостью яркости или цвета, где такие изменения будут наиболее незаметны.
3. **Большая емкость:** По сравнению с предыдущими методами, такими как LSB (наименьший значащий бит), PVD позволяет встраивать гораздо больше информации, при этом качество изображения заметно не ухудшается.

Однако, у такого метода также есть и недостатки:

1. Потеря данных при сжатии. При применении данного метода и последующего использования сжатия, например, с использованием алгоритма JPEG, внедренная информация, изза изменений в значениях пикселей, имеет возможность частично или даже полностью быть утерянной.
2. Сложность реализации. Для вычисления необходимых интервалов и обработки пикселей, такой метод обязывает применение более сложных методов, что в дальнейшем увеличивает вычислительные затраты и может усложнить реализацию.
3. Уязвимость к современным методам стегоанализа. Хотя этот метод устойчив к традиционным методам стеганографического анализа, он может оказаться уязвимым перед современными методами, основанными на машинном обучении, такими как нейронные сети.

Можно сделать вывод, что метод PVD следует использовать, поскольку он устойчив к статистическому анализу, адаптируется к особенностям изображения, позволяя скрывать больше данных без заметного ухудшения качества. Однако его не рекомендуется применять, если возможно сжатие с потерями, так как данные могут быть утрачены, а также из-за сложности реализации и уязвимости перед современными методами стегоанализа.

## 1.3 Примеры применения метода PVD

Метод PVD применяется в различных областях, где требуется скрыть информацию в изображениях. Вот некоторые примеры:

1. **Защита авторских прав (рисунок 1.2):** Встраивание водяных знаков в изображения для защиты авторских прав — один из распространенных способов применения метода PVD. Водяной знак может содержать информацию об авторе, дате создания или идентификаторе, и эта информация остается незаметной для пользователей, но может быть извлечена в случае необходимости доказать авторство.

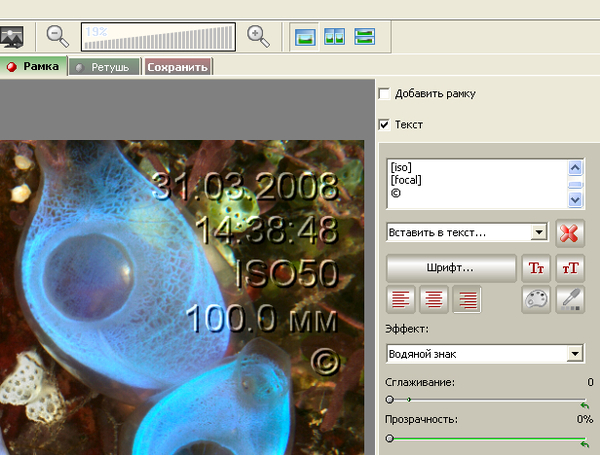


Рисунок 1.2 – Метод PVD в защите авторского права

1. **Безопасная передача данных:** PVD используется для сокрытия конфиденциальных данных в изображениях, которые передаются через интернет или хранятся на внешних носителях. Например, это может быть полезно для скрытия текстовых сообщений или зашифрованных данных в изображениях, отправляемых через незащищенные каналы связи.
2. **Медицинская стеганография (рисунок 1.3):** В медицинской сфере PVD применяется для встраивания дополнительной информации в медицинские изображения. Например, в рентгеновские снимки могут быть встроены данные о пациенте, диагноз или история болезни, что позволяет объединить визуальные данные и текстовые данные в одном файле.

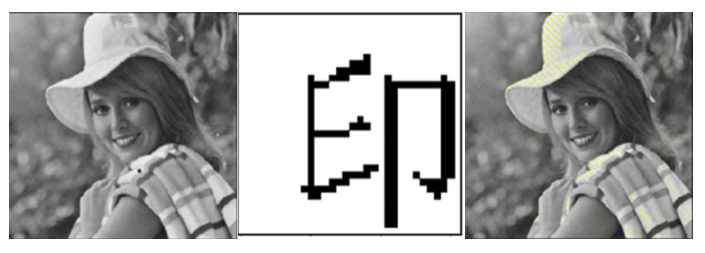


Рисунок 1.4 – Метод PVD в медицинской стеганографии

1. **Военные и разведывательные операции:** PVD используется для скрытой передачи данных в критически важных коммуникациях, таких как военные операции или разведывательные миссии. Это позволяет передавать важную информацию, оставаясь незамеченным для противников или злоумышленников.

Каждое из этих применений иллюстрирует, как метод PVD может служить инструментом для защиты интеллектуальной собственности, обеспечения приватности данных, улучшения медицинской диагностики и сохранения секретности в критически важных коммуникациях. С помощью этого метода возможно интегрировать дополнительные данные в изображения, не вызывая подозрений и сохраняя целостность оригинального контента.

## 1.4 Методы улучшения безопасности стегосистем на основе PVD

Несмотря на значительные преимущества метода PVD, для обеспечения более высокого уровня безопасности и скрытности данных существуют различные методы его улучшения. Одним из таких методов является использование криптографических алгоритмов перед встраиванием информации в изображение. Это обеспечивает дополнительный уровень защиты, так как даже если скрытая информация будет обнаружена, её расшифровка потребует значительных усилий.

Еще одним подходом является адаптивная стеганография. В данном случае алгоритм PVD применяется не ко всему изображению, а только к определенным областям, которые содержат высокую изменчивость яркости и цвета. Такие зоны менее подвержены вниманию и анализу, что делает внедренную информацию труднее обнаружимой. Адаптивные методы анализа изображения позволяют выбрать наиболее подходящие области для скрытия информации, уменьшая вероятность её визуального обнаружения.

Также для повышения безопасности можно использовать методы защиты от современных стегоаналитических атак, таких как анализ с применением машинного обучения и нейронных сетей. Например, для защиты от таких методов можно комбинировать PVD с другими стеганографическими техниками, создавая многослойные системы защиты, которые значительно усложняют процесс выявления скрытых данных.

Эти подходы позволяют повысить безопасность стеганографических систем на основе метода PVD, делая их более устойчивыми к различным атакам и анализу.

## 1.5 Альтернативы методу PVD

Несмотря на преимущества метода PVD, существуют и другие методы цифровой стеганографии, которые могут быть использованы в зависимости от конкретных требований:

1. **LSB (Least Significant Bit) — метод наименьшего значащего бита:** Один из самых популярных методов стеганографии, который заключается в замене младших битов каждого пикселя изображения на биты скрытых данных. Этот метод очень прост в реализации, но его основным недостатком является низкая устойчивость к сжатию и изменению изображения.
2. **DCT (Discrete Cosine Transform) — дискретное косинусное преобразование:** Используется в сжатии изображений формата JPEG. В этом методе данные скрываются в коэффициентах косинусного преобразования, что делает его более устойчивым к сжатию и визуальному обнаружению. Однако этот метод сложнее в реализации и требует большего объема вычислений.
3. **Метод спектрального домена:** В этом методе скрытые данные встраиваются в частотное представление изображения, что делает их менее заметными для человеческого глаза. Примером может быть применение в преобразовании Фурье или вейвлет-преобразовании. Этот метод обеспечивает высокую устойчивость к изменениям изображения, таким как сжатие или фильтрация, но также требует более сложных вычислений.
4. **Фазовая кодировка (Phase Coding):** Метод используется преимущественно для скрытия информации в аудиофайлах, однако может применяться и для изображений. Он заключается в изменении фазы сигнала для встраивания скрытых данных. Этот метод также обеспечивает высокий уровень защиты, но его реализация сложнее по сравнению с методами на основе пикселей.
5. **Метод цветовых каналов (Color Channel Manipulation):** Этот метод встраивает данные в различные цветовые каналы изображения (например, в RGB-каналы), что позволяет более эффективно скрывать информацию в изображениях с высокой цветовой сложностью. Однако метод также может быть заметен при детальном анализе цветовой структуры изображения.

Каждый из этих методов имеет свои уникальные преимущества и недостатки, которые могут быть определяющими в зависимости от конкретных требований и условий использования. Выбор метода стеганографии должен основываться на балансе между простотой реализации, устойчивостью к изменениям и требованиями к безопасности данных. В условиях быстрого развития технологий и растущей необходимости в защите информации, разнообразие методов стеганографии открывает новые возможности для разработки безопасных и надежных решений.

# Заключение

Метод PVD (Pixel-Value Differencing) представляет собой мощный инструмент цифровой стеганографии, который находит широкое применение в различных областях, от защиты авторских прав до обеспечения конфиденциальности данных. Его способность скрывать информацию, минимально влияя на визуальное восприятие изображений, делает его особенно ценным в условиях, когда сохранение целостности оригинального контента и незаметность скрытой информации играют ключевую роль.

Несмотря на его преимущества, таких как высокая емкость и устойчивость к традиционным методам анализа, метод PVD также сталкивается с определенными вызовами. Уязвимость к современным стегоаналитическим методам и потенциальные потери данных при сжатии требуют осторожного подхода к его использованию. Актуальность методов улучшения безопасности, таких как комбинирование PVD с криптографическими алгоритмами и адаптивная стеганография, подтверждает необходимость постоянного развития и адаптации стеганографических технологий в ответ на возникающие угрозы.

Таким образом, метод PVD демонстрирует высокую эффективность и многообещающие возможности в области цифровой стеганографии, однако его успешное применение зависит от тщательного выбора условий, в которых он будет использован, а также от внимания к актуальным угрозам и технологиям, способным повысить уровень защиты скрытой информации. В условиях непрерывного развития технологий и увеличения значимости конфиденциальности данных, дальнейшие исследования и разработки в области стеганографии остаются важными для обеспечения безопасности информации в цифровом пространстве.

# Список используемых источников

1. Steganography [Электронный ресурс] / Режим доступа: https://en.wikipedia.org/wiki/Steganography – Дата доступа: 30.09.2024.
2. List of steganography techniques [Электронный ресурс] / Режим доступа: https://en.wikipedia.org/wiki/List\_of\_steganography\_techniques – Дата доступа: 30.09.2024.
3. Методы внедрения информации в изображения [Электронный ресурс] / Режим доступа: https://rrinformation.ru/media/information/2024/2/%D0%98%D0%A2\_%D0%9D%D0%A0\_9\_2\_3.pdf – Дата доступа: 30.09.2024.
4. Multi-directional PVD steganography avoiding PDH and boundary issue [Электронный ресурс] – Режим доступа: https://www.sciencedirect.com/science/article/pii/S1319157821002949 – Дата доступа: 01.10.2024.