Использование качественных характеристик изображения для комплексного стегоанализа

Using the qualitative characteristics of an image for comprehensive steganalysis

Грачев Я.Л.[1]*, Сидоренко В.Г.[1]
Grachev Ya.L., Sidorenko V.G.

[1]Российский университет транспорта, Москва, Российская Федерация
[1]Russian University of Transport, Moscow, Russian Federation
**yaroslav446@mail.ru*

Грачев Я.Л.

Сидоренко В.Г.

Резюме. Цель. *Задача стегоанализа изображений стоит особенно актуально ввиду использования стеганографического скрытия в графических файлах для доставки вредоносного кода и информации при совершении кибератак. В этой связи требуется совершенствование существующих способов детектирования встроенной средствами стеганографии информации. Одним из подходов является использование методики комплексного стегоанализа, предполагающей формирование вывода о детектировании встраивания на основе результатов применения группы из нескольких методов стегоанализа, а также вспомогательных расчетов.* **Методы.** *Для повышения точности детектирования скрытой информации предлагается использовать качественные оценки изображений. В статье продемонстрирована связь между значениями таких оценок и увеличением ошибок работы методов стегоанализа. Методика комплексного стегоанализа, включающая в себя учет качественных характеристик изображений, позволяет повысить точность формируемой оценки путем уменьшения ложноположительных результатов. В статье используются статистические методы подсчета качественных характеристик изображения, оценки корреляции Спирмена, методы машинного обучения.* **Результаты.** *Разработан программный комплекс, интегрирующий описанные в статье элементы методики комплексного стегоанализа, включающие в себя как группу методов стегоанализа, так и набор оцениваемых качественных характеристик изображения. Дана оценка связи качественных характеристик изображения с ошибками в результатах работы методов стегоанализа на пустых контейнерах. Сформированы тестовые выборки и построены модели машинного обучения, формирующие вывод об обнаружении скрытой информации в изображении.* **Заключение.** *Предложенный подход позволяет увеличить точности детектирования скрытой информации при учете оценок качественных характеристик изображения в рамках стегоанализа, что подтверждается экспериментально.*

Abstract. Aim. *The problem of image steganalysis is especially relevant given the use of steganographical concealment in graphic files for delivering malicious code and information as part of cyber attacks. That requires improvements to the existing methods of detecting steganographically embedded information. One method is to use a comprehensive steganalysis technique that involves concluding on the detection of embedded information based on the findings of a group of steganalysis methods, as well as auxiliary calculations.* **Methods.** *It is proposed improving the accuracy of hidden information detection by using qualitative image estimation. The paper demonstrates the relationship between the estimates and the increased rate of steganalysis errors. The method of comprehensive steganalysis that involves accounting for the qualitative characteristics of images allows improving the accuracy of estimation by reducing the rate of false positives. The paper uses statistical methods for calculating the qualitative characteristics of images, Spearman correlation, and machine learning.* **Results.** *A software package has been developed that integrates elements of the comprehensive steganalysis method described in the paper that includes both a group of steganalysis methods, and a set of evaluated qualitative characteristics of an image. The author evaluates the relationship between the qualitative characteristics of an image and the steganalysis errors in the case of empty containers. Test samples have been defined and machine learning models have been built that generate a conclusion as regards the detection of hidden information in an image.* **Conclusion.** *The proposed method enables improved accuracy of hidden information detection, while taking into account the estimates of the qualitative characteristics of an image as part of steganalysis, which is confirmed experimentally.*

Ключевые слова: *стегоанализ, стеганография, изображение, метод Хи-квадрат, метод Regular-Singular, качественные характеристики.*
Keywords: *steganalysis, steganography, image, Chi-square method, Regular-Singular method, qualitative characteristics.*

Для цитирования: *Грачев Я.Л.[1*], Сидоренко В.Г. Использование качественных характеристик изображения для комплексного стегоанализа // Надежность. 2025. №1. С. 67-74. https://doi.org/10.21683/1729-2646-2025-25-1-67-74*
For citation: *Grachev Ya.L., Sidorenko V.G. Using the qualitative characteristics of an image for comprehensive steganalysis. Dependability 2025;1:67-74. https://doi.org/10.21683/1729-2646-2025-25-1-67-74*

Поступила: *13.09.2024* / **После доработки:** *19.11.2024* / **К печати:** *05.03.2025*
Received on: *13.09.2024* / **Revised on:** *19.11.2024* / **For printing:** *05.03.2025*

Введение

Стеганография является одним из актуальных способов доставки необходимой злоумышленнику для совершения атаки информации внутрь атакуемой системы [1]. Как правило, это происходит после внедрения в атакуемую систему специального загрузчика, способного принять файл, содержащий скрытые данные, и извлечь вредоносную информацию (например, исполняемый вредоносный код) [1]. Часто такими файлами являются изображения – то есть файлы графических форматов. Это связано с большим доступным объемом контейнера, в котором методы стеганографии позволяют скрыть данные.

Задача обнаружения подобного рода скрытой информации в файлах изображений является важной составляющей мер по предотвращению осуществления кибератак, позволяя вовремя пресечь проникновение внутрь системы подозрительных данных, имеющих шансы быть вредоносными. Эту задачу решают методы стегоанализа.

1. Методика комплексного стегоанализа

Одной из ключевых проблем стегоанализа является невозможность в общем случае заранее знать метод или технику стеганографического скрытия, примененного для встраивания информации в контейнер. Большинство методов стегоанализа направлены на выявление только определенных видов стеганографии – например, скрытия в наименьших значащих битах (НЗБ) или скрытия, произведенного по методу Коха-Жао [2].

Задачу осуществления стегоанализа при неимении какой-либо дополнительной информации, кроме непосредственно подозрительного файла изображения, призваны решать методы т.н. «слепого стегоанализа» (также – «слепые методы») [3, 4]. Можно выделить два общих подхода к развитию таких методов:

1. Анализ статистических характеристик изображения с целью обнаружить нарушения и искажения, практически неизменно сопровождающие применение любых стеганографических методов;

2. Анализ на основе применения сразу нескольких методов стегоанализа и оценки различных характеристик изображения – данный подход предлагается называть «комплексным стегоанализом».

Первый подход, фактически, преследует цель создания некоего универсального метода стегоанализа – детектора, способного обнаруживать искажения, неизбежно вносимые сокрытием информации при помощи стеганографии. На данный момент такого универсального метода не существует, и исследование возможности его построения является отдельной подзадачей теории стегоанализа.

Второй же подход является более реалистичным и применимым на практике. В частности, его примером является предложенный Джессикой Фридрих анализатор "*cover-versus-all-stego classifier*" [3].

Комплексный стегоанализ подразумевает выполнение трех основных операций:

1. Применение методов стегоанализа;

2. Осуществление дополнительных вычислений и оценок (подсчет статистических характеристик, вычисление общего количества пикселей и т.п.);

3. Принятие решения об обнаружении стеганографического скрытия на основе результатов, полученных в п. 1 и п. 2.

При этом второй шаг дополнительных вычислений может быть опущен в конкретных реализациях данного подхода – в таких случаях решение об обнаружении стеганографии применяется исключительно на основе набора результатов применения методов стегоанализа. Примером такого подхода является метод совместного применения стегоаналитических методов, предложенный в [5]: в нем на основе результатов работы методов оценки по критерию Хи-квадрат и *Regular-Singular* предложен способ формирования вывода о наличии либо отсутствии стеганографического скрытия в файле изображения и даже, при выполнении некоторых условий, оценке объема скрытой информации [6, 7]. Однако данный метод позволяет обнаружить только встраивание, произведенное в НЗБ.

Для реализации комплексного стегоанализа в более полном виде требуется расширить набор применяемых

методов стегоанализа за счет алгоритмов, направленных на обнаружение информации, скрытой наиболее различными и наиболее популярными методами стеганографии. В частности, необходимо включить в набор методы анализа не только в пространственной области изображения (например, стегоанализ скрытия в НЗБ), но и частотной (например, реверсивные методы анализа скрытия, произведенного по Коха-Жао [8]).

Помимо формирования набора используемых методов стегоанализа важной задачей является реализация третьего пункта – то есть выбор алгоритма для принятия решения об обнаружении скрытой информации. Если при совместном применении лишь двух методов стегоанализа возможно формирование системы простых условий, как показано в [1], то при наличии более обширного контекста, полученного на первых двух шагах комплексного стегоанализа, требуется иной подход. Наиболее очевидным решением является применение методов машинного обучения, как было показано в [3].

Существуют два основных подхода к использованию машинного обучения для модуля принятия решения об обнаружении стеганографии [3]:

1. Обучение бинарного классификатора, различающего пустые и заполненные графические контейнеры;

2. Обучение распознаванию пустых графических контейнеров (чтобы любой результат, не распознанный как изображение с пустым контейнером, сигнализировал об обнаружении скрытия).

Анализатор «*cover-versus-all-stego classifier*» использует первый подход, и ключевым выводом, основанным на тестировании его эффективности, является способность обнаруживать информацию, встроенную методами стеганографии, методы атак на которые не были включены в набор стегоаналитических методов комплексного стегоанализа и на которых не проводилось обучение [3].

Таким образом, важной задачей методики комплексного стегоанализа является выбор алгоритмов стегоанализа, а также иных, результаты работы которых способны оказывать позитивный эффект на обучение и работу модуля принятия решений об обнаружении стеганографии, основанного на методах машинного обучения.

2. Использование качественных характеристик изображения для комплексного стегоанализа

Помимо оценок непосредственно методов стегоанализа возможно также использование иных числовых характеристик, вычисленных на основе анализируемого изображения, для передачи их в качестве входных данных в модуль принятия решений в целях корректировки получаемых результатов. Таким образом, комплексный стегоанализ может включать в себя не только стегоаналитические методы, но и вспомогательные алгоритмы, используемые для повышения точности оценки.

Одними из таких характеристик могут быть оценки качества изображений. Так как изображения, имеющие низкое качество, могут иметь нетипичные или аномальные статистические характеристики, может снижаться точность ряда математических методов стегоанализа, алгоритмы которых основаны на аппарате математической статистики.

Это легко проследить путем визуального осмотра: изображения низкого качества зачастую имеют завышенные показатели предполагаемого объема скрытой информации, вычисленного методами Хи-квадрат и *Regular-Singular* при пустом контейнере – примеры приведены в табл. 1.

Согласно [1], критическими значениями оценки (превышение которых сигнализирует об обнаружении стеганографического встраивания в изображения) методом Хи-квадрат является 0,105%, а методом *Regular-Singular* – 4,055%. Для каждого из приведенных выше изображений оценка хотя бы одним из методов превышает критическую несмотря на то, что в данных изображениях не осуществлялось скрытие информации.

К качественным характеристикам изображения относят, как правило, следующие [9]:

1. Резкость;
2. Размытость;
3. Зашумленность;
4. Контрастность;
5. Энтропия.

Для использования в рамках комплексного стегоанализа требуются алгоритмы вычисления данных характери-

Табл. 1. Примеры завышенных стегоаналитических оценок низкокачественных изображений

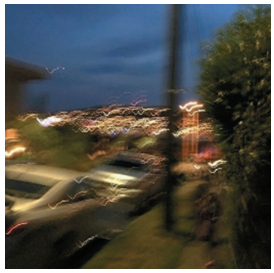
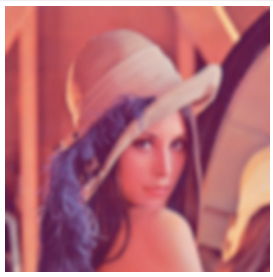
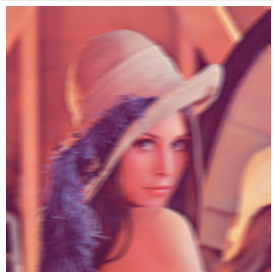
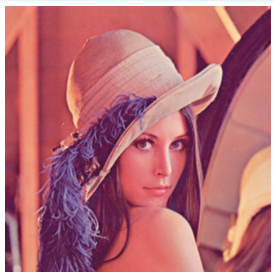
Изображение				
Оценка методом Хи-квадрат	1,67%	0%	0%	0,33%
Оценка методом *Regular-Singular*	1,97%	6,92%	6,5%	1,84%

Табл. 2. Примеры оценок уровня размытости тестового изображения «*fruits*»

Изображение				
Оценка уровня резкости	2,964	1,320	0,565	0,309

Табл. 3. Примеры оценок уровня размытости тестового изображения «*lena*»

Изображение				
Оценка уровня резкости	2,325	1,579	0,526	0,277

стик, не требующие эталона или сравнения двух различных изображений между собой, и способные в качестве результата представить некую числовую характеристику – оценку, соответствующую степени, соответственно, резкости, размытости и т.д. Согласно классификации качественных оценок изображений, представленной Монич и Старовойтовым, вышеописанным условиям соответствует группа абсолютных количественных оценок [9].

Поскольку изображения низкого качества могут получать завышенные оценки скрытого объема информации, анализ результатов подсчета качественных характеристик может использоваться, в первую очередь, для снижения количества ложноположительных результатов: значительная оценка скрытого объема информации при характеристиках, указывающих на заметные искажения в качестве изображения, для метода *Regular-Singular* скорее всего должна игнорироваться. Поскольку оценка объема скрытого сообщения для пустого контейнера фактически является величиной ошибки – отклонения в оценке размера встроенной информации (от нуля) – наличие корреляции между данной величиной и вышеуказанными качественными характеристиками изображения означает возможность использования оценки данной характеристики для уточнения результатов комплексного стегоанализа.

Способ оценки уровней зашумленности и резкости изображения в рамках подсчета качественных характеристик описан в [10]. Для подсчета уровня шума предлагается использовать метод, предложенный Новиковым и Пронькиным [11], основанный на сравнении нескольких групп пикселей с наименьшей дисперсией с их сглаженными версиями.

Для оценки уровня резкости используется безэталонный метод, основанный на поиске расстояния между пикселями с минимальной и максимальной интенсивностью в окрестностях каждого краевого пикселя, полученного в результате применения детектора Канни [12]. Мерой резкости в данном методе предлагается считать максимальное из полученных значений резкости по каждому из краевых пикселей.

Метод оценки размытости, предложенный Монич и Старовойтовым, подразумевает сведение задачи о безэталонной оценке к задаче получения сравнительной оценки [13]. С помощью свертки исходного изображения с усредняющим фильтром формируется его размытая версия, которая впоследствии сравнивается с оригинальной. Примеры оценок размытости для тестовых изображений приведены в табл. 2 и табл. 3.

Метод подсчета контраста основан на вычислении локальных оценок контраста по формуле Гордона, которая использует для этого средние значения яркости в квадратных окрестностях пикселей с линейными размерами 3 и 9 [14]. Для получения единой оценки контраста используются параметры распределения Вейбулла [14]. Примеры оценок контраста приведены в табл. 4 и табл. 5.

В качестве оценок энтропии используются формулы энтропии по Шеннону и Реньи [15]. Для подсчета энтропии изображения используется единый подход, при котором вначале формируется гистограмма изображения – то есть распределение градаций яркости пикселей (отношение числа появлений пикселей k-ого уровня яркости к общего числу пикселей). На основе этой гистограммы осуществляется вычисление энтро-

Табл. 4. Примеры оценок уровня контраста тестового изображения «*fruits*»

Изображение				
Оценка уровня шума	0,713	0,733	0,770	0,843

Табл. 5. Примеры оценок уровня контраста тестового изображения «*lena*»

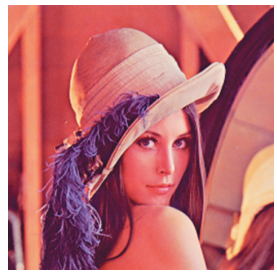
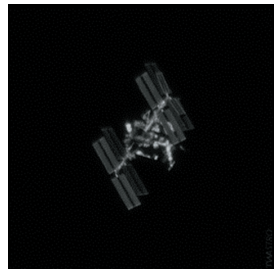
Изображение				
Оценка уровня шума	0,621	0,633	0,651	0,688

Табл. 6. Примеры оценок уровня энтропии набора тестовых изображений

Изображение				
Энтропия Шеннона	0,452	2,608	2,800	4,164
Энтропия Реньи	0,091	1,487	1,782	2,507

пий. В табл. 6 представлены примеры оценок энтропии Шеннона и Реньи для изображений.

3. Связь между качественными оценками изображения и результатами стегоанализа

Для подсчета корреляции между качественными оценками изображения и результатами его стегоанализа при незаполненном контейнере была сформирована выборка из 16614-ти изображений, в которую вошли графические файлы из различных открытых датасетов, включающих в себя:

- изображения с размытием в движении;
- шумные изображения;
- нечеткие изображения.

Для каждого изображения были осуществлены процедуры стегоанализа методами Хи-квадрат и *Regular-Singular*, а также выполнены подсчеты качественных характеристик. Далее были вычислены коэффициенты корреляции Спирмена между характеристиками и результатом оценки каждым из стегоаналитических методов. Полученные значения коэффициенты представлены в табл. 7.

Статистическую значимость полученных значений корреляции можно определить с помощью *t*-критерия Стьюдента [16]:

$$t = \frac{r\sqrt{n-2}}{\sqrt{1-r^2}},$$

где r – коэффициент корреляции, n – размер выборки.

Табл. 7. Коэффициенты корреляции между оценками методами стегоанализа и оценками качества изображения

	Шум	Резкость	Размытость	Контраст	Шеннон	Реньи
Regular-Singular	0,5606	0,5838	-0,7327	0,0672	0,3821	0,2715
Хи-квадрат	0,3873	0,2546	-0,4472	-0,1162	0,2939	0,3576

Табл. 8. Значения *t*-критерия Стьюдента

	Шум	Резкость	Размытость	Контраст	Шеннон	Реньи
Regular-Singular	87,249	92,673	-138,759	8,690	53,296	36,359
Хи-квадрат	54,132	33,934	-64,454	-15,072	39,637	49,349

Вычисленные величины *t*-критерия Стьюдента для каждого из полученных коэффициентов корреляции приведены в табл. 8.

Критическое значение критерия Стьюдента при заданном уровне значимости $\alpha = 0,01$ равняется 2,5761. Поскольку все вычисленные значения *t*-критерия превышают критическое, все исследуемые корреляционные связи являются статистически значимыми.

Поскольку критерий Стьюдента позволяет понять, является ли корреляция значимой, но не то, насколько она значима (насколько сильна корреляционная связь), значения коэффициентов корреляции были проанализированы по шкале Чеддока [17]. Согласно ей, существует высокая корреляция между размытостью и оценками методом *Regular-Singular* (причем повышение размытости ведет к уменьшению оценки по RS). Также сильными (заметными) являются корреляции оценок по RS с шумом и резкостью. Остальные корреляции являются умеренными или слабыми (оставаясь, при этом, статистически значимыми).

4. Учет качественных характеристик при принятии решений об обнаружении стеганографии

Поскольку статистически значимая корреляционная связь между качественными оценками изображения и результатами стегоанализа методами Хи-квадрат и *Regular-Singular* подтверждена, эти данные могут быть использованы для обучения модуля принятия решения об обнаружении стеганографического скрытия, выполняющего финальную операцию комплексного стегоанализа.

Поскольку оба вышеуказанных метода стегоанализа осуществляют атаки на стеганографию только в пространственной области, следует включить в набор используемых методов алгоритм, способный детектировать скрытую информацию в частотной области. В данном случае не рассматривается связь между методами стегоанализа в частотной области и качественными оценками изображения, такой метод предлагается рассматривать также как вспомогательный для уменьшения количества ложноположительных результатов, связанных с чувствительностью метода *Regular-Singular* ко встраиванию в частотную область изображения в ряде случаев. В табл. 9 продемонстрировано, каким образом меняется оценка методом *Regular-Singular* в зависимости от объема информации, реально скрытой методом Коха-Жао в тестовом изображении.

Табл. 9. Примеры изменения оценок методом *Regular-Singular* при скрытии данных методом Коха-Жао для изображения «*fruits*»

Объем информации, скрытой методом Коха-Жао, бит	0	426	822	2484
Оценка относительного объема скрытой информации методом *Regular-Singular*, %	3,46	4,03	5,16	9,66

Таким образом, рассматривается метод комплексного стегоанализа, в первую очередь рассчитанный на обнаружение стеганографического скрытия в пространственной области изображения. Он включает в себя алгоритмы стегоанализа по методам Хи-квадрат, *Regular-Singular* и реверсивного метода стегоанализа скрытия, произведенного по методу Коха-Жао, а также набор алгоритмов расчета оценок качественных характеристик изображения – зашумленности, резкости, размытости, контраста и энтропии.

Для экспериментальной проверки данного метода была подготовлена выборка из 16592 изображений. В половине изображений выборки было осуществлено встраивание информации последовательной или псевдослучайной вариацией методов НЗБ или Коха-Жао случайным образом. Объем и содержимое скрытой информации также выбирались случайным образом.

Для каждого изображения были выполнены расчеты:

- оценки относительного объема скрытой информации методом Хи-квадрат;
- оценки относительного объема скрытой информации методом *Regular-Singular*;
- оценки предполагаемого порога встраивания и битового объема скрытой информации методом анализа скрытия, произведенного по Коха-Жао;
- оценок качественных характеристик.

Для выбора наиболее эффективного метода машинного обучения и проведения обучения используется фреймворк *ML.NET*. Наибольшую точность на обучающем наборе данных показал алгоритм случайного леса (в терминологии, используемой фреймворком *ML.NET* – «*FastForest*») – 0,84. Точности других методов составили:

- «*FastTree*» (реализация алгоритма градиентного бустинга *MART*): 0,82.

- «*LightGBM*» (алгоритм стохастического градиентного бустинга): 0,81.

- «*LBFGS*» (реализация оптимизированного с точки зрения потребления памяти варианта алгоритма Бройдена-Флетчера-Гольдфарба-Шанно): 0,77.

- «*SDCA*» (алгоритм «*Stochastic Dual Coordinate Ascent*» стохастического градиентного бустинга): 0,74.

Алгоритм случайного леса основан на применении большого ансамбля решающих деревьев, за счет количества которых достигается достаточная точность классификации. Классификация осуществляется путем жесткого голосования – то есть выбирается тот класс, который получен большинством решающих деревьев.

Полученная вышеописанным алгоритмом точность составила 0,84. При аналогичном наборе входных данных, из которых были исключены оценки качественных характеристик изображения (оставлены только данные о результатах стегоанализа методами *Regular-Singular*, Хи-квадрат и анализа скрытия по Коха-Жао) наибольшую точность также показал алгоритм случайного леса, однако его точность составила 0,79. Таким образом, обучение на данных, содержащих оценки качественных характеристик изображений помимо исключительно результатов стегоанализа, оказалось более эффективным.

Для дополнительной проверки обученной модели была использована отдельная непересекающаяся с обучающей выборка из 994 изображений, в половине из которых было осуществлено встраивание информации. Результаты проверки собраны в матрице ошибок в табл. 10.

Табл. 10. Матрица ошибок обученной модели

Действительные данные	Оценка моделью	
	Определено скрытие	Не определено скрытие
Со скрытием	492	5
Без скрытия	12	485

Как видно, ложноотрицательный результат был получен в примерно 1% случаев, а ложноположительный – в 2,4%. Суммарная точность модели на проверочной выборке составила 98,3%.

Заключение

Методика комплексного стегоанализа представляет собой актуальный подход к выявлению информации, скрытой при помощи стеганографии, в графических файлах. Помимо использования непосредственно различных стегоаналитических алгоритмов, направленных на обнаружении определенных видов стеганографии, для уточнения результата возможно использовать дополнительные данные о присущих изображению характеристиках – в частности, оценки качества изображения, выражающиеся в подсчете резкости, размытости, зашумленности, контраста и энтропии изображения.

Включение оценок качественных характеристик изображения в наборы данных для обучения систем, принимающих решение об обнаружении стеганографического встраивания в изображении, в рамках методики комплексного стегоанализа позволяет повысить точность детектирования факта такого встраивания. Это достигается за счет отсечения ложноположительных результатов, связанных с завышением оценок, получаемых при работе методов стегоанализа для изображений низкого качества, в которые не производилось встраивание (пустых контейнеров).

Построение обученной модели машинного обучения, способной формировать вывод о наличии или отсутствии стеганографического встраивания в изображении, с использованием не только оценок, получаемых при работе стегоаналитических алгоритмов, но и вычисленных оценок качественных характеристик, позволяет повысить точность работы подобного стегодетектора в сравнении с аналогом, не учитывающим показатели качества изображения.

Библиографический список

1. Грачев Я.Л., Сидоренко В.Г. Задачи автоматизации стегоанализа // Материалы II Международной научно-практической конференции «Интеллектуальные транспортные системы» (25 мая 2023 г.). М.: РУТ МИИТ, 2023. С. 450-455.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. Киев: «МК-Пресс», 2006. 286 с.

3. Jessica Fridrich. Steganography in Digital Media. Principles, Algorithms, and Applications. Cambridge: «Cambridge University Press», 2010. 431 с.

4. Грачев Я.Л., Сидоренко В.Г. Применение стегоанализа для обеспечения целостности информации в интеллектуальных системах транспорта // Материалы Международной научно-практической конференции «Интеллектуальные транспортные системы» (26 мая 2022 г.). М.: РУТ МИИТ, 2023. С. 389-396.

5. Грачев Я.Л., Сидоренко В.Г. Стегоанализ методов скрытия информации в графических контейнерах // Надежность. 2021. Т. 21. № 3. С. 39-46.

6. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems. Dresden University of Technology, Department of Computer Science. Dresden, Germany, 1999. DOI: 10.1007/10719724_5

7. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghamton University, New York, USA, 2001. DOI: 10.1145/1232454.1232466

8. Белим С.В., Вильховский Д.Э. Стегоанализ алгоритма Коха-Жао // Математические структуры и моделирование. 2018. № 4(48). С. 113-119. DOI: 10.25513/2222-8772.2018.4.113-119

9. Монич Ю.И., Старовойтов В.В. Оценки качества для анализа цифровых изображений // Искусственный интеллект. 2008. № 4. С. 376-386.

10. Грачев Я.Л., Сидоренко В.Г. Использование статистических характеристик изображения для уточнения результатов стегоанализа // Материалы III Международной научно-практической конференции «Интеллектуальные транспортные системы» (30 мая 2024 г.). С. 563-569.

11. Новиков А.И., Пронькин А.В. Метод оценки уровня шума цифрового изображения // Компьютерная оптика. 2021. Т. 45. № 5. С. 713-720.

12. Wang X., Tian B., Liang C. et al. Blind Image Quality Assessment for Measuring Image Blur // Proceedings of 2008 Congress on Image and Signal Processing (27-30 May 2008). 2008. Vol. 1. Pp. 467-470.

13. Монич Ю.И., Старовойтов В.В. Мера оценки резкости цифрового изображения // Доклады БГУИР. 2011. № 1(55). С. 80-84.

14. Голуб Ю.И., Старовойтов Ф.В. Исследование локальных оценок контраста цифровых изображений при отсутствии эталона // Системный анализ. 2019. № 2. С. 4-11.

15. Тимошенко А.В., Кошкаров А.С. Сравнительный анализ энтропийных метрик информативности оптических изображений космических объектов // Труды МАИ. 2020. № 112. С. 1-18.

16. Kendall M.G., Stuart A. The advanced theory of statistics. London: «Griffin», 1969. 676 c.

17. Chaddock R.E. Principles and methods of statistics. Boston «Houghton Mifflin Company», 1925. 471 c.

References

1. Grachev Y.L., Sidorenko V.G. Tasks of stegoanalysis automation. In: Proceedings of the II International Science and Practice Conference Intelligent Transportation Systems (May 25, 2023). Moscow: RUT MIIT; 2023. Pp. 450-457. (in Russ.)

2. Konakhovich G.F., Puzyrenko A.Y. [Computer steganography. Theory and practice]. Kiev: MK-Press; 2006. (in Russ.)

3. Fridrich J. Steganography in Digital Media. Principles and Applications. Cambridge: Cambridge University Press; 2010.

4. Grachev Ya.L., Sidorenko V.G. [Using stegoanalysis to ensure the integrity of information in intelligent transport systems]. In: [Proceedings of the International Science and Practice Conference Intelligent Transportation Systems] (May 26, 2022). Moscow: RUT MIIT; 2023. Pp. 389-396. (in Russ.)

5. Grachev Ya.L., Sidorenko V.G. Steganalysis of the methods of concealing information in graphic containers. *Dependability* 2021;21(3):39-46.

6. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems. Dresden University of Technology, Department of Computer Science. Dresden (Germany); 1999. DOI: 10.1007/10719724_5.

7. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghamton University, New York (USA); 2001. DOI: 10.1145/1232454.1232466.

8. Belim S.V., Vilkhovsky D.E. Koch-Zhao algoritm stganalysis. *Mathematical Structures and Modeling* 2018;4(48):113-119. DOI: 10.25513/2222-8772.2018.4.139-119. (in Russ.)

9. Monich Yu.I., Starovoitov V.V. [Quality assessments for the analysis of digital images]. *Iskusstvenny intellekt* 2008;4:376-386. (in Russ.)

10. Grachev Ya.L., Sidorenko V.G. [Using statistical characteristics of an image to improve the results of steganalysis]. In: [Proceedings of the III International Science and Practice Conference Intelligent Transportation Systems] (May 30, 2024). Pp. 563-569. (in Russ.)

11. Novikov A.I., Pronkin A.V. Methods for image noise level estimation. *Computer Optics* 2021;45(5): 713-720. (in Russ.)

12. Wang X., Tian B., Liang C. et al. Blind Image Quality Assessment for Measuring Image Blur. In: Proceedings of 2008 Congress on Image and Signal Processing (27-30 May 2008) 2008;1:467-470.

13. Monich Y.I., Starovoitov V.V. Measure of digital image blur evaluation. *Doklady BGUIR* 2011;1(55):80–84. (in Russ.)

14. Golub Yu.I., Starovoitov F.V. Study of local assessments of contrast for digital images. *Sistemny analiz* 2019;2:4-11. (in Russ.)

15. Timoshenko A.V., Koshkarov A.S. Comparative analysis of entropic metrics of space objects optical images informativity. *Trudy MAI* 2020;112:1-18. (in Russ.)

16. Kendall M.G., Stuart A. The advanced theory of statistics. London: Griffin; 1969.

17. Chaddock R.E. Principles and methods of statistics. Boston: Houghton Mifflin Company; 1925.

Сведения об авторах

Грачев Ярослав Леонидович (Yaroslav L. Grachev) – аспирант, Российский университет транспорта (*Russian University of Transport (MIIT)*), Российская Федерация, Москва, e-mail: yaroslav446@mail.ru.

Сидоренко Валентина Геннадьевна (Valentina G. Sidorenko) – доктор технических наук, профессор, профессор кафедры «Управление и защита информации», Российский университет транспорта (*Russian University of Transport (MIIT)*), Российская Федерация, Москва, e-mail: valenfalk@mail.ru.

About the authors

Yaroslav L. Grachev, postgraduate student, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: yaroslav446@mail.ru.

Valentina G. Sidorenko, Doctor of Engineering, Professor, Chair Professor, Department of Management and Protection of Information, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: valenfalk@mail.ru.

Вклад авторов в статью

Грачев Я.Л. – исследование методики комплексного стегоанализа в части использования качественных оценок изображения для увеличения эффективности, формирование тестовых выборок изображений, подсчеты корреляции, анализ результатов.

Сидоренко В.Г. – анализ оценки эффективности предложенной методики.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.