Гудимов Виктор Николаевич,
Студент 2 курса магистратуры,
ФГБОУ ВО «АмГУ»

СТЕГОАЛИЗ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Цель исследования – систематизация методов стегоанализа цифровых изображений в задачах информационной безопасности. Сопоставлены статистические, признаковые и нейросетевые подходы, рассмотрена роль GAN в подготовке обучающих примеров и ограничения применения методов. Обнаружение скрытых данных не устанавливает вредоносность содержимого.

Ключевые слова: Стегоанализ, цифровые изображения, скрытые данные, машинное обучение, генеративно-состязательные сети, GAN.

Введение

Цифровые изображения могут выступать контейнерами скрытых данных. Для информационной безопасности существенны риски несанкционированной передачи сведений через разрешённые каналы и доставки скрытых компонентов вредоносного программного обеспечения. Примеры таких угроз и подходы к их выявлению рассматриваются В. Г. Сидоренко и Я. Л. Грачевым [1].

В обзоре сопоставляются способы формирования признаков, зависимость методов от данных и ограничения обнаружения. Материалом служат научные публикации 2025 года.

Принципы скрытого встраивания и задачи обнаружения

Стеганография направлена на сокрытие факта передачи сообщения, тогда как шифрование защищает его содержание. При встраивании используются исходный контейнер, сообщение, алгоритм и, если это предусмотрено схемой, ключ. Результатом становится стегоконтейнер. Извлечение восстанавливает последовательность данных при наличии необходимых параметров; последующее расшифрование представляет отдельную операцию [2].

В пространственной области могут изменяться наименее значащие биты значений пикселей. Для изображений JPEG применяются методы, изменяющие коэффициенты дискретного косинусного преобразования (DCT). Визуальная малозаметность изменений не гарантирует сохранения статистических свойств контейнера. Поэтому область встраивания и характеристики исходного изображения необходимо учитывать при выборе признаков обнаружения [1, 2].

Скрытое встраивание используется и в легитимных целях, включая маркировку контента. Цифровые водяные знаки относятся к смежному направлению, ориентированному на сохранение и проверку маркировки. Наличие скрытого сообщения требует оценки контекста передачи и не подтверждает вредоносность содержимого.

Стегоанализ исследует признаки встраивания и не предполагает обязательного восстановления сообщения. При зашифрованной нагрузке анализ также направлен на изменения контейнера; определение шифра является отдельной задачей. Для выполнения скрытого кода требуется механизм извлечения и запуска: хранение изображения само по себе не означает исполнения данных.

Статистические и нейросетевые методы стегоанализа

Статистические методы оценивают распределения значений и зависимости между элементами изображения. Критерий хи-квадрат и RS-анализ применяются к признакам, связанным с изменением наименее значащих битов. Их выводы необходимо соотносить с

проверяемой схемой встраивания. В исследовании Я. Л. Грачева и В. Г. Сидоренко изучается связь качества изображения с ошибками анализа контейнеров без скрытых данных [3].

В признаковых моделях рассчитанные характеристики поступают на вход классификатора. Например, Д. Д. Скалдин и А. В. Шевченко используют признаки DCT-коэффициентов, межблочных разностей и шума совместно с полносвязной нейронной сетью [2]. Полученное решение относится к рассмотренному способу встраивания и не подтверждает универсальность выбранных признаков.

Свёрточные детекторы обучают представления по данным изображений. Исследуются SRNet, Xu-Net и другие архитектуры, включая их устойчивость к сжатию, изменению размера и шуму [4]. Обычное редактирование также меняет характеристики контейнера, поэтому визуальные искажения не служат достаточным признаком встраивания.

Подходы сопоставлены в таблице 1 по способу формирования признаков и условиям применения.

Таблица 1

Сопоставление подходов к стегоанализу

Подход	**Основание решения**	**Условие применения**
Статистические тесты	Распределения значений и зависимости	Соответствие признаков способу встраивания
Классификация по признакам	Заранее рассчитанные характеристики	Обоснование состава признаков и выборки
Свёрточные детекторы	Обучаемые представления изображения	Проверка на новых источниках данных

Роль GAN в стегоанализе

GAN объединяет генератор и дискриминатор, обучаемые в условиях противоборства. В классической постановке генератор формирует синтетические данные, а дискриминатор различает реальные и сгенерированные объекты [5]. Для стегоанализа постановка меняется: необходимо различать контейнеры без сообщения и изображения со встроенными данными. Обычный дискриминатор генерации изображений не становится стегоанализатором без соответствующих примеров и цели обучения.

В состязательной стеганографии генеративный компонент подбирает изменения контейнера с учётом реакции детектора. Примером является применение UT-GAN для адаптивного встраивания в JPEG-изображения [6]. Такие исследования ориентированы на скрытность передачи. С защитной позиции их можно рассматривать как основу формирования контролируемых сложных примеров для обучения и проверки стегоанализатора.

GAN представляет способ обучения, который может сочетаться со свёрточным детектором. Его применение не гарантирует повышения качества: требуется сравнение с обучением без GAN при одинаковых условиях. Проверка должна охватывать разные способы встраивания и новые источники изображений. При анализе файлов может использоваться только обученный детектор.

Условия применения в информационной безопасности

Результат обзора показывает, что выбор подхода требует согласования формата изображения, области встраивания и состава данных. Для обучаемых методов следует раздельно учитывать исходные контейнеры, стегоизображения и изображения со следами обычной обработки. Проверка на новых источниках необходима для определения границ применимости, а воздействие преобразований рассматривается отдельно [3, 4].

В контролируемом обмене файлами результат стегоанализа используется для выделения подозрительных объектов. Дополнительная проверка может включать

независимый стегоанализ, антивирусные средства и изучение происхождения файла. Ошибки чтения не должны интерпретироваться как отсутствие скрытых данных. Практическая оценка детектора должна учитывать доли пропусков и ложных срабатываний, время анализа и объём последующей проверки.

Заключение

Систематизированы методы стегоанализа изображений и условия их защитного применения. GAN рассматривается как механизм состязательной подготовки примеров для детектора. Проверка на представительных данных определяет границы применимости подхода. Результат анализа служит основанием для дополнительного исследования подозрительных файлов.

Список литературы:

1. Сидоренко В. Г., Грачев Я. Л. Противодействие угрозам информационной безопасности, связанным с применением средств стеганографии // Автоматика, связь, информатика. 2025. № 1. С. 17–22. DOI: 10.62994/AT.2025.1.1.004.

2. Скалдин Д. Д., Шевченко А. В. Разработка аналитического программного комплекса по детектированию стеганографических сообщений в графических изображениях с применением объяснительного искусственного интеллекта // Системный анализ в науке и образовании. 2025. № 4. С. 9–23. EDN: KRFRGW.

3. Грачев Я. Л., Сидоренко В. Г. Использование качественных характеристик изображения для комплексного стегоанализа // Надежность. 2025. Т. 25, № 1. С. 67–74. DOI: 10.21683/1729-2646-2025-25-1-67-74.

4. Alrusaini O. A. Deep learning for steganalysis: evaluating model robustness against image transformations // Frontiers in Artificial Intelligence. 2025. Vol. 8. Article 1532895. DOI: 10.3389/frai.2025.1532895.

5. Катаев А. В., Власова Ю. М., Ким В. А., Гусынин Д. А. Сравнительный анализ современных методов генерации изображений: VAE, GAN и диффузионные модели // Инженерный вестник Дона. 2025. № 5. URL: https://www.ivdon.ru/ru/magazine/archive/n5y2025/10060 (дата обращения: 14.10.2026).

6. Tan L., Li Y., Zeng Y., Chen P. An Adaptive JPEG Steganography Algorithm Based on the UT-GAN Model // Electronics. 2025. Vol. 14, no. 20. Article 4046. DOI: 10.3390/electronics14204046.