https://doi.org/10.25559/SITITO.020.202402.519-529
УДК 004.4

Оригинальная статья

Сравнительный анализ алгоритмов обнаружения скрытой информации в цифровых изображениях

А. И. Банников*, Е. А. Мельникова
ФГБОУ ВО «Российский государственный социальный университет», г. Москва, Российская Федерация
Адрес: 129226, Российская Федерация, г. Москва, ул. Вильгельма Пика, д. 4, стр. 1
* 123bannikov.a.i@gmail.com

Аннотация
В статье приведён анализ научных исследований в области стегоанализа цифровых изображений, рассмотрена классификация стегоаналитических алгоритмов. Сформулированы требования к программному обеспечению для автоматизации стегоанализа и сравнения алгоритмов обнаружения информации, скрытой в графических файлах. На примере парного анализа, а также метода Хи-квадрат и RS-анализа рассмотрен принцип работы стегоаналитических алгоритмов применительно к цифровым изображениям формата PNG. На языке Ruby разработан программный комплекс для исследования алгоритмов стегоанализа. Приведены результаты вычислительных экспериментов и сравнительного анализа точности работы описанных алгоритмов с использованием ROC-кривых. Представлены возможности программы и дана характеристика её работы при анализе изображений с разным объёмом скрытой информации. Практическим применением разработанного программного комплекса является проведение в университете лабораторных работ по изучению методов стегоанализа, а также исследование свойств стегоаналитических алгоритмов.

Ключевые слова: стегоанализ, стеганография, цифровые изображения, информационная безопасность

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Банников А. И., Мельникова Е. А. Сравнительный анализ алгоритмов обнаружения скрытой информации в цифровых изображениях // Современные информационные технологии и ИТ-образование. 2024. Т. 20, № 2. С. 519-529. https://doi.org/10.25559/SITITO.020.202402.519-529

Original article

Comparative Analysis of Algorithms for Detecting Hidden Information in Digital Images

A. I. Bannikov*, E. A. Melnikova
Russian State Social University, Moscow, Russian Federation
Address: 4 Wilhelm Pieck St., build. 1, Moscow 129226, Russian Federation
* 123bannikov.a.i@gmail.com

Abstract
The article provides an analysis of scientific research in the field of steganalysis of digital images, and considers the classification of steganalytic algorithms. Requirements for software for automating steganalysis and comparing algorithms for detecting information hidden in graphic files are formulated. Using the example of pair analysis, as well as the Chi-square and RS analysis methods, the principle of operation of steganalytic algorithms for digital images of PNG format is considered. A software package for researchment of steganalysis algorithms has been developed in the Ruby programming language. The results of computational experiments and a comparative analysis of the accuracy of the described algorithms using ROC curves are presented. The capabilities of the program are presented and the characteristics of its work with different amounts of hidden information are given. The practical application of the developed software package is the conducting laboratory work at the university to study steganalysis methods, as well as researching the properties of steganalytic algorithms.

Keywords:steganalysis, steganography, digital images, information security

Conflict of interests: The authors declares no conflict of interest.

For citation: Bannikov A.I., Melnikova E.A. Comparative Analysis of Algorithms for Detecting Hidden Information in Digital Images. *Modern Information Technologies and IT-Education.* 2024;20(2):519-529. https://doi.org/10.25559/SITITO.020.202402.519-529

Введение

В связи с развитием информационных технологий в наше время всё большее использование в цифровой среде находят технологии стеганографии, которая является одним из базовых способов защиты информации и служит для незаметной передачи данных по различным каналам. В последние годы исследователи отмечают применение стеганографии в интернете вещей [1], в медицинской сфере [2], при защите интеллектуальной собственности, при противодействии анализу исходных кодов приложений [1]. Данные технологии всё чаще используются злоумышленниками для проведения вирусных атак и в кибершпионаже[1] [3]. При этом наиболее используемыми контейнерами для передачи данных являются цифровые изображения из-за их большого распространения и высокой избыточности хранимой информации, количество научных публикаций на данную тему продолжает расти[2] [4, 5].

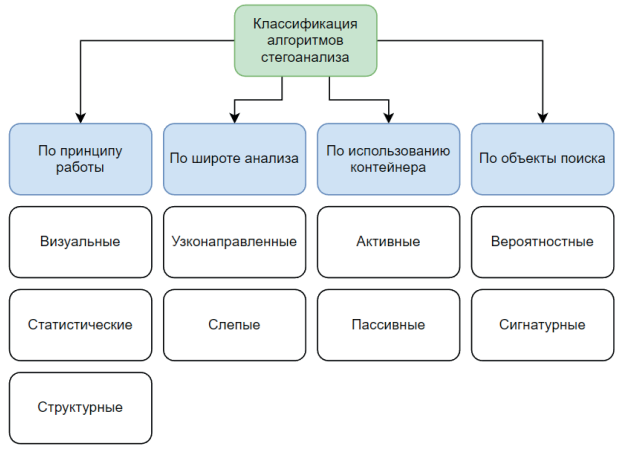
Поэтому является актуальной тема исследования стегоанализа, который позволяет выявлять сам факт наличия скрытой информации, а также определять её примерный объём и возможность извлечения. Изучение эффективности алгоритмов стегоанализа, а также их сравнительный анализ является достаточно комплексным вопросом, потому что их применение зависит от большого количества параметров, таких как тип изображения-контейнера, его характеристики, вид используемого стеганографического метода для встраивания информации, объём скрытого сообщения[3] [6, 7]. Разрабатываются новые алгоритмы и методы стегоанализа, которые должны отвечать современным вызовам [8].

Следует отметить, что в настоящее время в открытом доступе практически отсутствует программное обеспечение, позволяющее не только применять конкретные стеганографические алгоритмы, но и проводить сравнение эффективности их работы. При этом многие программы работают с устаревшими форматами изображений [9-11].

Целью данного исследования является разработка программного комплекса для исследования алгоритмов стегоанализа. С его помощью можно проводить вычислительные эксперименты и сравнивать точность работы исследуемых алгоритмов. Практическим применением разработанного программного комплекса является проведение в университете лабораторных работ по изучению методов стегоанализа, а также исследованию свойств стегоаналитических алгоритмов.

Алгоритмы стегоанализа

Широта существующих методов стеганографии с использованием цифровых изображений [12] порождает большой спектр подходов к стеганографическому анализу, которые встречаются в литературе [13], включая, например, субъективный визуальный анализ (рис. 1). Однако более актуальными для рассмотрения являются структурные и статистические методы из-за возможности их эффективной компьютерной автоматизации [4]. Вместе с тем, всё большее применение получают и гибридные алгоритмы стегоанализа, применяющие машинное обучение [13-14].



Р и с. 1. Классификация алгоритмов стегоанализа

F i g. 1. Steganalysis algorithms classification

Источник: здесь и далее в статье все таблицы и рисунки составлены авторами.

Source: Hereinafter in this article all tables and figures were made by the authors.

Так или иначе, принцип работы различных алгоритмов стегоанализа сводится к тому, что при внедрении скрытых данных в изображение изменяются некоторые закономерности, которых характерны для немодифицированных естественных изображений [13]. Каждый алгоритм, как правило, имеет свои недостатки и ограничения, в настоящее время до сих пор ведётся поиск наиболее универсального слепого метода обнаружения скрытой информации в изображениях [8]. На рисунке 2 слева направо представлена исходная версия чистого естественного изображения, а также изображение, для которого изменены наименее значимые биты цветовых значений первых 40% пикселей, красным выделены пиксели, отличающиеся по значению. Как видно, подобное внедрение практически незаметно для человеческого глаза.

[1] Красов А. В. Разработка модели нарушителя использующего стеганографические приемы компьютерных вирусов // Региональная информатика (РИ-2022): Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. СПб: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 553-554. EDN: KQVTNW; Грачев Я. Л., Сидоренко В. Г. Задачи автоматизации стегоанализа // Интеллектуальные транспортные системы: Материалы II Межд. НПК. М.: РУТ, 2023. С. 450-455. http://doi.org/10.30932/9785002182794-2023-450-455

[2] Караулова О. А., Шакурский М. В. Особенности оценки стеганографических систем с точки зрения стеганографического анализа // Инновационные, информационные и коммуникационные технологии: Сборник трудов XIX Международной НПК. Сочи, 2022. С. 66-70. EDN: UUHCRK

[3] Банников А. И., Терентьев А. Д., Мельникова Е. А. Разработка приложения для анализа алгоритмов сокрытия данных в цифровых изображениях // Современные информационные технологии в образовании, науке и промышленности. М.: ООО Изд-во «Экон-Информ», 2021. С. 5-7. EDN: BGNMVY

Р и с. 2. Сравнение пустого и заполненного изображения-контейнера
F i g. 2. Comparison of empty and filled container image

Вместе с тем, в современных исследованиях до сих пор отмечают частое практическое применение в современном прикладном стеганографическом ПО[4] [15] относительно простых в реализации методов стеганографии, таких как метод замены наименее значимых бит (LSB), потому что он позволяет передавать большой объём скрытых данных и довольно вариативен [16-18].

В качестве форматов изображений для передачи внедрённых данных наиболее перспективными считаются PNG и JPEG из-за их широкого применения и возможности встраивать данные напрямую в биты цветовых значений пикселей или коэффициенты дискретного косинусного преобразования, используемого при сжатии, соответственно [17], [19-20].

В качестве примеров стегоаналитических алгоритмов рассмотрим статистический метод Хи-квадрат [21], а также структурные методы Sample Pairs и RS-анализ [22] в силу их широкого рассмотрения в литературе, а также эффективности против различных типов LSB-внедрения [13].

Примером парных структурных методов стегоанализа является алгоритм Sample Pairs, использующий гипотезу об изменении соотношения пар значений цветов пикселей у заполненного изображения-контейнера. Пусть P будет набором всех пар значений цветовых каналов по горизонтали и вертикали. Для P можно определить множества K и M так, что:

K – пары где V четно и U < V, или V нечетно и U > V;

M – пары где V четно и U > V, или V нечетно и U < V.

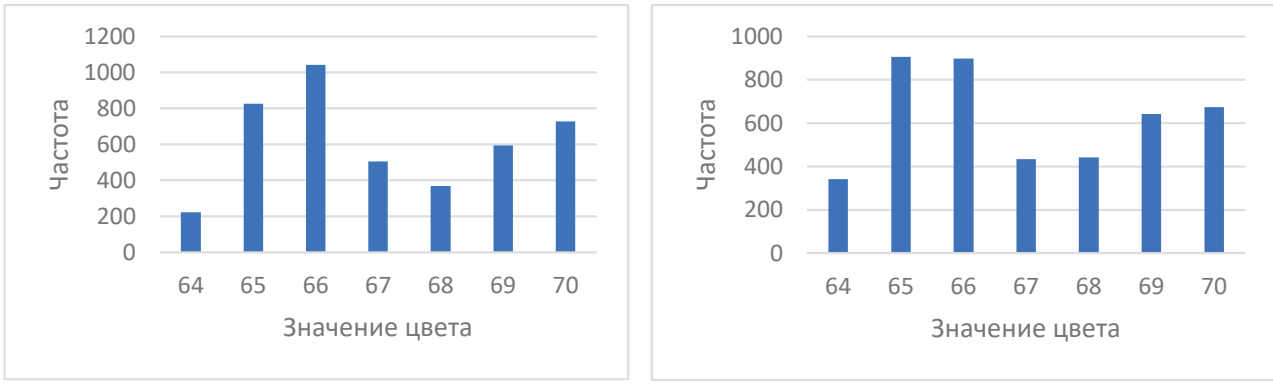
Для естественных изображений соблюдается гипотеза о том, что |K| = |M|. Дополнительно выделяется множество пар Z (U, V) ∈ P где U = V, а также множество подмножества W и V, где W – пары вида (2a, 2a + 1) или (2a + 1, 2a) и V = Y – W. Тогда P = X ∪ W ∪ V ∪ Z. Пусть p – длина встроенного сообщения в битах, разделенная на общее количество пикселей в P. Пусть γ = |W' ∪ Z'|, где штрихом обозначаются множества, куда уже осуществлено встраивание скрытой информации. Тогда длину скрытого сообщения можно примерно вычислить как наименьший корень следующего уравнения [22]:

$$0.5\gamma p^2 + (2|X'| - |\mathrm{P}|)p + |Y'| - |X'| = 0.$$

Более точным, но ресурсоёмким алгоритмом стегоанализа является RS-анализ, который также позволяет выявлять сообщения, встроенные с псевдослучайным распределением скрываемой в изображении информации. Данный метод, как и парные, использует гипотезы соотношений некоторых специальных групп значений, называемых регулярными и сингулярными, а также позволяет вычислить приближённый объём встроенного сообщения, однако этот метод довольно сложен в реализации. Его более подробное описание и связи с другими структурными алгоритмами можно найти в литературе [22].

Популярным примером статистического стегоанализа является Хиквадрат [21], по которому можно сравнить насколько гистограмма блоков значений цветов пикселей изображения близка к характерному для заполненных стегоконтейнеров распределению. На рисунке 3 представлены гистограммы, полученные при исследовании изображений с помощью разработанного программного комплекса – слева представлен график, характерный для естественного PNG-изображения, а справа – для содержащего скрытую информацию.

[4] Вильховский Д. Э. Стеганографический анализ искусственных изображений на предмет обнаружения LSB-вставок // Математическое и компьютерное моделирование: Сборник материалов IX Международной научной конференции, посвященной 85-летию профессора В.И. Потапова. Омск: ОмГУ им. Ф.М. Достоевского, 2021. С. 316-318. EDN: SIQTTC



Р и с. 3. Гистограммы значений пустого и заполненного изображения-контейнера
F i g. 3. Histograms of empty and filled container image values

При анализе с помощью метода Хи-квадрат для каждого j-го пикселя рассчитывают, сколько раз n_j пиксель x_j принимает каждое из k возможных цветовых значений. Приблизительную вероятность встречи этих элементов в стего-изображении для данного общего числа пикселей n можно получить по формуле $p_j = n_j/n$, тогда и для исходного набора значений искомая вероятность будет равна $p_j^* = n_j^*/n$.

Мы знаем предполагаемое и реальное распределение, поэтому можно вычислить значение статистики Хиквадрат для блока значений цветов. Пускай m – число степеней свободы, которое вычисляется как разность количества элементов k и числа независимых условий, наложенных на вероятности p_j^*, тогда получим:

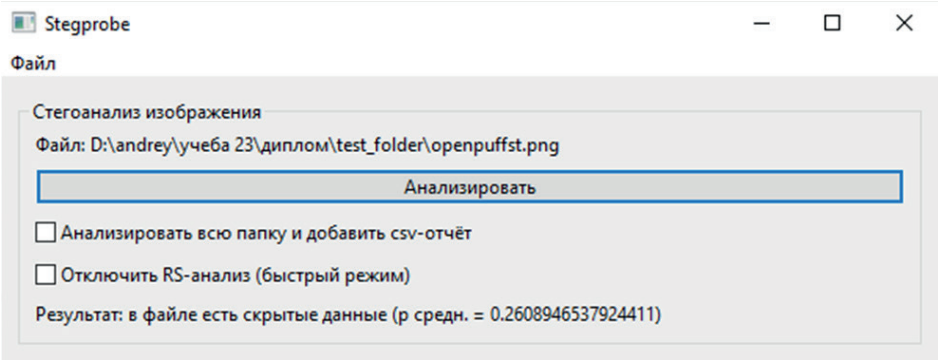
$$\chi^2 = \sum_{j=1}^{m} \frac{\left(n_j - np_j\right)^2}{np_j}.$$

При этом вероятность p совпадения предполагаемого и реального распределения рассчитывается по формуле:

$$p = 1 - \int_0^{\chi^2} \frac{t^{\frac{m-2}{2}} * e^{-\frac{t}{2}}}{2^{\frac{m}{2}} * \Gamma\left(\frac{m}{2}\right)} dt.$$

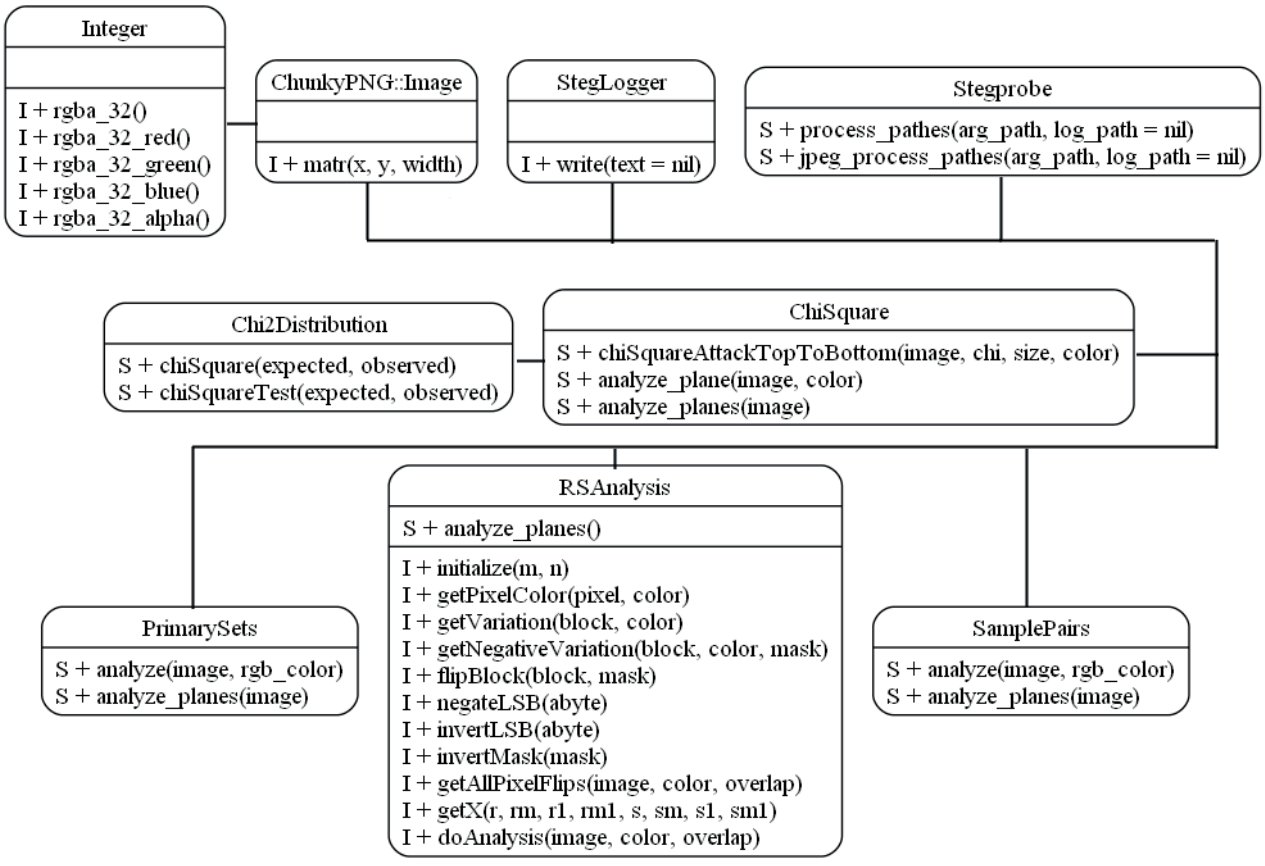
Программный комплекс для проведения исследований

После анализа существующих в открытом доступе программных инструментов для стеганографии, а также изучения условий тестирования стегоаналитических моделей [23-25], на языке Ruby был разработан программный комплекс для исследования алгоритмов стегоанализа (рис. 4). В качестве форматов изображений выбраны PNG и JPEN из-за их широкого использования в качестве стеганографических контейнеров [24-25].



Р и с. 4. Графический интерфейс программы для стегоанализа
F i g. 4. Graphical interface of the program for steganalysis

Разработанное приложение для стегоанализа имеет графический интерфейс, а также модульную структуру для работы со стегоаналитическими алгоритмами (рисунок 5). В программный комплекс можно как добавлять новые алгоритмы, так и исключать их из вычислений при получении результатов для исследуемой выборки изображений. Это позволяет получать новые и актуальные данные при появлении новых более точных или заточенных под более современные методы стеганографии алгоритмов стегоанализа, что является важным аспектом для исследовательского ПО.



Р и с. 5. UML-диаграммы программного комплекса для стегоанализа

F i g. 5. UML diagrams of the software package for steganalysis

Приложение позволяет проводить стегоанализ сразу для папки с изображениями, выводить в консоль подробные результаты работы по каждому применённому алгоритму стегоанализа, а также позволяет получить csv-файл с общими результатами по каждому конкретному изображению-контейнеру, его цветовым каналам и применённым к ним методам стегоанализа, а также с количественными значениями предполагаемого объёма сообщений, скрытых в исследуемых изображениях.

Результаты исследования

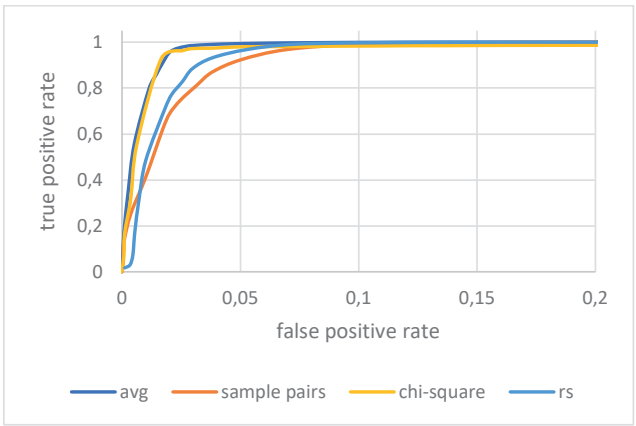
При помощи разработанного программного комплекса были проведены вычислительные эксперименты, в качестве сравниваемой величины использовалась точность (формула 1) при заданном пороге внедрения скрытой информации в 20% от общего объёма контейнера, по три наименее значимых бита на каждый цветовой канал.

$$\text{Точность} = \frac{\text{ИО} + \text{ИП}}{\text{ИП} + \text{ЛП} + \text{ИО} + \text{ЛО}} \qquad (1)$$

где ИО – количество истинно отрицательных срабатываний, ИП – истинно положительных, ЛО – ложно отрицательных, а ЛП – ложно положительных срабатываний. Каждый конкретный алгоритм считается тем более точным, чем больше площадь под ROC кривой. Иными словами, такой классификатор признаётся более качественным по сравнению с остальными.

Т а б л и ц а 1. **Доля ложно положительных и истинно положительных срабатываний в зависимости от выбранного порогового значения**
T a b l e 1. **The proportion of false positives and true positives depending on the selected threshold value**

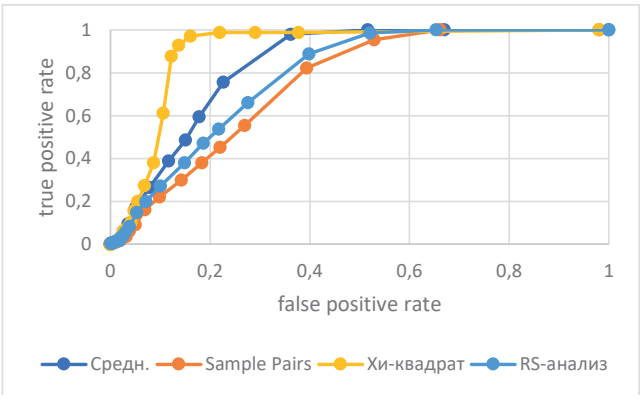
Порог	Парный анализ		Хи квадрат		RS анализ	
	ЛП	ИП	ЛП	ИП	ЛП	ИП
0	0,98109	1	0,980235	1	1	1
0,015	0,6617	1	0,377256	0,988803	0,65397	1
0,025	0,52936	1	0,290748	0,987941	0,52134	1
0,04	0,39416	1	0,219421	0,986649	0,39874	1
0,062	0,26984	1	0,160412	0,985788	0,27585	1
0,075	0,21999	1	0,136637	0,984496	0,2177	1
0,085	0,1839	0,99957	0,122601	0,984496	0,18648	1
0,1	0,14294	0,99699	0,106273	0,983204	0,14867	0,99957
0,125	0,09825	0,98923	0,087081	0,982343	0,10054	0,99699
0,15	0,06932	0,96727	0,068748	0,98062	0,07161	0,99009
0,175	0,05013	0,92291	0,054712	0,980189	0,05271	0,9677
0,2	0,0381	0,86951	0,047264	0,978467	0,0381	0,93152
0,225	0,03151	0,81137	0,041535	0,975452	0,02979	0,88501
0,25	0,02463	0,74677	0,036379	0,973299	0,02549	0,82773
0,275	0,02005	0,68777	0,029791	0,972007	0,02091	0,77089
0,3	0,01719	0,62059	0,025781	0,963394	0,01805	0,70801
0,4	0,01003	0,41214	0,016614	0,928941	0,01003	0,4845
0,5	0,00372	0,2528	0,006302	0,555986	0,00716	0,31352
0,6	0,00086	0,13092	0,003724	0,321275	0,00544	0,17614
0,7	0,00057	0,04522	0,001146	0,170112	0,00458	0,07321
0,8	0	0,00904	0,000859	0,083549	0,00344	0,03101
1	0	0	0	0	0,00115	0,0168



Р и с. 6. Кривые ошибок для 20% внедрения
F i g. 6. Error curves for 20% implementation

Следует отметить, что для реальных изображений со встроенной информацией объём скрытых данных может варьироваться, при этом даже вполне естественные цифровые изображения имеют определённую долю шума, характерного для следов применения стеганографии – каждый исследованный алгоритм показывает, что в чистом изображении есть несколько процентов скрытой информации. Поэтому для определения конкретного изображения в ту или иную категорию необходимо выбрать пороговое значение (таблица 1). Его можно определять как среднее по всем алгоритмам, так и для каждого из них в отдельности. С учётом неизвестного объёма скрытой информации в качестве базового порога по умолчанию в данной работе экспериментально подобрано значение в 20% от общего объёма изображения.

Среди рассмотренных алгоритмов для выборки из нескольких тысяч цветных широкоформатных фото в формате PNG более точным относительно других оказался комбинированный алгоритм (рис. 6), учитывающий среднее по каждому конкретному детектору – он показывает примерно 90% точности выявления изображений, содержащих скрытые данные. Методы Хи-квадрат, RS-анализ и парный анализ имеют примерно одинаковую и тоже относительно высокую точность обнаружения заполненных стегоконтейнеров.



Р и с. 7. Кривые ошибок для 7.5% внедрения
F i g. 7. Error curves for 7.5% implementation

При уменьшении процента изменённых при внедрении пикселей ниже порога в 5-7% практическая точность стегоанализа при помощи рассмотренных алгоритмов начинает резко снижаться (рисунок 7) вплоть до 50% вероятности успешного определения при минимальных значениях объёма внедрённой информации. Однако при 7.5% внедрения точность среднего значения работы алгоритмов всё ещё продолжает составлять порядка 80%. При увеличении объёма встраивания изменённых пикселей сохраняется высокий процент распознавания.

Обсуждение и заключение

Таким образом, в работе представлен обзор применения методов стегоанализа, их классификация, Рассмотрены некоторые популярные структурные и статистические стегоаналитические алгоритмы, для сравнения точности работы которых проведены вычислительные эксперименты с использованием разработанного исследовательского программного комплекса, построены ROC-кривые. Практическим применением разработанного программного комплекса является проведение в университете лабораторных работ по изучению методов стегоанализа, а также исследование свойств стегоаналитических алгоритмов.

Список использованных источников

[1] Евсютин О. О., Кокурина А. С., Мещеряков Р. В. Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «Интернете вещей» // Компьютерная оптика. 2019. Т. 43, № 1. С. 137-154. https://doi.org/10.18287/2412-6179-2019-43-1-137-154
[2] Chowdhuri P., Pal P., Si T. A novel steganographic technique for medical image using SVM and IWT // Multimedia Tools and Applications. 2023. Vol. 82, issue 13. P. 20497-20516. https://doi.org/10.1007/s11042-022-14301-0
[3] Авсентьев О. С., Цыганов К. А. Функциональная модель процесса реализации угрозы утечки информации по скрытому стеганографическому каналу // Вестник Воронежского института МВД России. 2024. № 1. С. 36-49. EDN: YTALJK
[4] Грачев Я. Л., Сидоренко В. Г. Стегоанализ методов скрытия информации в графических контейнерах // Надежность. 2021. Т. 21, № 3. С. 39-46. https://doi.org/10.21683/1729-2646-2021-21-3-39-46
[5] On the Capacity and Security of Steganography Approaches: An Overview / A. K. Hmood [et al.] // Journal of Applied Sciences. 2010. Vol. 10, issue 16. P. 1825-1833. https://doi.org/10.3923/jas.2010.1825.1833
[6] Eid W. M., Alotaibi S. S., Alqahtani H. M., Saleh S. Q. Digital Image Steganalysis: Current Methodologies and Future Challenges // IEEE Access. 2022. Vol. 10. p. 92321-92336. https://doi.org/10.1109/ACCESS.2022.3202905
[7] Comprehensive Exploration of Data Security Techniques Using Image Steganography / V. Singh [et al.] // 2024 4th International Conference on Sustainable Expert Systems (ICSES). Kaski, Nepal: IEEE Press, 2024. P. 396-401. https://doi.org/10.1109/ICSES63445.2024.10763010
[8] Сизов А. С., Никутин Е. И., Котенко С. В. Обзор и тенденции развития методов анализа стеганографических сообщений // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2013. № 4. С. 43-48. EDN: RXGKFX
[9] A Review of Image Steganography Tools / A. Kumar [et al.] // International Journal of Computers and their Applications. 2023. Vol. 30, No. 1. P. 75-87.
[10] Hassan M., Amin M., Mahdi S. Steganalysis Techniques and Comparison of Available Softwares // Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC-SDSP 2020, Cyperspace, 28-30 June 2020. EAI, 2020. http://dx.doi.org/10.4108/eai.28-6-2020.2297970
[11] Veena S. T., Arivazhagan S. Forensic steganalysis for identification of steganography software tools using multiple format image // International Journal of Informatics and Communication Technology. 2021. Vol. 10, No. 3. 188-197. http://doi.org/10.11591/ijict.v10i3.pp188-197
[12] Dhawan S., Gupta R. Analysis of various data security techniques of steganography: A survey // Information Security Journal: A Global Perspective. 2020. Vol. 30, issue 2. P. 63-87. https://doi.org/10.1080/19393555.2020.1801911
[13] Вильховский Д. Э. Обзор методов стеганографического анализа изображений в работах зарубежных авторов // Математические структуры и моделирование. 2020. № 4(56). С. 75-102. https://doi.org/10.24147/2222-8772.2020.4.75-102
[14] Selvaraj A., Ezhilarasan A., Wellington S. L. J., Sam A. R. Digital image steganalysis: A survey on paradigm shift from machine learning to deep learning based techniques // IET Image Processing. 2021. Vol. 15, issue 2. P. :504-522. https://doi.org/10.1049/ipr2.12043
[15] Islam M. A., Riad M. A.-A. K., Pias T. S. Performance Analysis of Steganography Tools // 2020 2nd International Conference on

Advanced Information and Communication Technology (ICAICT). Dhaka, Bangladesh: IEEE Press, 2020. P. 428-433. http://doi.org/10.1109/ICAICT51780.2020.9333473

[16] Belim S. V., Vilkhovskiy D. E. Algorithm for detection of steganographic inserts type LSB-substitution on the basis of an analysis of the zero layer // Journal of Physics: Conference Series. 2018. Vol. 944. Article number: 012012. http://doi.org/10.1088/1742-6596/944/1/012012

[17] Ejidokun T., Omitola O. O., Nnamah I., Adeniji K. Implementation and Comparative Analysis of Variants of LSB Steganographic Method // 2022 30th Southern African Universities Power Engineering Conference (SAUPEC). Durban, South Africa: IEEE Press, 2022. P. 1-4. http://doi.org/10.1109/SAUPEC55179.2022.9730643

[18] Ghosh B. R. A Comparative Study of LSB based Statistical Steganalysis and Gray Level Co-Occurrence Matrix based Blind Image Steganalysis // International Journal of Computer Sciences and Engineering. 2022. Vol. 10, issue 4. P. 1-5. http://doi.org/10.26438/ijcse/v10i4.15

[19] Jamatia R., Bhuyan B. Cover selection for image steganography determined by distinct characteristics // 2023 12th International Conference on Advanced Computing (ICoAC). Chennai, India: IEEE Press, 2023. P. 1-8. http://doi.org/10.1109/ICoAC59537.2023.10249307

[20] Шумская О. О., Железны М. Адаптивный алгоритм встраивания информации в сжатые JPEG-изображения на основе операции замены // Информационно-управляющие системы. 2018. № 5(96). С. 44-56. http://doi.org/10.31799/1684-8853-2018-5-44-56

[21] Коржик В. И., Нгуен З. К., Даньшина А. В. Обнаружение стегосистем, использующих погружение конфиденциальной информации в контуры изображения // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13, № 5. С. 75-85. http://doi.org/10.36724/2409-5419-2021-13-5-75-85

[22] Dumitrescu S., Wu X., Memon N. On steganalysis of random LSB embedding in continuous-tone images // Proceedings. International Conference on Image Processing. Vol. 3. Rochester, NY, USA: IEEE Press, 2002. P. 641-644. http://doi.org/10.1109/ICIP.2002.1039052

[23] Megias D., Lerch-Hostalot D. Subsequent Embedding in Targeted Image Steganalysis: Theoretical Framework and Practical Applications // IEEE Transactions on Dependable and Secure Computing. 2023. Vol. 20, No. 02. P. 1403-1421. http://doi.org/10.1109/TDSC.2022.3154967

[24] Тимофеев М. В., Дудоладова П. Г. Исследование инструментов для стеганографии // Современные научные исследования и разработки. 2019. № 1(30). С. 1016-1019. EDN: VWNDMI

[25] Akbar M. H., Sunardi, Riadi I. Analysis of Steganographic on Digital Evidence using General Computer Forensic Investigation Model Framework // International Journal of Advanced Computer Science and Applications. 2020. Vol. 11, No. 11. P. 315-323. http://dx.doi.org/10.14569/IJACSA.2020.0111141

Поступила 20.02.2024; одобрена после рецензирования 29.03.2024; принята к публикации 16.05.2024.

Об авторах:

Банников Андрей Игоревич, аспирант кафедры информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества, ФГБОУ ВО «Российский государственный социальный университет» (129226, Российская Федерация, г. Москва, ул. Вильгельма Пика, д. 4, стр. 1), **ORCID: https://orcid.org/0009-0000-2384-3324,** 123bannikov.a.i@gmail.com

Мельникова Елена Анатольевна, доцент кафедры информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества, ФГБОУ ВО «Российский государственный социальный университет» (129226, Российская Федерация, г. Москва, ул. Вильгельма Пика, д. 4, стр. 1), кандидат физико-математических наук, **ORCID: https://orcid.org/0000-0003-1997-1846,** Ya.e.melnikova@yandex.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] Evsutin O.O., Kokurina A.S., Meshcheryakov R.V. A review of the methods of embedding information in digital objects for security in the Internet of things. *Computer Optics*. 2019;43(1):137-154. (In Russ., abstract in Eng.) https://doi.org/10.18287/2412-6179-2019-43-1-137-154

[2] Chowdhuri P., Pal P., Si T. A novel steganographic technique for medical image using SVM and IWT. *Multimedia Tools and Applications*. 2023;82(13):20497-20516. https://doi.org/10.1007/s11042-022-14301-0

[3] Avsentev O.S., Tsyganov K.A. Functional model of the process of implementing the information leak threat by an insider through a hidden steganography channel. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia.* 2024;(1):36-49. (In Russ., abstract in Eng.) EDN: YTALJK

[4] Grachev Ya.L., Sidorenko V.G. Steganalysis of the methods of concealing information in graphic containers. *Dependability*. 2021;21(3):39-46. (In Russ., abstract in Eng.) https://doi.org/10.21683/1729-2646-2021-21-3-39-46

[5] Hmood A.K., Jalab H.A., Kasirun Z.M., Zaidan B.B., Zaidan A.A. On the Capacity and Security of Steganography Approaches: An Overview. *Journal of Applied Sciences*. 2010;10(16):1825-1833. https://doi.org/10.3923/jas.2010.1825.1833

[6] Eid W.M., Alotaibi S.S., Alqahtani H.M., Saleh S.Q. Digital Image Steganalysis: Current Methodologies and Future Challenges. *IEEE Access*. 2022;10:92321-92336. https://doi.org/10.1109/ACCESS.2022.3202905

[7] Singh V., Sharma M., Shirode A., Mirchandani S. A Comprehensive Exploration of Data Security Techniques Using Image Steganography. In: 2024 4th International Conference on Sustainable Expert Systems (ICSES). Kaski, Nepal: IEEE Press; 2024. p. 396-401. https://doi.org/10.1109/ICSES63445.2024.10763010

[8] Sizov A.S., Nikutin E.I., Kotenko S.V. Overview and trends of the analysis methods of steganographic messages development. *Proceedings of the Southwest State University. Series: IT Management, Computer Science, Computer Engineering. Medical Equipment Engineering.* 2013;(4):43-48. (In Russ., abstract in Eng.) EDN: RXGKFX

[9] Kumar A., Jamnadas H., Sharma V., Muyeen S. M., Shawkat Ali A. B. M. A Review of Image Steganography Tools. *International Journal of Computers and their Applications*. 2023;30(1):75-87.

[10] Hassan M., Amin M., Mahdi S. Steganalysis Techniques and Comparison of Available Softwares. In: Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC-SDSP 2020, Cyperspace, 28-30 June 2020. EAI; 2020. http://dx.doi.org/10.4108/eai.28-6-2020.2297970

[11] Veena S.T., Arivazhagan S. Forensic steganalysis for identification of steganography software tools using multiple format image. *International Journal of Informatics and Communication Technology*. 2021;10(3):188-197. http://doi.org/10.11591/ijict.v10i3.pp188-197

[12] Dhawan S., Gupta R. Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective.* 2020;30(2):63-87. https://doi.org/10.1080/19393555.2020.1801911

[13] Vilkhovskiy D.E. A Survey of Steganalysis Methods in the Papers of Foreign Authors. *Mathematical Structures and Modeling.* 2020;(4):75-102. (In Russ., abstract in Eng.) https://doi.org/10.24147/2222-8772.2020.4.75-102

[14] Selvaraj A., Ezhilarasan A., Wellington S.L.J., Sam A.R. Digital image steganalysis: A survey on paradigm shift from machine learning to deep learning based techniques. *IET Image Processing*. 2021;15(2):504-522. https://doi.org/10.1049/ipr2.12043

[15] Islam M.A., Riad M.A.-A.K., Pias T.S. Performance Analysis of Steganography Tools. In: 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT). Dhaka, Bangladesh: IEEE Press; 2020. p. 428-433. http://doi.org/10.1109/ICAICT51780.2020.9333473

[16] Belim S.V., Vilkhovskiy D.E. Algorithm for detection of steganographic inserts type LSB-substitution on the basis of an analysis of the zero layer. *Journal of Physics: Conference Series*. 2018;944:012012. http://doi.org/10.1088/1742-6596/944/1/012012

[17] Ejidokun T., Omitola O.O., Nnamah I., Adeniji K. Implementation and Comparative Analysis of Variants of LSB Steganographic Method. In: 2022 30th Southern African Universities Power Engineering Conference (SAUPEC). Durban, South Africa: IEEE Press; 2022. p. 1-4. http://doi.org/10.1109/SAUPEC55179.2022.9730643

[18] Ghosh B.R.A Comparative Study of LSB based Statistical Steganalysis and Gray Level Co-Occurrence Matrix based Blind Image Steganalysis. *International Journal of Computer Sciences and Engineering.* 2022;10(4):1-5. http://doi.org/10.26438/ijcse/v10i4.15

[19] Jamatia R., Bhuyan B. Cover selection for image steganography determined by distinct characteristics. In: 2023 12th International Conference on Advanced Computing (ICoAC). Chennai, India: IEEE Press; 2023. p. 1-8. http://doi.org/10.1109/ICoAC59537.2023.10249307

[20] Shumskaya O.O., Zelezny M. Adaptive algorithm of replacement-based embedding of data into compressed JPEG images. *Informatsionno-upravliaiushchie sistemy* = Information and Control Systems. 2018;(5):44-56. (In Russ., abstract in Eng.) http://doi.org/10.31799/1684-8853-2018-5-44-56

[21] Korzhik V.I., Nguyen Z.K., Danshina A.V. Detection of stegosystem using embedding into contours of images. *H&ES Reserch.* 2021;13(5):75-85. (In Russ., abstract in Eng.) http://doi.org/10.36724/2409-5419-2021-13-5-75-85

[22] Dumitrescu S., Wu X., Memon N. On steganalysis of random LSB embedding in continuous-tone images. In: Proceedings. International Conference on Image Processing. Vol. 3. Rochester, NY, USA: IEEE Press; 2002. p. 641-644. http://doi.org/10.1109/ICIP.2002.1039052

[23] Megias D., Lerch-Hostalot D. Subsequent Embedding in Targeted Image Steganalysis: Theoretical Framework and Practical Applications. *IEEE Transactions on Dependable and Secure Computing*. 2023;20(02):1403-1421. http://doi.org/10.1109/TDSC.2022.3154967

[24] Timofeev M.V., Dudoladova P.G. An investigation tools for Steganography. *Sovremennye nauchnye issledovanija i razrabotki.* 2019;(1):1016-1019. (In Russ., abstract in Eng.) EDN: VWNDMI

[25] Akbar M.H., Sunardi, Riadi I. Analysis of Steganographic on Digital Evidence using General Computer Forensic Investigation Model Framework. *International Journal of Advanced Computer Science and Applications.* 2020;11(11):315-323. http://dx.doi.org/10.14569/IJACSA.2020.0111141

Submitted 20.02.2024; approved after reviewing 29.03.2024; accepted for publication 16.05.2024.

About the authors:

Andrey I. Bannikov, Postgraduate Student of the Chair of Information Technologies, Artificial Intelligence and Social Technologies of Digital Society, Russian State Social University (4 Wilhelm Pieck St., build. 1, Moscow 129226, Russian Federation), **ORCID: https://orcid.org/0009-0000-2384-3324,** 123bannikov.a.i@gmail.com

Elena A. Melnikova, Associate Professor of the Chair of Information Technologies, Artificial Intelligence and Social Technologies of Digital Society, Russian State Social University (4 Wilhelm Pieck St., build. 1, Moscow 129226, Russian Federation), Cand. Sci. (Phys.-Math.), **ORCID: https://orcid.org/0000-0003-1997-1846,** Ya.e.melnikova@yandex.ru

All authors have read and approved the final manuscript.