УДК 004.932.2 **DOI: 10.18413/2518-1092-2024-9-2-0-3**

Чурсин Д.С.

МЕТОДЫ ВНЕДРЕНИЯ КОНТРОЛЬНОЙ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯ

ООО «ЦЕНТРПРОГРАММСИСТЕМ»,
ул. Восточная, 71, Белгород, 308008, Россия

e-mail: dima.chursin@bk.ru

Аннотация
В работе рассматриваются различные методы стеганографии, используемые для внедрения контрольной информации в цифровые изображения. Основное внимание уделяется принципам работы, преимуществам и недостаткам каждого метода. Рассмотрены классические и современные методы, такие как LSB, FFT, PVD, MPVD, DCT, S-UNIWARD, WOW, HUGO и Steghide. Анализируются их устойчивость к стегоанализу, стеганографическая емкость и вычислительная сложность. Понимание этих методов позволяет повысить эффективность и безопасность использования стеганографических техник в различных практических задачах.
Ключевые слова: стеганография; стегоанализ; внедрение контрольной информации; цифровые изображения; защита данных; авторские права
Для цитирования: Чурсин Д.С. Методы внедрения контрольной информации в изображения // Научный результат. Информационные технологии. – Т.9, №2, 2024. С. 21-30. DOI: 10.18413/2518-1092-2024-9-2-0-3

Chursin D.S.

METHODS OF EMBEDDING CONTROL INFORMATION IN IMAGES

«CENTERPROGRAMSYSTEM» LLC,
71 Vostochnaya str., Belgorod, 308008, Russia

e-mail: dima.chursin@bk.ru

Abstract
The paper discusses various methods of steganography used to embed control information in digital images. The main focus is on the principles of operation, advantages and disadvantages of each method. Classical and modern methods such as LSD, FT, PVD, MPVD, DCT, S-UNIWARD, WOW, HUGO and Steghide are considered. Their resistance to steganalysis, steganographic capacity and computational complexity are analyzed. Understanding these methods makes it possible to increase the efficiency and safety of using steganographic techniques in various practical tasks.
Keywords: steganography; steganalysis; implementation of control information; digital images; data protection; copyright
For citation: Chursin D.S. Methods of embedding control information in images // Research result. Information technologies. – T.9, №2, 2024. – P. 21-30. DOI: 10.18413/2518-1092-2024-9-2-0-3

ВВЕДЕНИЕ

В эпоху цифровой трансформации и стремительного роста объемов данных, передача и хранение информации требуют все большего внимания к вопросам безопасности и защиты данных. Одним из наиболее эффективных и широко применяемых способов решения этих задач является внедрение контрольной информации в изображения. Этот процесс известен как стеганография [8] и представляет собой искусство и науку скрытия информации в цифровых мультимедийных файлах, тогда как стегоанализ направлен на выявление этой скрытой информации в файлах или сообщениях. Стеганография позволяет интегрировать дополнительные данные в цифровые изображения таким

образом, что это остается незаметным для человеческого глаза, но может быть извлечено и использовано при необходимости.

Методы стеганографии постоянно развиваются, адаптируясь к новым вызовам и требованиям. Современные подходы включают как классические методы, такие как Least Significant Bit (LSB) вставка, так и более сложные техники, использующие преобразования в частотной области, например, дискретное косинусное преобразование (DCT) или дискретное вейвлет-преобразование (DWT). Эти методы находят применение в различных областях, от защиты авторских прав до обеспечения конфиденциальности и целостности данных.

Цель данной статьи – рассмотреть основные методы внедрения контрольной информации в изображения, их принципы работы, преимущества и ограничения. Понимание этих аспектов позволит более эффективно использовать стеганографические техники в практических задачах, обеспечивая высокую степень защиты данных в цифровых изображениях.

LSB

Метод LSB (Least Significant Bit) [7] основан на замене младших битов пикселей изображения для внедрения битов скрываемого сообщения. В результате использования данного метода изменения настолько минимальны, что они не заметны для человеческого глаза.

Основные преимущества данного метода включают:

1. Надежность. Использование наименее значимого бита делает удаление информации невозможным без повреждения оригинального изображения.
2. Простота реализации и высокая скорость работы. Такой метод легко интегрируется в программное обеспечение и быстро выполняется.
3. Невидимость внедрения информации. Изменения, внесенные с помощью метода LSB, неразличимы невооруженным глазом.
4. Устойчивость к шумам. Такой метод дает возможность встраивать скрытую информацию в изображения, при этом существенно не уменьшая его качества.
5. Универсальность. Данный метод подходит для различных типов файлов, включая текстовые документы, аудио и видео.

Несмотря на достоинства, данный метод может быть обнаружен через анализ распределения наименее значимых битов. Следовательно, для сохранения конфиденциальности данных, важно использовать изображения, в которых изменения будут выделяться меньше всего. В качестве примера, на рисунке 1 показано использование такого метода.

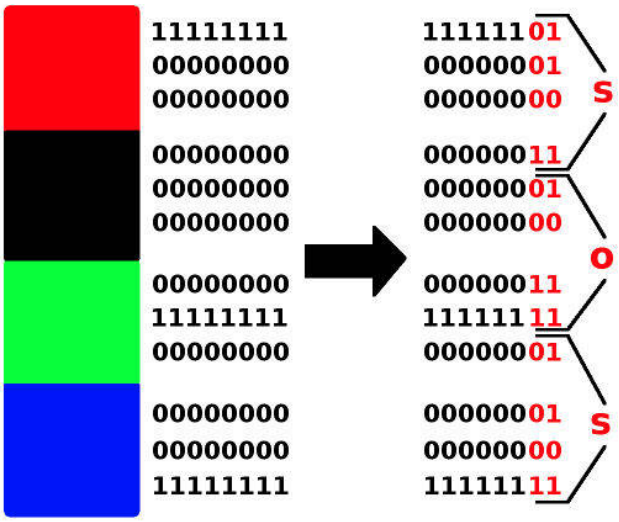

Рис. 1. Пример использование метода LSB для встраивания контрольной информации
Fig. 1. Example using the LSB method to embed control information

PVD

Метод PVD (Pixel Value Differencing) [10] в стеганографии – это один из методов внедрения скрытой информации в изображения. Он основан на изменении значений пикселей изображения с целью скрыть дополнительную информацию в них.

Основная идея данного метода заключается в том, чтобы изменять значения яркости (или цвета в случае цветных изображений) некоторых пикселей изображения на небольшие значения, которые могут быть использованы для кодирования скрытого бита информации. Эти изменения обычно незаметны для человеческого восприятия, особенно если скрываемая информация представляет собой небольшой объем данных.

К заметным преимущества такого метода можно отнести:

1. Устойчивость к статистическому анализу. Благодаря своей гибкости, такой метод обладает стойкостью к основным методам стеганографического анализа.
2. Адаптивность. Такой 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 большего всего не заметны.
3. Большая емкость. По сравнению с предыдущим методом (LSB), данный метод 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, из-за 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.

На рисунке 2 представлен пример использования данного метода и его сравнение с предыдущим методом (LSB) при классической атаке гистограммным анализом.

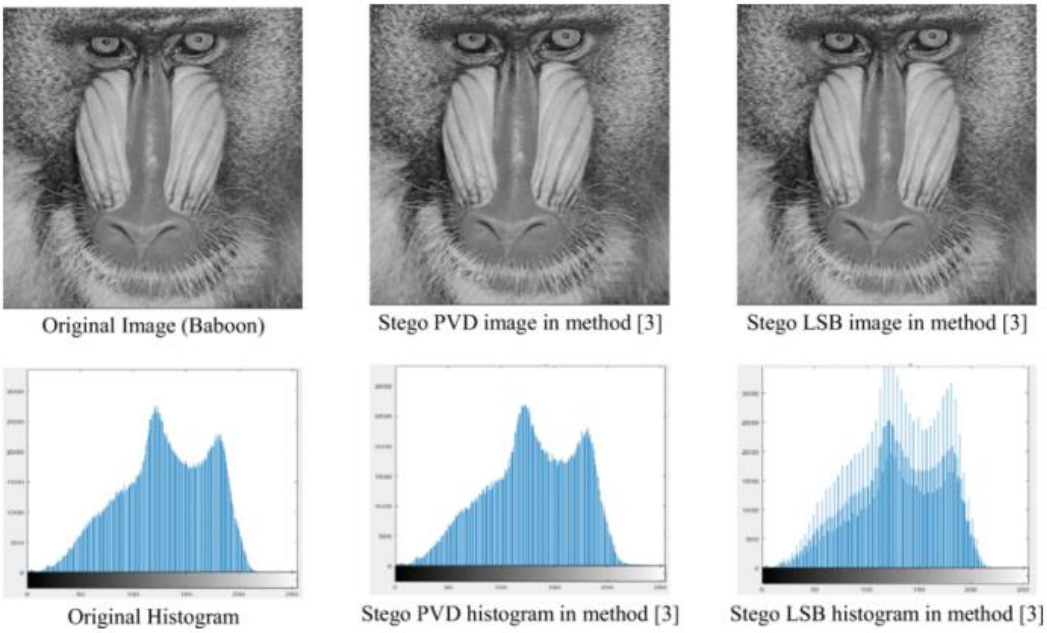

Рис. 2. Пример использования методов PVD и LSB, и сравнение их в устойчивости к гистограммному анализу

Fig. 2. An example of using PVD and LSB methods, and comparing them in resistance to histogram analysis

MPVD

Метод стеганографии MPVD (Modified Pixel Value Differencing) [2] в стеганографии является улучшенной версией метода PVD. Он представляет собой разновидность метода PVD, который стремится улучшить стойкость к атакам и вместимость скрываемой информации.

Основная идея метода MPVD также основана на изменении значений пикселей изображения, чтобы внедрить скрытую информацию. Однако, в отличие от метода PVD, который изменяет значения пикселей на фиксированные значения, метод MPVD использует адаптивный подход к определению величины изменения значения пикселя в зависимости от контекста.

Главные преимущества данного метода включают:

1. Устойчивость к статистическому анализу. Благодаря своей гибкости и сложности, такой метод, как и его предшественник (PVD), обладает стойкостью к основным методам стеганографического анализа.

2. Улучшенная адаптивность. Данный метод предоставляет более гибкую и адаптивную возможность внедрения информации, учитывая различные интервалы и комбинации соседних пикселей.

3. Более высокая емкость. По сравнению с предшественником (PVD), данный метод позволяет встраивать гораздо больше информации, без значительного ухудшения качества изображения.

При этом, данный метод имеет все те же недостатки, как и его предшественник, а именно: потеря данных при сжатии, сложность реализации и уязвимость к современным методам стеганографического анализа.

FFT

Метод FFT (Fast Fourier Transform) [6] в стеганографии внедряет скрытую информацию в изображения путем изменения значений яркости или цвета некоторых пикселей. Это достигается путем вычисления разницы между значениями выбранных пикселей и их соседей, где эта разница кодируется скрытыми битами информации. После внедрения информации изображение может быть восстановлено, и скрытая информация извлечена путем обратного вычисления разниц значений пикселей.

Главные преимущества данного метода включают:

1. Сложность обнаружения. Применение такого метода усложняет выявление скрытой информации основными методами стеганографического анализа.

2. Устойчивость к атакам. Поскольку информация встраивается в частотную область, она становится более устойчивой к шуму, изменению размера и сжатию изображений

3. Низкая видимость. Внедрение данных в частотную область делает стеганографические артефакты менее заметными в оригинальном изображении.

Главные недостатки такого метода:

1. Уязвимость к современным методам стегоанализа. Хотя этот метод устойчив к основным методам стеганографического анализа, он может оказаться уязвимым перед современными методами, основанными на машинном обучении, такими как нейронные сети

2. Вычислительная сложность. Данный метод требует значительных вычислительных ресурсов, увеличивая время обработки и затраты на реализации.

3. Ограниченная емкость. Внедрение информации в коэффициенты Фурье может искажать частотные характеристики изображения, что ограничивает объем скрываемых данных для сохранения качества изображения.

DCT

Метод DCT (Discrete Cosine Transform) [5] в стеганографии используется для внедрения скрытой информации в изображения путем манипуляции частотными компонентами. Этот метод основывается на преобразовании изображения из пространственной области в частотную область с помощью дискретного косинусного преобразования.

Процесс внедрения информации с использованием данного метода включает преобразование блоков пикселей изображения в частотное представление, где скрытая информация внедряется путем изменения коэффициентов низких или средних частот. Для сжатия и эффективного

внедрения информации используется алгоритм Хаффмана [4], который кодирует скрытые данные в наиболее часто встречающиеся коэффициенты. Затем блоки с измененными частотными компонентами обратно преобразуются в пространственную область с помощью обратного преобразования Фурье, создавая изображение с внедренной скрытой информацией.

К главным преимуществам такого метода относятся:

1. Низкая видимость. Изменения, внесенные в частотную область, делают следы стеганографии менее заметными на оригинальном изображении.

2. Устойчивость к атакам. Скрытая информация расположена в частотной области, которая менее подвержена к воздействиям в условиях различных атак, такими как сжатие, изменение размера и добавление шума.

3. Универсальность. Данный метод можно применять к любым типам файлов, что подчеркивает его как универсальный инструментом для внедрения контрольной информации.

4. Сложность обнаружения. Такой метод более устойчив и усложняет обнаружение внедренной информации при применении основных методов стеганографических анализов.

Однако, у данного метода можно выделить и ряд недостатков:

1. 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.

2. Вычислительная сложность: Данный метод требует значительных вычислительных ресурсов, увеличивая время обработки и затраты на реализации.

3. Ограниченная емкость. Встраивание данных в коэффициенты может исказить частотные особенности изображения, поэтому требуется ограничивать объем скрываемой информации, чтобы сохранить его качество.

На рисунке 3 изображена блок-схема реализации данного метода.

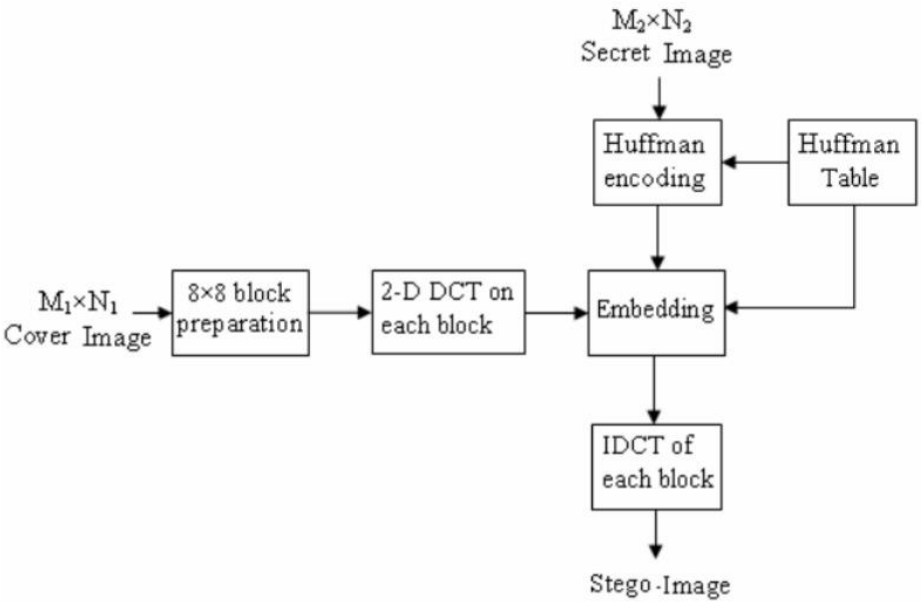

Рис. 3. Блок-схема DCT
Fig. 3. DCT Block Diagram

WOW

Метод WOW (Wavelet Obtained Weights) [9] является современным методом стеганографии и использует вейвлет-преобразование для анализа изображения на различные частотные составляющие и пространственные масштабы. После преобразования изображения выбираются определенные вейвлет-коэффициенты, в которые внедряется скрытая информация. Это достигается

путем изменения значений выбранных коэффициентов в соответствии со скрытыми битами данных. После манипуляций вейвлет-коэффициенты обратно преобразуются в пространственное представление, восстанавливая изображение с внедренной скрытой информацией. Этот метод позволяет эффективно внедрять информацию на разных уровнях детализации изображения, обеспечивая стеганографическую надежность.

Главные преимущества данного метода:

1. Устойчивость к атакам. Этот метод обеспечивает надежную защиту от разнообразных атак, включая передовые методы стегоанализа, основанные на машинном обучении.
2. Адаптивное внедрение. Этот метод модулирует процесс внедрения данных в зависимости от текстурных и частотных особенностей изображения, что приводит к сокрытию стеганографических артефактов и увеличению его емкости.
3. Низкая видимость. Затруднение обнаружения скрытой информации обусловлено использованием вейвлет-преобразования и весовых коэффициентов, что позволяет внедрять данные с минимальными искажениями исходного изображения.

Основные недостатки данного метода:

1. Сложность настройки параметров: Выбор оптимальных параметров для данного метода может быть сложным процессом, который требует глубоких знаний и опыта в области стеганографии.
2. Вычислительная сложность. В связи с использованием вейвлет-преобразования и адаптивного внедрения данных, данный метод требует значительных вычислительных ресурсов, что может привести к увеличению времени обработки и затрат на его реализацию.

S-UNIWARD

Метод S-UNIWARD (Spatial Universal Wavelet Relative Distortion) [9] является современным методом стеганографии, который использует вейвлет-преобразование для внедрения скрытой информации в изображения. Он основан на идее минимизации визуальных изменений в изображении после внедрения, чтобы скрытая информация была как можно менее заметной.

В процессе внедрения информации с использованием данного метода, изображение преобразуется в вейвлет-пространство, где осуществляется анализ его пространственных и частотных характеристик. Затем выбираются определенные коэффициенты вейвлета, в которые будет внедрена скрытая информация. Этот метод учитывает чувствительность человеческого зрения к изменениям в изображении и стремится минимизировать визуальные артефакты путем внедрения информации в те коэффициенты, которые приводят к наименьшим изменениям в изображении.

К главным преимуществам такого метода относятся:

1. Устойчивость к атакам. Этот метод обеспечивает надежную защиту от разнообразных атак, включая передовые методы стегоанализа, основанные на машинном обучении.
2. Универсальность. Данный метод можно применять к любым типам файлов, что подчеркивает его как универсальный инструментом для внедрения контрольной информации.
3. Низкая видимость. Благодаря адаптивному изменению коэффициентов вейвлетов, данный метод минимизирует видимость стеганографических артефактов, что значительно осложняет обнаружение внедренной информации.
4. Высокая емкость. Оптимизация внедрения данных в данном методе обеспечивает высокую емкость без существенного изменения качества изображения

Основные недостатки данного метода:

1. Сложность настройки параметров. Выбор подходящих параметров и оптимизация относительного искажения в данном методе могут быть сложными задачами, требующими глубоких знаний и опыта в области стеганографии.
2. Вычислительная сложность. Использование вейвлетной модели и оптимизация относительного искажения требуют значительных вычислительных ресурсов, что может увеличить время обработки и затраты на реализацию.

Рисунок 4 демонстрирует иллюстрацию процесса функционирования данного метода.

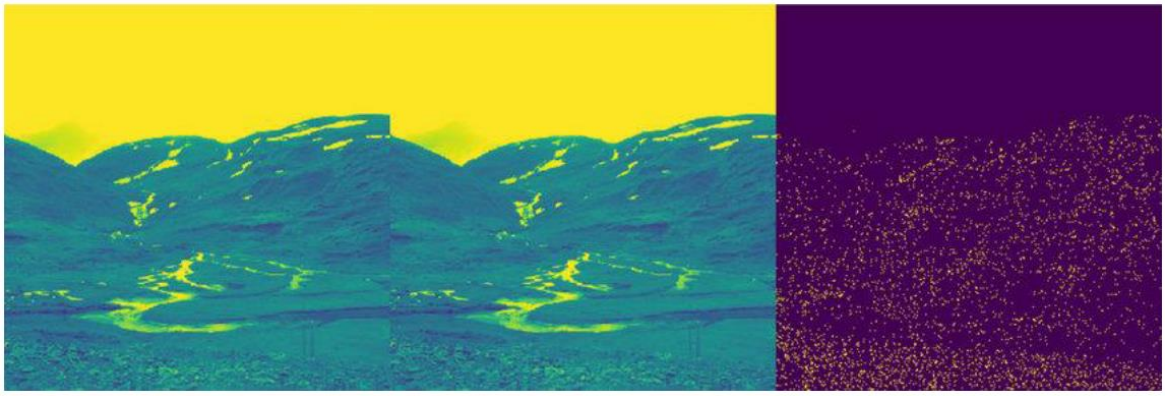

Рис. 4. Пример реализации метода
Fig. 4. An example of the method implementation

HUGO

Метод стеганографии HUGO (Highly Undetectable stego-GRaphy for Content-Adaptive Networks) [9] является современным методом стеганографии для внедрения скрытой информации в изображения с целью сохранения высокой невидимости изменений и стойкости к атакам. Этот метод основан на использовании искусственных нейронных сетей для определения оптимального способа внедрения информации, который минимизирует визуальные изменения в изображении.

В процессе внедрения информации с использованием данного метода, изображение анализируется с помощью нейронной сети, которая определяет оптимальные места и способы внедрения скрытой информации. Это позволяет адаптировать процесс внедрения к содержанию и структуре конкретного изображения, обеспечивая максимальную невидимость внесенных изменений.

К главным преимуществам данного метода относятся:

1. Устойчивость к атакам. Этот метод обеспечивает надежную защиту от разнообразных атак, включая передовые методы стегоанализа, основанные на машинном обучении.

2. Адаптивность к содержимому. Путём адаптации к характеристикам конкретного изображения, данный метод способствует снижению заметности стеганографических артефактов, а также повышению общей стеганографической емкости.

3. Низкая видимость. Затруднение обнаружения скрытой информации обусловлено использованием метода оптимизации графов, который позволяет внедрять данные с минимальными искажениями исходного изображения.

К главным недостаткам данного метода относятся:

1. Сложность настройки параметров: Выбор подходящих параметров и оптимизация относительного искажения в данном методе могут быть сложными задачами, требующими глубоких знаний и опыта в области стеганографии.

2. Вычислительная сложность. Использование метода оптимизации графов и адаптивного внедрения данных делает данный метод вычислительно сложным, что приводит к увеличению времени обработки и затрат на его реализацию.

Steghide

Steghide [1] представляет собой программное обеспечение, специализирующееся на внедрении скрытой информации в различные мультимедийные файлы, включая изображения. Уникальный алгоритм стеганографии, используемый в данном методе, объединяет теорию графов, сжатие данных и криптографию.

Процесс внедрения контрольной информации включает следующие этапы:

1. Сжатие и шифрование внедряемой информации на основе кодирования Хаффмана и алгоритма Rijndael с ключом длиной 128 бит.

2. Генерация последовательности позиций пикселей в контейнерном файле на основе генератора псевдослучайных чисел, инициализируемого паролем.

3. Выбор позиций, значения которых не требуют изменения, поскольку они случайно совпадают с вычисленными значениями.

4. Применение алгоритма сопоставления из теории графов для нахождения пар позиций, обмен значениями которых позволяет внедрить контрольную информацию.

5. Завершение фазы обменов, когда не удается найти больше подходящих пар.

6. Модификация оставшихся пикселей, не ставших частями пар, путем перезаписи для внедрения данных.

Обмен значениями пикселей, который позволяет сохранить статистическое распределение цветов в файле-контейнере, составляет основную идею этого метода.

К главным преимуществам данного метода относятся:

1. Простота и удобство использования. Программное обеспечение с данным методом часто предустановлен в некоторых дистрибутивах Linux, таких как Kali Linux [3], что подразумевает его доступность и удобность даже для использования новичкам.

2. Сжатие и криптография. Повышение безопасности внедренной информации достигается с помощью сжатия данных через кодирование Хаффмана и криптографии на основе паролей.

Недостатки данного метода:

1. Ограниченная поддержка форматов. Ограниченный набор поддерживаемых типов медиафайлов может сократить область применения данного метода.

2. Уязвимость к обнаружению. Хотя этот метод устойчив к традиционным методам стеганографического анализа, он может оказаться уязвимым перед современными методами, основанными на машинном обучении, такими как нейронные сети.

3. Низкая емкость. Данный метод имеет ограниченную емкость в отличии от других современных и сложных методов.

ЗАКЛЮЧЕНИЕ

Обзор различных методов стеганографии для внедрения информации в изображения дает возможность сделать следующие выводы:

1. Уникальные характеристики каждого метода: каждый метод обладает уникальными особенностями и принципами встраивания информации в изображения.

2. Степень скрытности и устойчивость к атакам: разные методы имеют разную степень заметности внедренной информации и устойчивости к различным видам атак, таким как статистический анализ, обработка изображений и сжатие.

3. Вместимость и качество изображений: вместимость для скрытой информации и сохранение качества изображения также различаются в зависимости от метода. Некоторые методы обеспечивают большую вместимость, но могут повлиять на качество изображения.

4. Целевые области применения: каждый метод может находить свое применение в различных областях, таких как конфиденциальная передача данных, медицинская стеганография, цифровая подпись и другие.

5. Необходимость компромиссов: ни один метод не обладает идеальными характеристиками. При выборе метода часто приходится искать компромиссы между вместимостью, стойкостью к атакам и визуальной незаметностью внедренной информации.

6. Анализ показал, что каждый метод стеганографии имеет свои уникальные преимущества и ограничения. Оптимальный выбор метода зависит от конкретных требований проекта или задачи, а также уровня угроз безопасности и желаемой степени скрытности информации. Важно учитывать, что эффективное применение стеганографии требует адекватного баланса между скрытностью внедренной информации, ее устойчивостью к обнаружению и сохранением качества изображения.

Также анализ методов стеганографии в изображениях открывает перспективы для развития исследований в этой области, предлагая ряд направлений для дальнейших исследований:

1. Развитие устойчивых к атакам методов: требуется разработка более устойчивых к различным видам атак методов стеганографии. Важным направлением является работа над методами, способными обеспечить высокую скрытность внедренной информации при минимальном воздействии на качество изображения.

2. Увеличение вместимости и сохранение качества изображений: дальнейшие исследования могут сосредоточиться на повышении емкости для скрытой информации в изображениях, не ухудшая их качества. Разработка методов, позволяющих увеличить емкость при сохранении визуальной целостности изображений, представляет собой важную задачу.

3. Исследование новых подходов стеганографии: исследование и разработка новых подходов, основанных на комбинации существующих методов или использовании новых техник, таких как машинное обучение, глубокие нейронные сети и квантовая стеганография, могут открыть новые перспективы для стеганографии в изображениях.

4. Исследование робастности методов: исследование робастности методов стеганографии к различным условиям и искажениям изображений является важным направлением. Развитие методов, способных поддерживать высокую эффективность при различных условиях съемки, сжатия, изменения размеров и других факторах, является актуальной задачей.

5. Применение в реальных областях: исследования, направленные на применение методов стеганографии в реальных областях, таких как медицина, финансы, правоохранительная деятельность и информационная безопасность, позволят определить специфические требования и эффективность методов в конкретных сценариях.

Таким образом, дальнейшие исследования в области стеганографии в изображениях обещают развитие новых методов и технологий, способных обеспечить более высокий уровень скрытности, устойчивость к атакам и сохранение качества изображений. Разнообразие сфер применения стеганографии предоставляет широкий спектр возможностей для развития и улучшения существующих методов.

Список литературы

1. Denemark T., Fridrich J., Holub V. Further study on the security of S-UNIWARD // SPIE Proceedings. – 2014. DOI: 10.1117/12.2044803.

2. Gajjala R. R., Banchhor S., Abdelmoniem A. M., Dutta A., Canini M., Kalnis P. Huffman Coding Based Encoding Techniques for Fast Distributed Deep Learning // Proceedings of the 1st Workshop on Distributed Machine Learning. – 2020. DOI: 10.1145/3426745.3431334.

3. Kali Linux [Electronic resource]. – URL: https://www.kali.org/ (date of application: 01.06.2024).

4. Negi L., Negi L. Image Steganography Using Steg with AES and LSB // 2021 IEEE 7th International Conference on Computing, Engineering and Design (ICCED). – 2021. – DOI: 10.1109/icced53389.2021.9664834.

5. Patel H., Dave P. Steganography technique based on DCT coefficients // International Journal of Engineering Research and Applications. – 2012. – Vol. 2, no. 1. – p. 713-717.

6. Rabie T. Digital Image Steganography: An FFT Approach // Communications in Computer and Information Science. – 2012. – 294 P. DOI: 10.1007/978-3-642-30567-2_18.

7. Rojali, Siahaan I., Soewito B. Steganography algorithm multi pixel value differencing (MPVD) to increase message capacity and data security // AIP Conference Proceedings. – 2017. – 1867. – 020035. DOI: 10.1063/1.4994438.

8. Steghide [Electronic resource]. – URL: https://github.com/StefanoDeVuono/steghide (date of application: 01.06.2024).

9. Sumathi C., Santanam T., Umamaheswari G. A study of various steganographic techniques used for information hiding // arXiv. – 2014. – arXiv:1401.5561.

10. Zhang H., Zhang T., Chen H. Revisiting weighted Stego-image Steganalysis for PVD steganography // Multimedia Tools and Applications. – 2018. – Vol. 78, No. 6. – P. 7479-7497. DOI: 10.1007/s11042-018-6473-8.

References

1. Denemark T., Fridrich J., Holub V. Further study on the security of S-UNIWARD // SPIE Proceedings. – 2014. DOI: 10.1117/12.2044803.
2. Gajjala R. R., Banchhor S., Abdelmoniem A. M., Dutta A., Canini M., Kalnis P. Huffman Coding Based Encoding Techniques for Fast Distributed Deep Learning // Proceedings of the 1st Workshop on Distributed Machine Learning. – 2020. DOI: 10.1145/3426745.3431334.
3. Kali Linux [Electronic resource]. – URL: https://www.kali.org/ (date of application: 01.06.2024).
4. Negi L., Negi L. Image Steganography Using Steg with AES and LSB // 2021 IEEE 7th International Conference on Computing, Engineering and Design (ICCED). – 2021. – DOI: 10.1109/icced53389.2021.9664834.
5. Patel H., Dave P. Steganography technique based on DCT coefficients // International Journal of Engineering Research and Applications. – 2012. – Vol. 2, no. 1. – p. 713-717.
6. Rabie T. Digital Image Steganography: An FFT Approach // Communications in Computer and Information Science. – 2012. – 294 P. DOI: 10.1007/978-3-642-30567-2_18.
7. Rojali, Siahaan I., Soewito B. Steganography algorithm multi pixel value differencing (MPVD) to increase message capacity and data security // AIP Conference Proceedings. – 2017. – 1867. – 020035. DOI: 10.1063/1.4994438.
8. Steghide [Electronic resource]. – URL: https://github.com/StefanoDeVuono/steghide (date of application: 01.06.2024).
9. Sumathi C., Santanam T., Umamaheswari G. A study of various steganographic techniques used for information hiding // arXiv. – 2014. – arXiv:1401.5561.
10. Zhang H., Zhang T., Chen H. Revisiting weighted Stego-image Steganalysis for PVD steganography // Multimedia Tools and Applications. – 2018. – Vol. 78, No. 6. – P. 7479-7497. DOI: 10.1007/s11042-018-6473-8.

Чурсин Дмитрий Сергеевич, специалист по внедрению программных продуктов ООО «ЦЕНТРПРОГРАММСИСТЕМ», аспирант кафедры информационно-телекоммуникационных систем и технологий НИУ «БелГУ»

Chursin Dmitry Sergeevich, Specialist in the Implementation of Software Products of «CENTROPROGRAMSYSTEM» LLC, postgraduate student of the Department of Information and Telecommunication Systems and Technologies of the National Research University "BelSU"