УДК 004.896:614.8

РЕАЛИЗАЦИЯ КОМПЛЕКСНОГО СТАТИСТИЧЕСКОГО СТЕГОДЕТЕКТОРА В РАМКАХ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ

СИДОРЕНКО Валентина Геннадьевна, д-р техн. наук, профессор, профессор кафедры; e-mail: valenfalk@mail.ru
ГРАЧЕВ Ярослав Леонидович, аспирант; e-mail: yaroslav446@mail.ru

Российский университет транспорта, кафедра «Управление и защита информации», Москва

В статье рассмотрен вопрос разработки комплексного статистического стегодетектора и его внедрения в модуль анализа достоверности графических данных автоматизированных систем управления технологическими процессами и интеллектуальных транспортных систем для проверки подлинности и подтверждения достоверности циркулирующих в этих системах графических данных, поступающих от средств технического зрения и иных средств фотофиксации и фотосенсоров, и повышения надежности функционирования систем. Разработанный программный стегодетектор реализован в форме сервера API, что позволяет интегрировать его в рассматриваемые системы и в автоматическом режиме осуществлять стеганографический анализ с формированием бинарного вывода о наличии либо отсутствии встроенных данных в анализируемых файлах изображений. Разработанный стегодетектор представлен программным комплексом StegoRevealer, зарегистрированным в Роспатенте, который демонстрирует возможности стегоанализа на тестовом стенде с производительностью 656 гигафлопс: изображение с разрешением около 1,2 мегапикселя обрабатывается за 300 мс. Комплекс также эффективно обрабатывает до 100 поступающих запросов одновременно. При этом на тестовом стенде сервер способен выдерживать нагрузку до 10 запросов в секунду (*RPS*) с 2 % деградации производительности. Это позволяет осуществлять стегоанализ изображений в режиме, близком к режиму реального времени, особенно при использовании современного серверного микропроцессорного оборудования.

Ключевые слова: стегоанализ; стеганография; стегодетектор; изображения; автоматизированные системы.

DOI: 10.20295/2412-9186-2025-11-03-226-238

▼ Введение

Работа современных автоматизированных систем управления технологическими процессами (АСУ ТП) и интеллектуальных транспортных систем (ИТС) связана с использованием средств технического зрения для визуального мониторинга и фотофиксации. В этой связи в данных системах, как правило, присутствует циркуляция графической информации в форме файлов изображений, получаемых с камер и сенсоров. Они возникают, в частности, в рамках:

- систем дистанционного видеоконтроля при движении вагонами вперед (в блоках индикации, где графические данные передаются по радиоканалу с камер машинисту) [1];
- систем определения препятствий [2];
- систем дистанционного наблюдения (в частности, визуального контроля за свободностью пути, диагностики дефектов пути и т. п.) [3, 4];
- бортовых систем тягового подвижного состава, работающих, например, в рамках пилотных проектов на Московском центральном кольце и обеспечивающих автоматическую передачу ограничений скорости, в том числе при обнаружении препятствий, расшифровке знаков и сигналов [5];
- подсистемы интеллектуального коммерческого осмотра поездов и вагонов, которая использует средства технического зрения для осуществления фотодиагностики при осмотре состояния вагонов, контейнеров и грузов [6];
- интеллектуальных систем обнаружения нарушений в соблюдении требований безопасности при работах на объектах железнодорожной инфраструктуры [7];
- модулей Цифровой железнодорожной станции, где файлы графических данных могут быть частью информации, циркулирующей

в модуле электронного документооборота, модуле автоматизированной диагностики технического состояния и коммерческих неисправностей, а также в других модулях, использующих средства технического зрения для автоматического управления работой станции [8, 9].

Угроза наличия несанкционированных скрытых данных или их повреждения в файлах изображений, циркулирующих в подсистемах сбора и обработки данных АСУ ТП и ИТС, повышает вероятность принятия ложных управляющих решений, особенно при формировании сигналов в автоматическом режиме.

Целью работы является автоматизация стегоанализа путем создания программного комплекса для АСУ ТП и ИТС, обеспечивающего достоверность и аутентичность графической информации. Для достижения цели решены следующие задачи:

- определение задач автоматизации стегоанализа;
- выбор автоматизируемой методики осуществления стегоанализа изображений;
- разработка схемы интеграции стегодетектора в АСУ ТП и ИТС;
- проектирование и программная реализация стегодетектора;
- тестирование разработанного стегодетектора.

1. Обзор проблемы

В настоящее время стеганография является перспективным средством обеспечения защищенных и надежных каналов связи в рамках ИТС [10]. Помимо уже существующих и активно развивающихся направлений, связанных с использованием цифровых водяных знаков (ЦВЗ) [11, 12] на основе стеганографии, ведется также разработка систем стеганографической передачи изображений между транспортными средствами и инфраструктурой [10, 13].

При этом рост популярности стеганографии как средства обеспечения надежных и защищенных каналов передачи данных сказывается также и на росте инцидентов информационной безопасности, связанной со встраиванием данных в файлы изображений [14]. Цифровые системы транспорта все чаще сталкиваются со злоумышленным применением стеганографии в файлах изображений [15, 16], что ведет к нарушению подлинности и достоверности графических данных, циркулирующих в системе.

Так как ИТС являются объектами критической информационной инфраструктуры, циркулирующие в них данные передаются по защищенным каналам связи. Существуют решения, нацеленные на предотвращение возможности интегрирования вредоносного программного обеспечения в управляющие программы на стадии разработки — например, за счет применения технологии *Security-by-Design* [17].

Тем не менее ИТС регулярно подвергаются кибератакам на узлы подсистем технического зрения, сбора и обработки графических данных. Зачастую атакам подвергаются камеры [18, 19], что позволяет злоумышленникам осуществлять подмену или модификацию графических данных. Подобные инциденты представляют угрозу для любых систем, использующих средства технического зрения, например — комплексов контроля скорости [20]. Уязвимости могут возникать в разных узлах и на различных этапах работы систем сбора, передачи и обработки графической информации, что позволяет подменять, обрезать и иным образом модифицировать визуальные данные [21].

Таким образом, возникает необходимость в разработке средств независимого (от уже используемых средств работы со стеганографией или проверки достоверности) контроля за наличием стеганографически встроенных в файлы изображений данных в целях обеспечения надежности АСУ ТП и ИТС.

2. Обеспечение достоверности графических данных

Задача обеспечения надежности АСУ ТП включает поддержание аутентичности (подлинности[1]) и анализ достоверности графических данных в подсистемах сбора, хранения и обработки информации. В рамках систем железнодорожного транспорта такие данные могут поступать от бортовых систем в

[1] ГОСТР 43.0.26—2022. Информационное обеспечение техники и операторской деятельности. Качество информации в технической деятельности.

информационные системы ОАО «РЖД», где происходит накопление и сохранение диагностических и эксплуатационных данных [8].

Комплексная программа развития ОАО «РЖД» ставит соответствующие задачи обеспечения надежности и безопасности в рамках цифровизации транспортной инфраструктуры [22]. Аналогичные требования устанавливаются и для других ИТС и АСУ ТП, особенно связанных с отраслями, объектами и производствами, отнесенными к перечню объектов критической информационной инфраструктуры[2].

Применительно к файлам изображений важную роль в обеспечении достоверности и подлинности может играть стеганография. В этой связи можно выделить два основных аспекта, не исключающих друг друга:

1. Злоумышленное использование стеганографии, приводящее к нарушению подлинности и/или достоверности графической информации.

2. Использование стеганографии для установки ЦВЗ в целях подтверждения подлинности файлов изображений и предотвращения возможных нарушений или искажений (как случайных, так и умышленных), приводящих к невозможности корректной интерпретации ЦВЗ.

В обоих случаях решение возникающих проблем требует применения средств стеганографического анализа. Слепые методы стегоанализа позволяют идентифицировать стеганографическое встраивание на основе исследования лишь самого файла изображения без использования дополнительных входных данных. Это позволяет:

1. Обнаруживать несанкционированное применение стеганографии в файлах изображений.

2. Быстро проверять наличие либо отсутствие встроенной информации в случае ее ожидания (например, не пытаться извлекать встроенный ЦВЗ, если он отсутствует, и идентифицировать проблему подтверждения подлинности файла на основе ЦВЗ как возникающую из-за отсутствия ЦВЗ как такового, а не его повреждения или нарушения протоколов встраивания и извлечения данных).

3. Осуществлять проверку отсутствия стеганографического встраивания, в том числе:
- проверять устойчивость к анализу и необнаруживаемость используемых стеганографических алгоритмов (например, используемых для установки ЦВЗ);
- разделять следование графических данных по разным каналам передачи данных при необходимости отправки их на различные конвейеры обработки в зависимости от наличия или отсутствия встроенной информации (в данном случае независимо от целей использования стеганографии).

Таким образом, методы стегоанализа должны применяться в системах, связанных с обработкой графической информации и реализующих функционал технического зрения, совместно с методами стеганографии или для потенциального противодействия ее использованию.

Отдельную проблему может представлять использование нейросетевых технологий для осуществления фотодиагностики [6] в связи с появлением различного рода адверсариальных атак [23, 24], способных за счет незначительных преднамеренных искажений нарушать корректную работу распознающих моделей, построенных на основе искусственных нейросетей и других методов машинного обучения.

Передача недостоверных графических данных в упомянутых системах может вести к формированию некорректных выводов и ошибкам, непосредственно ухудшающим надежность и безопасность функционирующих автоматизированных систем. Достоверность данных — в том числе графических — на основе которых выполняются оценки и принимаются решения, является базовым фактором, определяющим эффективность формирования управляющих сигналов.

3. Особенности реализации автоматизированного стегоанализа в рамках ИТС

Реализация автоматизированного стегоанализа в рамках ИТС требует формального выделения задач автоматизации стегоанализа

[2] ГОСТ 24.701—86. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения.

с целью обеспечения возможности внедрения стегоаналитического детектора изображений в ИТС [25]. Ключевыми являются две задачи:

1. Обеспечение автоматизации процессов стегоанализа и вычисления дополнительных характеристик — в частности, оценок качества изображений.

2. Возможность осуществления автоматизированного анализа графических данных — то есть предоставление программного или аппаратно-программного интерфейса для запуска анализа и получения в результате стегоаналитического вывода (в бинарной форме («встраивание обнаружено» / «встраивание не обнаружено») и/или в виде числовой оценки вероятности наличия встроенной информации).

Рассмотрим варианты решения первой задачи.

В связи с наличием угроз адверсариальных атак (и, возможно, схожих с ними непреднамеренных искажений, также способных нарушать работу модулей нейросетевой фотодиагностики) затруднительным выглядит использование нейросетевых методов стегоанализа: помимо прочих проблем, они могут быть крайне чувствительны к такого рода искажениям [26]. С точки зрения надежности автоматизированной системы приоритет следует отдавать более «стабильным» методам стегоанализа. Они в меньшей степени подвержены резкому снижению точности при искажениях во входных данных и универсальны в обнаружении непредусмотренных видов встраивания. Хотя их точность при анализе известных методов стеганографии ниже, чем у нейросетевых, зато они нацелены на обнаружение конкретных данных.

Этим условиям отвечает стегоаналитический подход с применением «богатых моделей» признаков, бинарных классификаторов и ансамблевых моделей [26–29].

Для обнаружения наиболее частого типа стеганографии в пространственной области (значения цветовой интенсивности пикселей) предлагается методика комплексного статистического стегоанализа. Она основана на совместном применении методов *Chi-Square Attack* (*CSA*) и *Regular-Singular* (*RS*), а также учете оценок качества изображения в бинарном классификаторе на основе модели случайного леса [29].

В соответствии с классификацией, представленной в [30], методы *CSA* и *RS* являются слепыми, не требуют для своей работы иных данных, кроме непосредственно файла графического формата, задействуют статистический аппарат и не предполагают использование процедур машинного обучения.

Методика комплексного статистического стегоанализа основана на формировании совместного вывода согласно оценкам относительного объема скрытой информации, полученным с применением методов *CSA* и *RS*.

В рамках метода *CSA* анализируется статистика *pair of values* (*PoV*) — пар из двух байт цветовой интенсивности, которые между собой отличаются на один наименее значащий бит (НЗБ) [31]. В незаполненном стегоконтейнере вероятность одновременного появления обоих значений каждой *PoV* мала, поэтому частоты значений одной пары существенно различаются. Таким образом, применение стеганографии приближает значение каждой из частот пары к их среднему арифметическому в рамках *PoV*. Для оценки существенности приближения частот пар значений к их средним значениям используется критерий Хи-квадрат.

Метод *Regular-Singular* (*RS*) основан на анализе небольших непересекающихся групп смежных пикселей и их подсчете [32]. Для классификации этих групп по трем категориям — обычные, необычные и непригодные — осуществляется вычисление функции регулярности для оригинальной и перевернутой группы (переворот эмулирует добавление обратимого шума, уменьшая регулярность группы) по выбранной маске и инвертированной версии этой же маски.

Таким образом, подсчитываются четыре ключевых значения: R_M — относительное количество обычных групп (доля от общего количества групп) для обычной маски, S_M — относительное количество необычных групп для обычной маски, R_{-M} — относительное количество обычных групп для инвертированной маски, S_{-M} — относительное количество необычных групп для инвертированной маски. Метод *RS* основывается на утверждении, что в

незаполненном стегоконтейнере количества групп одного класса для обычной и инвертированной маски должны быть равны: $R_M \approx R_{-M}$ и $S_M \approx S_{-M}$ [32].

Первый метод точнее при анализе последовательного встраивания в НЗБ пикселей, второй — при псевдослучайном. Их совместное применение дает более точную оценку, чем использование каждого метода по отдельности [33].

Помимо этого, созданная авторами методика использует ряд дополнительных оценок и параметров изображения в целях повышения итоговой точности результата — в особенности при небольших значениях относительного объема встроенных данных. Для этого используются:

- оценка стегоанализа потенциального встраивания по методу Коха — Жао, снижающая влияние статистических аномалий в частотной области изображения на точность метода *RS*;
- суммарное количество пикселей изображения, влияющее на точность статистических методов стегоанализа в связи с тем, что именно значения интенсивности цвета пикселей изображения составляют набор данных, к которому применяются методы математической статистики и теории вероятности.

Ключевой особенностью методики комплексного статистического стегоанализа является учет абсолютных количественных оценок качества изображения: зашумленности, резкости, размытости, контраста и энтропии. Традиционные статистические методы стегоанализа чувствительны к визуальному качеству изображений. Учет этих оценок увеличивает точность стегоанализа (особенно для низкокачественных изображений) и снижает вероятность ложноположительных результатов.

Это важно при анализе изображений систем технического зрения, где съемка может вестись в движении (что вызывает размытость), в плохую погоду, при недостаточной освещенности или переэкспозиции. Все это влияет на контрастность и оценку энтропии.

В этой связи именно предлагаемая методика оценивается как рекомендуемая для осуществления стегоанализа изображений в условиях возможного наличия изображений низкого качества — в частности, в модулях анализа достоверности графических данных в системах АСУ ТП и ИТС.

Для формирования окончательного вывода о наличии либо отсутствии стеганографического встраивания в изображении в рамках методики комплексного статистического стегоанализа используются методы машинного обучения: а именно обученная модель бинарной классификации на основе алгоритма случайного леса [29]. Ее точность на тестовых выборках (изображения разного качества и разрешения со встраиванием в НЗБ и пустыми стегоконтейнерами) составляет 95,9 % при анализе изображений с одним НЗБ и 95,7 % — с двумя НЗБ.

В рамках конкретного внедрения в те или иные АСУ ТП или ИТС данные, используемые для обучения модели, могут быть уточнены на основе массивов реальных накопленных в таких системах графических данных с целью увеличения эффективности стегоанализа для конкретных автоматизированных систем.

Решение второй задачи представляет собой стандартный подход в виде развертывания прикладного программного интерфейса (*API*) — например, в форме развертывания сервера *API*, который будет принимать стегоаналитические запросы и возвращать запрашивающей системе или пользователю требуемый, соответствующий поставленной задаче машинно-интерпретируемый результат.

Данный интерфейс основан на клиент-серверной архитектуре, где сервером выступает *API*, инициирующий по запросу от клиента осуществление стегоаналитической процедуры. Так как отсутствует необходимость хранения информации о состоянии клиентов между запросами, разумной является реализация такого сервера *API* с применением архитектурного стиля *REST*, соответствие которому отвечает возможностям повышения надежности, производительности и масштабируемости [34].

Таким образом, решение обеих задач — это программный комплекс с функцией детектирования стеганографии, или стегодетектор.

Схема интеграции такого стегодетектора в АСУ ТП или ИТС представлена на рис. 1.

В качестве реализации методики комплексного статистического стегоанализа был

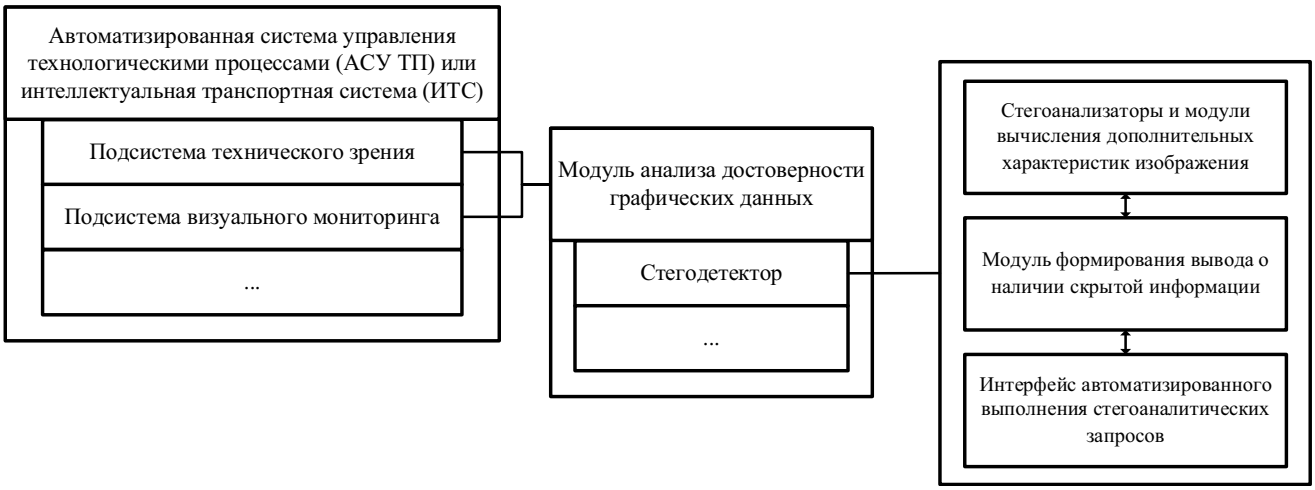

Рис. 1. Схема интеграции стегодетектора в АСУ ТП или ИТС

разработан программный стегодетектирующий комплекс StegoRevealer, зарегистрированный в Роспатенте [35].

4. Программный стегодетектирующий комплекс StegoRevealer

Разработанный программный комплекс имеет несколько форм взаимодействия с ним — интерфейсов. Ключевым в рамках решения поставленных задач автоматизации выполнения стеганографического анализа является интерфейс взаимодействия посредством сервера *API*: развертывание данного сервера позволяет осуществлять в автоматизированном режиме запросы на выполнение стегоанализа изображения и получать бинарный ответ — вывод о наличии либо отсутствии встроенной информации согласно результату работы реализованного алгоритма методики комплексного статистического стегоанализа.

Помимо этого, предоставляются и два интерфейса ручного взаимодействия с программным комплексом — консольный (*CLI*) и графический (*GUI*) (рис. 2). Это необходимо для поддержки возможности выполнения стегоаналитических операций аналитиком или оператором системы в случае возникновения инцидентов или спорных ситуаций, в рамках которых именно оператор должен принять то или иное управляющее решение — в том числе на основе выводов о достоверности учитываемой графической информации.

CLI- и GUI-интерфейсы обеспечивают возможность ручного выполнения стегоанализа как в системах без графического интерфейса, так и с ним.

В рамках программной реализации необходима выработка решений по ряду ключевых вопросов:

1. Выбор языка программирования и фреймворков, ключевых библиотек.
2. Выбор архитектурных паттернов.

В рамках разработки комплекса StegoRevealer используются:

- язык программирования *C#* и среда *.NET 9.0*;
- *UI*-фреймворк *Avalonia* и архитектура *MVVM*;
- *API*-фреймворк *ASP.NET* и архитектура *MVC*.

Выбор языка, среды и фреймворков в первую очередь обуславливался возможностями кроссплатформенной разработки и развертывания приложения на операционных системах как семейства *Windows*, так и *Linux* для возможности использования программного обеспечения в рамках современных отечественных систем (реализующих программы импортозамещения и имеющих сертификаты Минцифры) — таких как *Astra Linux*, *Red OS*, *Alt*. Выбранный технологический стек позволил вести разработку универсальным способом, практически не прибегая к ветвлению и вызовам различных функций и операторов в зависимости от операционной системы. Большинство различий в реализации уже инкапсулированы внутри используемых фреймворков и среды *.NET*.

На рис. 3 представлена архитектурная схема основных компонентов разработанного программного комплекса.

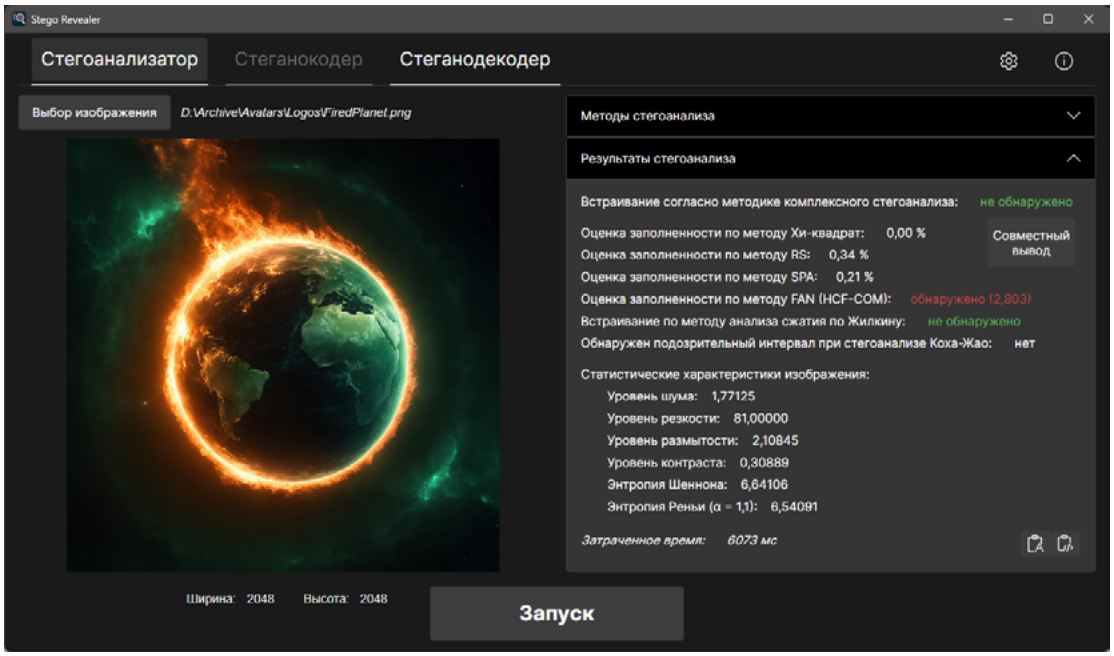

Рис. 2. Скриншот *GUI*-интерфейса программы

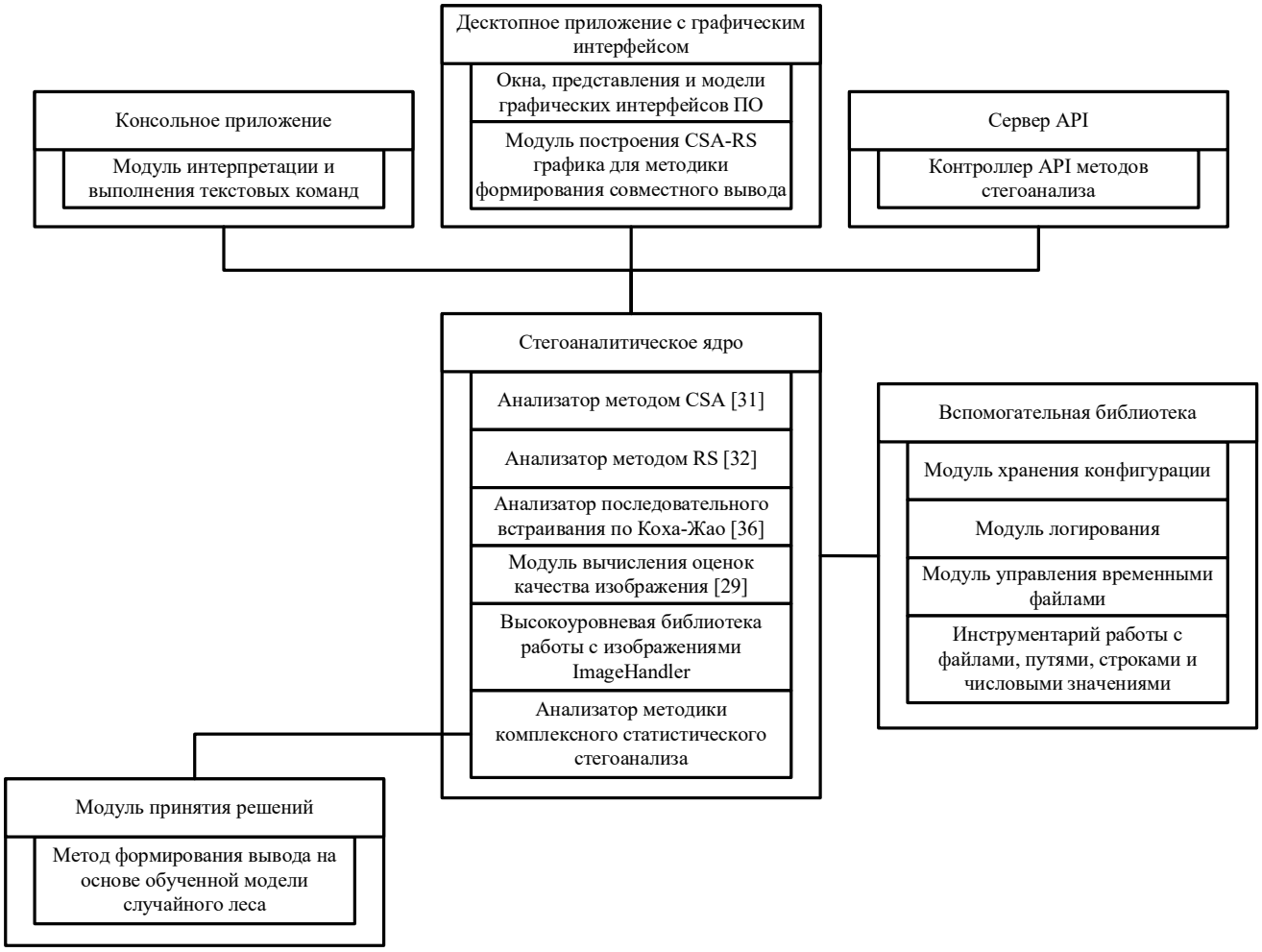

Рис. 3. Архитектурная схема организации модулей StegoRevealer

Точность работы стегодетектора определяется модулем принятия решений — то есть результатами использования методики комплексного статистического стегоанализа, точностью обученного бинарного классификатора на основе модели случайного леса [37]. Вторым по важности ключевым фактором оценки применимости стегодетектора следует считать скорость стегоанализа файлов изображений, что соответствует адекватности решения задачи выполнения автоматизированного анализа трафика в системе. Слишком долгое выполнение стегоаналитических операций будет приводить к существенным задержкам на этапе анализа достоверности и, соответственно, общему увеличению задержек передачи информации в системе.

Так как в рамках АСУ ТП первоочередной является эффективность и скорость работы стегодетектора, развернутого в форме сервера *API*, было выполнено тестирование скорости работы данного компонента. Тестирование производилось на макете, представляющем собой два персональных компьютера (стенда), связанных по локальной сети со скоростью не менее 1 Гбит/с. Стенд, на котором было выполнено развертывание сервера *API* StegoRevealer, обладает процессором с производительностью около 656 Гигафлопс (при точности *FP32*) и 20 логическими потоками. Так как осуществленная реализация стегодетектора использует именно процессорные вычисления для выполнения алгоритмов, производительность центрального процессора является ключевым фактором, определяющим быстродействие.

В рамках тестирования было выполнено несколько тестовых испытаний.

Первое включало в себя последовательный стегоанализ 2642 файлов изображений различного разрешения, как включающих встроенные данные, так и являющиеся пустыми контейнерами. Общее время выполнения составило 799,99 с, среднее арифметическое время выполнения одного стегоаналитического запроса — 302,75 мс.

Второе испытание было направлено на проверку быстродействия при параллельном выполнении стегоаналитических запросов. Для одинаковой по составу выборки из 1000 изображений формировалось и направлялось к стенду с сервером *API* различное количество одновременных запросов. После отправки запросов ожидались все ответы, после чего направлялась следующая группа запросов. Таким образом была осуществлена фактически пакетная обработка всего тестового набора. Результаты испытания приведены в табл. 1.

Таблица 1. Испытание быстродействия сервера *API* при различном числе одновременно отправленных запросов

Количество параллельных запросов	Среднее время выполнения одного запроса, мс	Суммарное время анализа тестируемого набора изображений, с
1	264,99	265,29
2	360,49	180,5
5	683,67	137,16
10	1 300,09	130,78
100	11 223,4	118,79
1000	94 096,96	171,72

Таблица 2. Результаты нагрузочного тестирования

$RPS_ц$	$RPS_ф$	e, %	Средняя нагрузка на процессор, %
1	1	0	5,69
5	5	0	9,99
10	9,8	2	26,49
20	18,9	5,5	63,45
50	43,2	13,6	78,49
100	82,4	17,6	78,38
200	143,3	28,35	78,29
500	256,3	48,74	79,13
1000	410,7	58,93	79,59

Заметно, что при тестировании до 100 запросов включительно эффективность растет — суммарное время анализа всей выборки уменьшается, однако при выполнении одновременно 1000 запросов производительность сервера *API* начинает деградировать.

В рамках третьего тестового испытания было организовано нагрузочное тестирование сервера с различными целевыми значениями запросов в секунду (*RPS*). Такой вид тестирования подразумевает направление определенного количества

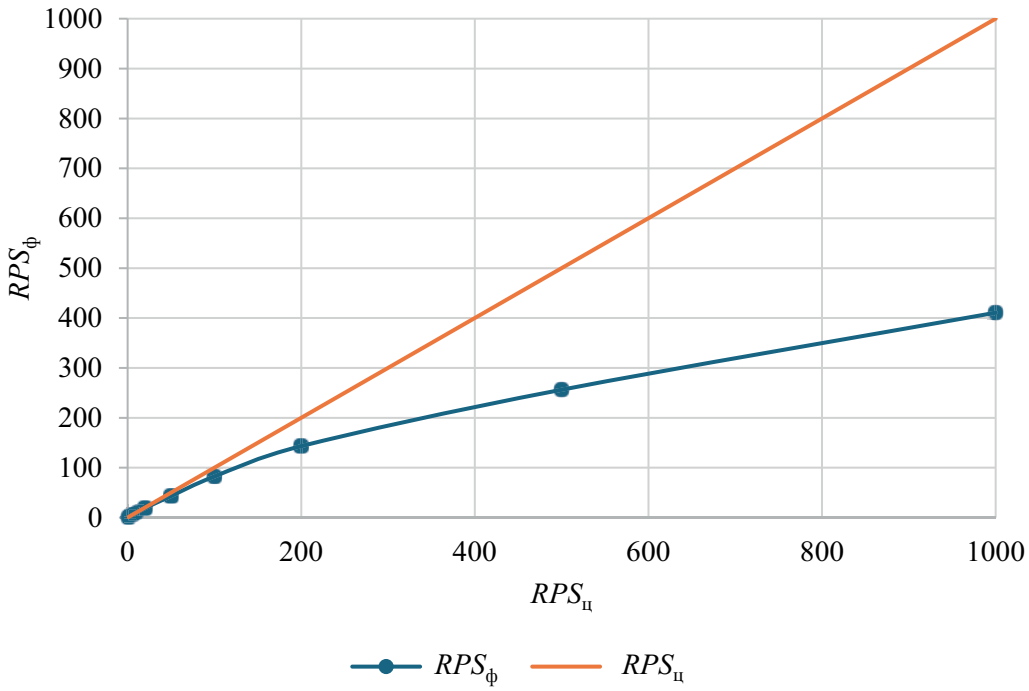

Рис. 4. График *RPS* при нагрузочном тестировании

запросов обработки в секунду вне зависимости от скорости их выполнения. Для каждого *RPS* была вычислена степень деградации производительности, отражающая относительную величину падения фактического *RPS* по сравнению с целевым:

$$e = 100\left(1 - \frac{RPS_ф}{RPS_ц}\right), \quad (1)$$

где e — степень деградации (относительная величина падения фактического *RPS* в %);

$RPS_ф$ — фактическое значение *RPS*;

$RPS_ц$ — целевое значение *RPS*.

В табл. 2 представлены результаты тестового испытания, на рис. 4 — график зависимости между целевым и фактическим значением *RPS*.

В ходе всех трех проведенных испытаний значение пиковой нагрузки на центральный процессор при осуществлении стегоанализа составляло 100 % рабочего времени. Как видно из результатов нагрузочного тестирования, в среднем это значение составляет почти 80 %. Это отражает достаточно высокую эффективность использованных методов многопоточной реализации алгоритмов стегоанализа, позволяющих в полной мере задействовать все доступные ядра и логические потоки процессора, исключая редкие логические ситуации вынужденного ожидания (например, ожидания завершения вычисления всех оценок методами стегоанализа и оценок качества изображения перед выполнением процедуры формирования итогового вывода — в этом случае время выполнения параллельных операций определяется временем выполнения самого долгого из методов; или в рамках алгоритма стегоанализа методом *CSA*, где выполняется обход строк матрицы пикселей последовательно с учетом значений всех предыдущих строк).

Для оценки быстродействия стегодетектора при анализе изображений конкретных размеров (имеющих практическую значимость с точки зрения применения в реальных системах технического зрения) были выполнены аналогичные первым двум испытаниям тесты на выборке, состоящей из изображений одинакового разрешения. Для выборки использован датасет [38], состоящий из графических файлов размера 1280 × 960, то есть с общим разрешением в 1,23 мегапикселя. Выбор подобного разрешения в целях тестирования обусловлен наличием требований к источникам видеосигнала в рамках технических средств обеспечения транспортной безопасности, согласно которым разрешение кадра должно составлять

не менее 1200 × 1000 пикселей, то есть не менее 1,2 мегапикселя[3].

Выполнение последовательного стегоанализа на вышеописанной выборке из 8570 изображений составило 2568 с в сумме и 299,75 мс в среднем на изображение. Продолжительность стегоанализа всей выборки при пакетной отправке по 10 запросов одновременно составила 214 с, при отправке по 100 запросов — 200 с, при этом средняя нагрузка на центральный процессор составляла 88,76 и 86,27 % рабочего времени соответственно. Таким образом, при отправке параллельно по 100 запросов для данной выборки среднее арифметическое времени обработки на одно изображение составило около 43 с (данное значение синтетическое и не отражает реально затраченного времени на анализ одного изображения (что демонстрировалось первым тестом) ввиду распределения нагрузки во время простоев и ожиданий на выполнение операций для параллельно обрабатываемых изображений).

При пакетной отправке на обработку одновременно по 200 запросов ранее продемонстрированная деградация производительности (около 30 %) уже начала оказывать существенное влияние на общее время работы: суммарное время выполнения составило 522 с.

Аналогичные тесты были выполнены для выборки из 2096 изображений из датасета [39] с разрешением 1920 × 1080 (свыше 2 мегапикселей), которые являются распространенным разрешением съемки камер — например, изображения такого размера снимаются блоками индикации мобильных блоков видеоконтроля, используемых на поездах для передачи изображений машинисту. Для них время стегоанализа одного изображения составило в среднем 495 мс, при этом последовательный стегоанализ составил в сумме 1038 с, а анализ пакетами по 100 одновременных запросов — 128 с.

Заключение

Современные серверные процессоры имеют производительность при вычислениях с плавающей точкой (*FP*32) на уровне 2 Терафлопс и более, что превышает производительность процессора использованного тестового стенда более чем в 3 и раза. Поскольку стегодетектор выполняет вычисления только с помощью процессора, а большинство операций — это вычисления с плавающей точкой *FP*32, при широком использовании многопоточности можно предположить, что на современном серверном оборудовании StegoRevealer выдержит нагрузку 25–30 *RPS* без потери производительности. Это подтверждается тестированием: при целевом значении 10 *RPS* деградация составила 2 %. Дальнейшее увеличение производительности может достигаться за счет установки балансировщиков нагрузки и распределения стегоаналитических запросов между несколькими копиями стегодетектора, развернутыми параллельно на нескольких серверах.

Для применяемых в настоящее время систем технического зрения характерна частота кадров не менее 15 кадров в секунду. Таким образом, имеющаяся у разработанного программного стегодетектора производительность при использовании в реальных производительных системах, предназначенных для обработки графических данных от систем технического зрения, позволяет осуществлять стегоанализ поступающих изображений в режиме реального времени при съемке с частотой 15–25 кадров в секунду, что соответствует техническим характеристикам камер, используемых в таких системах.

Стегодетектор StegoRevealer реализует разработанную авторами методику комплексного статистического стегоанализа, основанную на совместном применении ряда традиционных статистических стегоаналитических методов. При использовании бинарной классификации для формирования вывода точность (*precision*) стегодетектора на тестовых выборках составляет 96 %, правильность (*accuracy*) — 95 % при анализе встраивания в 1 НЗБ и 92 % при анализе встраивания в 2 НЗБ.

Разработанный программный комплекс StegoRevealer внедрен в процесс обучения студентов кафедры «Управление и защита информации» РУТ (МИИТ) в 2022 году. Использование его студентами при решении стегоаналитических задач позволило

[3] Постановление Правительства Российской Федерации от 26 сентября 2016 г. № 969.

осуществить его апробацию при выполнении анализа изображений через графический интерфейс в ручном режиме (эмулируя действия стегоаналитика — специалиста или оператора, которому требуется осуществить проверку подозрительного файла графического формата). Поскольку и графический интерфейс, и *API* комплекса используют одно и то же программное ядро для выполнения стегоаналитических операции, успешное использование комплекса студентами в образовательных целях подтверждает корректность работы реализации выбранных методов и методики комплексного статистического стегоанализа.

Благодарности

Работа выполнена за счет бюджетного финансирования в рамках государственного задания от 20.03.2025 № 103-00001-25-02. ▲

Список источников

1. Александров Е. А. Система дистанционного видеоконтроля при движении вагонами вперед / Е. А. Александров // Железные дороги мира. — 2025. — № 4. — С. 48–50.
2. Патент на полезную модель № 212718 U1 Российская Федерация, МПК B61L 29/00. Устройство обнаружения препятствий на пути движения рельсового транспортного средства: № 2022111729: заявл. 28.04.2022: опубл. 03.08.2022 / И. А. Дейлид, И. Н. Королев, С. В. Кудряшов, П. А. Попов; заявитель ОАО «РЖД».
3. Малинский С. В. Автоматическое определение границ опасных участков железнодорожного пути / С. В. Малинский, А. В. Абрамов, В. О. Шарова // Интеллектуальные транспортные системы : материалы IV Междунар. науч.-практ. конф., Москва, 22 мая 2025 г. — М.: РУТ (МИИТ), 2025. — С. 624–630.
4. Патент № 2680927 C1 Российская Федерация, МПК B61K 9/08, G01N 27/82, G01N 29/04. Способ диагностики рельсового пути и синхронизации результатов измерений: № 2018104776: заявл. 07.02.2018: опубл. 28.02.2019 / А. А. Марков, А. Г. Антипов, А. Ю. Веревкин; заявитель ОАО «Радиоавионика».
5. Розенберг Е. Н. Актуальность и этапы перехода на интеллектуальное управление эксплуатационной работой железнодорожного транспорта / Е. Н. Розенберг, М. А. Дежков, А. А. Никонюк // Интеллектуальные транспортные системы: материалы IV Междунар. науч.-практ. конф., Москва, 22 мая 2025 г. — М.: РУТ (МИИТ), 2025. — С. 369–375.
6. Нутович В. Е. Формализованные методы обработки информации, анализа и синтеза системы интеллектуального коммерческого осмотра вагонов / В. Е. Нутович // Наука и техника транспорта. — 2023. — № 3. — С. 77–85.
7. Сидоренко В. Г. Интеллектуальная система обнаружения нарушений в соблюдении требований безопасности при работах на объектах железнодорожной инфраструктуры / В. Г. Сидоренко, М. А. Кулагин, Д. М. Родина // Автоматика на транспорте. — 2025. — Т. 11. — № 1. — С. 55–65.
8. Андреев В. Е. Цифровая железнодорожная станция — от концепции к реальному внедрению / В. Е. Андреев, А. И. Долгий, В. В. Кудюкин и др. // Автоматика, связь, информатика. — 2023. — № 9. — С. 2–6.
9. Кудюкин В. В. Имитационное моделирование работы робототехнических комплексов, предназначенных для расформирования составов на сортировочных горках / В. В. Кудюкин, А. В. Вуколов, В. С. Кузьмин // Автоматика на транспорте. — 2025. — Т. 11. — № 1. — С. 16–29.
10. Ansari A. S. A Review on the Recent Trends of Image Steganography for VANET Applications / A. S. Ansari // Computers, Materials and Continua. — 2024. — Vol. 78. — Iss. 3. — Pp. 2865–2892.
11. Shedole S. M. A Comprehensive Study on Digital Watermarking for Security Threats and Research Directions / S. M. Shedole, V. Santhi // International Journal of Data Informatics and Intelligent Computing. — 2025. — Vol. 4. — Iss. 1. — Pp. 54–72.
12. Hu K. Learning-based image steganography and watermarking: A survey / K. Hu, M. Wang, X. Ma, J. Chen // Expert Systems with Applications. — 2024. — Iss. 249.
13. Hahn D. Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges / D. Hahn, A. Munir, V. Behzadan // IEEE Intelligent Transportation Systems Magazine. — 2021. — Vol. 13. — Iss. 1. — Pp. 181–196.
14. Сидоренко В. Г. Противодействие угрозам информационной безопасности, связанным с применением средств стеганографии / В. Г. Сидоренко, Я. Л. Грачев // Автоматика, связь, информатика. — 2025. — № 1. — С. 17–22.
15. Security Brief: Actor Uses Compromised Accounts, Customized Social Engineering to Target Transport and Logistics Firms with Malware. — URL: https://www.proofpoint.com/us/blog/threat-insight/security-brief-actor-uses-compromised-accounts-customized-social-engineering (дата обращения: 28.09.2024).
16. Sea-Tac Airport officials confirm cyberattack disrupted service, websites. — URL: https://www.seattletimes.com/business/sea-tac-airport-officials-say-cyberattack-disrupted-service-websites/ (дата обращения: 29.09.2024).
17. Матюшин А. Кибериммунный подход к проектированию как практическая реализация концепции Security-by-Design / А. Матюшин, Е. Рудина // CONNECT. Мир информационных технологий. — 2023. — № 7–8. — С. 38–44.
18. Anonymous hacked Russian cams, websites, announced a clamorous leak. — URL: https://securityaffairs.com/128847/hacktivism/anonymous-vs-russia.html (дата обращения: 16.08.2025).
19. Самый беззащитный — уже не Сапсан. Все оказалось куда хуже… — URL: https://habr.com/ru/articles/536750/ (дата обращения: 13.08.2025).
20. Cyberattack on Dutch prosecution service is keeping speed cameras offline. — URL: https://www.theregister.com/2025/08/15/cyberattack_on_dutch_prosecution_service/ (дата обращения: 15.08.2025).

21. Vulnerabilities in Johnson Controls' exacqVision Web Service Expose Security Systems to Video-Stream Hijacking. — URL: https://www.nozominetworks.com/blog/vulnerabilities-in-johnson-controls-exacqvision-web-service-expose-security-systems-to-video-stream-hijacking (дата обращения: 15.08.2025).
22. Комплексная программа инновационного развития холдинга «РЖД» на период до 2025 года. — URL: https://company.rzd.ru/ru/9990/page/103290?id=19093 (дата обращения: 05.01.2025).
23. Tao F. Adversarial Attack for Deep Steganography Based on Surrogate Training and Knowledge Diffusion / F. Tao, Ch. Cao, H. Li et al. // Applied Sciences (Switzerland). — 2023. — Vol. 13. — Iss. 11. — P. 6588.
24. Григоренко А. Г. Обзор методов защиты от адверсиальной атаки One Pixel в системах машинного обучения / А. Г. Григоренко, Н. А. Васильев, Д. С. Ситдиков // Системы интеллектуального управления и искусственный интеллект: теория и практика: сб. тр. II нац. науч.-практ. конф., Санкт-Петербург, 27 июня 2024 г. — СПб.: ГУМРФ им. адм. С. О. Макарова, 2024. — С. 30–36.
25. Грачев Я. Л. Задачи автоматизации стегоанализа / Я. Л. Грачев, В. Г. Сидоренко // Интеллектуальные транспортные системы: материалы II Междунар. науч.-практ. конф., Москва, 25 мая 2023 г. — М.: РУТ, 2023. — С. 450–455.
26. Грачев Я. Л. Анализ степени разработанности темы стегоанализа в файлах графических форматов / Я. Л. Грачев, В. Г. Сидоренко // Интеллектуальные транспортные системы: материалы IV Междунар. науч.-практ. конф., Москва, 22 мая 2025 г. — М.: РУТ (МИИТ), 2025. — С. 502–511.
27. Fridrich J. Rich Models for Steganalysis of Digital Images / J. Fridrich, J. Kodovsky // IEEE Transactions on Information Forensics and Security. — 2012. — Vol. 7. — Iss. 3. — Pp. 868–882.
28. Fridrich J. Steganography in Digital Media. Principles, Algorithms, and Applications / J. Fridrich. — Cambridge: Cambridge University Press, 2010. — 431 p.
29. Грачев Я. Л. Использование качественных характеристик изображения для комплексного стегоанализа / Я. Л. Грачев, В. Г. Сидоренко // Надежность. — 2025. — Т. 25. — № 1. — С. 67–74.
30. Грачев Я. Л. Применение стегоанализа для обеспечения целостности информации в интеллектуальных системах транспорта / Я. Л. Грачев, В. Г. Сидоренко // Интеллектуальные транспортные системы: материалы Междунар. науч.-практ. конф., Москва, 26 мая 2022 г. — М.: РУТ, 2022. — С. 389–396.
31. Westfeld A. Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools — and Some Lessons Learned / A. Westfeld, A. Pfitzmann // Lecture Notes in Computer Science. — 1999.
32. Fridrich J. Reliable detection of LSB steganography in color and grayscale images / J. Fridrich, M. Goljan, R. Du // Proceedings of the 2001 workshop on Multimedia and security new challenges — MM&Sec '01. — New York: ACM Press, 2001. — P. 27.
33. Грачев Я. Л. Стегоанализ методов скрытия информации в графических контейнерах / Я. Л. Грачев, В. Г. Сидоренко // Надежность. — 2021. — Т. 21. — № 3. — С. 39–46.
34. Fielding R. T. Architectural styles and the design of network-based software architectures / R. T. Fielding. — 2001. — Pp. 76–106.
35. Свид. 2025614424 Российская Федерация. Свидетельство о государственной регистрации программы для ЭВМ. Программа комплексного стегоаналитического детектирования «StegoRevealer» / Я. Л. Грачев. — зарегистр. 21.02.2025.
36. Белим С. В. Стегоанализ алгоритма Коха — Жао / С. В. Белим, Д. Э. Вильховский // Математическое и компьютерное моделирование: сб. материалов VI Междунар. науч. конф., Омск, 23 ноября 2018 г. — Омск: Омский гос. ун-т им. Ф. М. Достоевского, 2018. — С. 185–188.
37. Breiman L. Random Forests / L. Breiman // Machine Learning. — 2001. — Vol. 45. — Iss. 1. — Pp. 5–32.
38. LISA Traffic Light Dataset. — URL: https://www.kaggle.com/datasets/mbornoe/lisa-traffic-light-dataset (дата обращения: 01.07.2025).
39. Russian traffic sign images dataset. — URL: https://www.kaggle.com/datasets/watchman/rtsd-dataset (дата обращения: 01.07.2025).

TRANSPORT AUTOMATION RESEARCH, 2025, Vol. 11, No. 3, pp. 226–238
DOI: 10.20295/2412-9186-2025-11-03-226-238

Implementation of a Comprehensive Statistical Steganography Detector Within the Framework of Intelligent Transport Systems

Information about authors
Sidorenko V. G., Doctor in Engineering, Professor. E-mail: valenfalk@mail.ru
Grachev Ya. L., Postgraduate Student. E-mail: yaroslav446@mail.ru

Russian University of Transport, "Control and Information Security" Department, Moscow

Abstract: The paper discusses the development of a comprehensive statistical steganography detection tool and its implementation in the module for analyzing the reliability of graphic data from automated control systems and ITS. The purpose of this implementation is to verify the authenticity and confirm the reliability of graphic data circulating in the system, received from machine vision devices and other means of image recording and image sensors, and to improve the reliability of automated systems. The developed software steganography detector has been implemented in the form of an API server. This allows the detector to be integrated into an automated system circuit and perform steganographic analysis in automatic mode. The output of this analysis is binary, indicating the presence or absence of embedded data in the analyzed image files.

The developed steganography detector is represented by the StegoRevealer software complex, which is registered with Rospatent. This complex demonstrates the capabilities of steganographic analysis on a test bench, with a performance of 656 gigaflops of images with a resolution of approximately 1.2 megapixels in 300 ms. It also effectively processes a large number of incoming requests simultaneously, up to 100. Concurrently, the server demonstrates a capacity to endure a workload of up to 10 RPS, exhibiting a 2% performance decline. This facilitates the real-time analysis of images using steganography, particularly when employing advanced server microprocessor technology.

Keywords: steganalysis; steganography; steganography detector; images; automated systems.

References

1. Aleksandrov E. A. Sistema distantsionnogo videokontrolya pri dvizhenii vagonami vpered [Remote video monitoring system for train movement]. *Zheleznye dorogi mira* [World Railways]. 2025, Iss. 4, pp. 48–50. (In Russian)
2. Deylid I. A., Korolev I. N., Kudryashov S. V., Popov P. A. *Ustroystvo obnaruzheniya prepyatstviy na puti dvizheniya rel'sovogo transportnogo sredstva* [Obstacle detection device for rail vehicles]. Patent RF, no. 212718, 2022. (In Russian)
3. Malinsky S. V., Abramov A. V., Sharova V. O. Avtomaticheskoe opredelenie granits opasnykh uchastkov zheleznodorozhnogo puti [Automatic detection of dangerous railway sections]. *Intellektual'nye transportnye sistemy* [Intelligent Transport Systems]. Moscow: RUT (MIIT) Publ., 2025, pp. 624–630. (In Russian)

4. Markov A. A., Antipov A. G., Verevkin A. Yu. *Sposob diagnostiki rel'sovogo puti i sinkhronizatsii rezul'tatov izmereniy* [Method for railway diagnostics and measurement synchronization]. Patent RF, no. 2680927, 2019. (In Russian)
5. Rozenberg E. N., Dezhkov M. A., Nikonuk A. A. Aktual'nost' i etapy perekhoda na intellektual'noe upravlenie ekspluatatsionnoy rabotoy zheleznodorozhnogo transporta [Relevance and stages of transition to intelligent railway management]. *Intellektual'nye transportnye sistemy* [Intelligent Transport Systems]. Moscow: RUT (MIIT) Publ., 2025, pp. 369–375. (In Russian)
6. Nutovich V. E. Formalizovannye metody obrabotki informatsii, analiza i sinteza sistemy intellektual'nogo kommercheskogo osmotra vagonov [Formalized methods for intelligent wagon inspection system]. *Nauka i tekhnika transporta* [Science and Technology of Transport]. 2023, Iss. 3, pp. 77–85. (In Russian)
7. Sidorenko V. G., Kulagin M. A., Rodina D. M. Intellektual'naya sistema obnaruzheniya narusheniy v soblyudenii trebovaniy bezopasnosti pri rabotakh na ob»ektakh zheleznodorozhnoy infrastruktury [Intelligent safety violation detection system]. *Avtomatika na transporte* [Automation in Transport]. 2025, vol. 11, Iss. 1, pp. 55–65. (In Russian)
8. Andreev V. E., Dolgiy A. I., Kudyukin V. V. et al. Tsifrovaya zheleznodorozhnaya stantsiya — ot kontseptsii k real'nomu vnedreniyu [Digital railway station — from concept to implementation]. *Avtomatika, svyaz', informatika* [Automation, Communication, Informatics]. 2023, Iss. 9, pp. 2–6. (In Russian)
9. Kudyukin V. V., Vukolov A. V., Kuzmin V. S. Imitatsionnoe modelirovanie raboty robototekhnicheskikh kompleksov, prednaznachennykh dlya rasformirovaniya sostavov na sortirovochnykh gorkakh [Simulation of robotic complexes for train marshalling]. *Avtomatika na transporte* [Automation in Transport]. 2025, vol. 11, Iss. 1, pp. 16–29. (In Russian)
10. Ansari A. S. A Review on the Recent Trends of Image Steganography for VANET Applications. Computers, Materials and Continua. 2024, vol. 78, Iss. 3, pp. 2865–2892.
11. Shedole S. M., Santhi V. A Comprehensive Study on Digital Watermarking for Security Threats and Research Directions. International Journal of Data Informatics and Intelligent Computing, 2025, vol. 4, Iss. 1, pp. 54–72.
12. Hu K., Wang M., Ma X., Chen J. Learning based image steganography and watermarking: A survey. Expert Systems with Applications. 2024, Iss. 249.
13. Hahn D., Munir A., Behzadan V. Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. IEEE Intelligent Transportation Systems Magazine. 2021, vol. 13, Iss. 1, pp. 181–196.
14. Sidorenko V. G., Grachev Y. L. Protivodeystvie ugrozam informatsionnoy bezopasnosti, svyazannym s primeneniem sredstv steganografii [Counteracting information security threats associated with the use of steganography]. *Avtomatika, svyaz', informatika* [Automation, communication, informatics]. 2025, Iss. 1, pp. 17–22. (In Russian)
15. Security Brief: Actor Uses Compromised Accounts, Customized Social Engineering to Target Transport and Logistics Firms with Malware. Available at: https://www.proofpoint.com/us/blog/threat-insight/security-brief-actor-uses-compromised-accounts-customized-social-engineering (accessed: September 28, 2024).
16. Sea-Tac Airport officials confirm cyberattack disrupted service, websites. Available at: https://www.seattletimes.com/business/sea-tac-airport-officials-say-cyberattack-disrupted-service-websites/ (accessed: September 29, 2024).
17. Matyushin A., Rudina E. Kiberimmunnyy podkhod k proektirovaniyu kak prakticheskaya realizatsiya kontseptsii Security-by-Design [Cyberimmune Approach to Design as a Practical Implementation of the Security-by-Design Concept]. *CONNECT. Mir informatsionnykh tekhnologiy* [CONNECT. The World of Information Technologies]. 2023, Iss. 7–8, pp. 38–44. (In Russian)
18. Anonymous hacked Russian cams, websites, announced a clamorous leak. Available at: https://securityaffairs.com/128847/hacktivism/anonymous-vs-russia.html (accessed: August 16, 2025).
19. *Samyy bezzashchitnyy — uzhe ne Sapsan. Vse okazalos' kuda khuzhe…* [The Most Defenseless Is No Longer Sapsan. Everything turned out to be much worse…]. Available at: https://habr.com/ru/articles/536750/ (accessed: August 13, 2025). (In Russian)
20. Cyberattack on Dutch prosecution service is keeping speed cameras offline. Available at: https://www.theregister.com/2025/08/15/cyberattack_on_dutch_prosecution_service/ (accessed: August 15, 2025).
21. Vulnerabilities in Johnson Controls' exacqVision Web Service Expose Security Systems to Video-Stream Hijacking. Available at: https://www.nozominetworks.com/blog/vulnerabilities-in-johnson-controls-exacqvision-web-service-expose-security-systems-to-video-stream-hijacking (accessed: August 15, 2025).
22. *Kompleksnaya programma innovatsionnogo razvitiya kholdinga "RZhD" na period do 2025 goda* [Comprehensive innovation development program of RZD holding for the period up to 2025]. Available at: https://company.rzd.ru/ru/9990/page/103290?id=19093 (accessed: January 5, 2025). (In Russian)
23. Tao F., Cao Ch., Li H. et al. Adversarial Attack for Deep Steganography Based on Surrogate Training and Knowledge Diffusion. Applied Sciences (Switzerland). 2023, vol. 13, Iss. 11, p. 6588.
24. Grigorenko A. G., Vasil'ev N. A., Sitdikov D. S. Obzor metodov zashchity ot adversial'noy ataki One Pixel v sistemakh mashinnogo obucheniya [Review of methods for protecting against One Pixel adversarial attack in machine learning systems]. *Sistemy intellektual'nogo upravleniya i iskusstvennyy intellekt: teoriya i praktika: sb. tr. II nats. nauch.-prakt. konf., Sankt-Peterburg, 27 iyunya 2024 g.* [Intelligent control systems and artificial intelligence: theory and practice: Coll. t. II nat. sci.-pract. Conf., St. Petersburg, June 27, 2024]. Saint Petersburg: GUMRF Publ., 2024, pp. 30–36. (In Russian)
25. Grachev Y. L., Sidorenko V. G. Zadachi avtomatizatsii stegoanaliza [Steganalysis Automation Tasks]. *Intellektual'nye transportnye sistemy: materialy II Mezhdunar. nauch.-prakt. konf., Moskva, 25 maya 2023 g.* [Intelligent Transport Systems: Proc. of the II Int. Res. and Pract. Conf., Moscow, May 25, 2023]. Moscow: RUT Publ., 2023, pp. 450–455. (In Russian)
26. Grachev Y. L., Sidorenko V. G. Analiz stepeni razrabotannosti temy stegoanaliza v faylah graficheskikh formatov [Analysis of the Degree of Development of the Steganalysis Topic in Graphic Format Files]. *Intellektual'nye transportnye sistemy: materialy IV Mezhdunar. nauch.-prakt. konf., Moskva, 22 maya 2025 g.* [Intelligent Transport Systems: Proc. of the IV Int. Res. and Pract. conf., Moscow, May 22, 2025]. Moscow: RUT (MIIT) Publ., 2025, pp. 502–511. (In Russian)
27. Fridrich J., Kodovsky J. Rich Models for Steganalysis of Digital Images. IEEE Transactions on Information Forensics and Security. 2012, vol. 7, Iss. 3, pp. 868–882.
28. Fridrich J. Steganography in Digital Media. Principles, Algorithms, and Applications. Cambridge: Cambridge University Press, 2010. 431 p.
29. Grachev Y. L., Sidorenko V. G. Ispol'zovanie kachestvennykh kharakteristik izobrazheniya dlya kompleksnogo stegoanaliza [Using Qualitative Image Characteristics for Complex Steganalysis]. *Nadezhnost'* [Reliability.]. 2025, vol. 25, Iss. 1, pp. 67–74. (In Russian)
30. Grachev Y. L., Sidorenko V. G. Primenenie stegoanaliza dlya obespecheniya tselostnosti informatsii v intellektual'nykh sistemakh transporta [Application of steganalysis to ensure information integrity in intelligent transport systems]. *Intellektual'nye transportnye sistemy: materialy Mezhdunar. nauch.-prakt. konf., Moskva, 26 maya 2022 g.* [Intelligent transport systems: proc. Int. scientific-practical. conf., Moscow, May 26, 2022]. Moscow: RUT Publ., 2022, pp. 389–396. (In Russian)
31. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganographic Utilities Ez-Stego, Jsteg, Steganos, and S-Tools. Lecture Notes in Computer Science, 1999.
32. Fridrich J., Goljan M., Du R. Reliable detection of LSB steganography in color and grayscale images. Proceedings of MM&Sec '01. New York: ACM Press, 2001, p. 27.
33. Grachev Y. L., Sidorenko V. G. Stegoanaliz metodov skrytiya informatsii v graficheskikh konteynerakh [Steganalysis of methods for hiding information in graphic containers]. *Nadezhnost'* [Reliability]. 2021, vol. 21, Iss. 3, pp. 39–46. (In Russian)
34. Fielding R. T. Architectural styles and the design of network-based software architectures. 2001, pp. 76–106.
35. Grachev Y. L. *Programma kompleksnogo stegoanaliticheskogo detektirovaniya "StegoRevealer"* [Complex steganalytical detection program "StegoRevealer"]. Svidetel'stvo RF, no. 2025614424, 2025. (In Russian)
36. Belim S. V., Vilkhovsky D. E. Stegoanaliz algoritma Koha — Zhao [Steganalysis of the Koch — Zhao algorithm]. *Matematicheskoe i komp'yuternoe modelirovanie: sb. materialov VI Mezhdunar. nauch. konf., Omsk, 23 noyabrya 2018 g.* [Mathematical and computer modeling: collection of materials of the VI Int. scientific conf., Omsk, November 23, 2018]. Omsk: Omskiy gos. un-t Publ., 2018, pp. 185–188. (In Russian)
37. Breiman L. Random Forests. Machine Learning. 2001, vol. 45, Iss. 1, pp. 5–32.
38. LISA Traffic Light Dataset. Available at: https://www.kaggle.com/datasets/mbornoe/lisa-traffic-light-dataset (accessed: July 1, 2025).
39. Russian traffic sign images dataset. Available at: https://www.kaggle.com/datasets/watchman/rtsd-dataset (accessed: July 1, 2025).