



УДК 004.932.2

DOI 10.52575/2687-0932-2025-52-2-476-484

EDN OLGWST

Об устойчивости стеганографических методов для защиты цифровых изображений в условиях внешних воздействий

Чурсин Д.С

ООО «ЦЕНТРПРОГРАММСИСТЕМ»,
Россия, 308008, г. Белгород, ул. Восточная, д. 71, кв. 501
dima.chursin@bk.ru

Аннотация. В данной статье представлен комплексный анализ устойчивости контрольной информации, внедренной в цифровые изображения, к внешним воздействиям. Исследование сосредоточено на трех популярных методах стеганографии: замене наименьшего значащего бита (LSB), методе Коха и Жао, а также методе расширения спектра. Основная цель исследования заключается в оценке способности этих методов сохранять целостность контрольной информации в условиях преднамеренного наложения шума на стегоконтейнеры. Результаты исследования представлены в виде графиков, демонстрирующих зависимость вероятности извлечения ошибки от уровня наложенного шума. Проведенная сравнительная оценка позволяет сделать выводы о сравнительной эффективности и устойчивости каждого из методов к внешним воздействиям. Полученные данные свидетельствуют о том, что не все методы демонстрируют определенную степень устойчивости, их эффективность варьируется в зависимости от уровня шума и специфики метода. Эти результаты имеют важное значение для разработки более надежных методов защиты цифровых изображений, особенно в контексте современных вызовов, связанных с обеспечением информационной безопасности и защитой авторских прав.

Ключевые слова: стеганография, контрольная информация, цифровые изображения, защита изображений, аутентификация изображений, устойчивость к внешним воздействиям, метод LSB, метод Коха и Жао, метод расширения спектра, цифровой водяной знак (ЦВЗ), зашумление изображения, PSNR, SSIM

Для цитирования: Чурсин Д.С. 2025. Об устойчивости стеганографических методов для защиты цифровых изображений в условиях внешних воздействий. *Экономика. Информатика*, 52(2): 476–484. DOI 10.52575/2687-0932-2025-52-2-476-484 EDN OLGWST

Analysis of the Stability of Steganographic Methods for Protecting Digital Images under Conditions of External Influences

Dmitry S. Chursin

CENTERPROGRAMSYSTEM LLC
71 Vostochnaya St., Belgorod 308008, Russia
dima.chursin@bk.ru

Abstract. This article analyzes the stability of control information embedded in digital images to external influences using various steganographic methods. The principles of introducing control information into images using popular steganography methods such as least significant bit substitution (LSB), the Koch and Zhao method, and the spectrum expansion method are considered. The study involves extracting control information from digital images that have been subjected to preliminary noise overlay. The main focus is on assessing the stability of each of the methods in conditions where the stegocontainer (an image with embedded

© Чурсин Д.С., 2025

information) is exposed to noise. The results of the study are presented in the form of graphs demonstrating the dependence of the probability of extracting an error from a stegocontainer on the level of pre-applied noise. The comparative assessment allows us to draw conclusions about the comparative effectiveness and resistance of each of the methods to external influences, which may be useful for developing more reliable methods of protecting digital images.

Keywords: steganography, control information, digital images, image protection, image authentication, resistance to external influences, LSB method, Koch and Zhao method, spectrum expansion method, digital watermark, image noise, PSNR, SSIM

For citation: Chursin D.S. 2025. Analysis of the Stability of Steganographic Methods for Protecting Digital Images under Conditions of External Influences. *Economics. Information technologies*, 52(2): 476–484 (in Russian). DOI 10.52575/2687-0932-2025-52-2-476-484 EDN OLGWST

Введение

В последние годы цифровые изображения стали неотъемлемой частью многих сфер деятельности, включая медицину, спутниковую съемку, безопасность и коммуникации. Этот рост обусловлен значительными достижениями в технологиях цифровой обработки изображений, что, в свою очередь, подчеркивает необходимость разработки надежных методов защиты и аутентификации таких изображений. Одним из наиболее эффективных подходов к обеспечению защиты является внедрение контрольной информации в цифровые изображения с использованием стеганографических методов.

Стеганография позволяет интегрировать дополнительные данные в цифровые изображения таким образом, что они остаются незаметными для человеческого глаза, но могут быть извлечены и использованы при необходимости [Конахович, 2006]. Современные стеганографические методы постоянно развиваются, чтобы соответствовать новым требованиям безопасности и вызовам. Среди них можно выделить как классические методы, такие как замена наименьших значащих битов (LSB), так и более сложные техники, включающие преобразования в частотной области, например, дискретное косинусное преобразование (ДКП) и дискретное вейвлет-преобразование (ДВП), а также методы расширения спектра.

В условиях, когда ежедневно создаются и распространяются миллионы уникальных изображений, контроль за их распространением приобретает особую важность. Это создает предпосылки для злоумышленников использовать эти изображения в своих целях, что требует применения стеганографических методов для подтверждения подлинности изображений и контроля авторских прав [ГОСТ Р 7.0.1-2003]. Однако злоумышленники также разрабатывают новые методы для обхода таких мер защиты [Федосенко, 2023]. Одним из таких методов является наложение шума на изображения, что приводит к разрушению контрольной информации, но при этом сохраняет видимое качество изображения. В результате становится невозможным восстановление контрольной информации, что делает невозможным контроль над такими изображениями.

В данной статье проводится анализ устойчивости контрольной информации, внедренной в цифровые изображения, к внешним воздействиям. Исследование охватывает различные популярные методы стеганографии, включая метод LSB, метод Коха и Жао, а также метод расширения спектра. Основная цель исследования заключается в оценке сравнительной устойчивости этих методов к внешним воздействиям, таким как наложение шума, и в определении их эффективности при извлечении контрольной информации.

Для достижения этой цели были проведены эксперименты по наложению шума с различными уровнями зашумленности на стегоконтейнеры и последующему извлечению контрольной информации. Результаты исследования представлены в виде графиков, демонстрирующих зависимость вероятности извлечения ошибки от уровня наложенного шума. Проведенная сравнительная оценка позволяет сделать выводы о сравнительной эффективности и устойчивости каждого из методов, что может быть полезно для разработки более надежных методов защиты цифровых изображений.

Эти результаты имеют важное значение для обеспечения информационной безопасности и защиты авторских прав в условиях постоянно развивающихся технологий и растущих угроз.

Описание исследуемых методов стеганографии и их характеристики

В данном исследовании были выбраны три метода стеганографии для анализа их устойчивости к внешним воздействиям:

1) метод наименьшего значащего бита (НБЗ/LSB) [Грибунин, Оков, Туринцев, 2009] – один из наиболее распространенных методов, основанный на замене наименьших значащих битов в пикселях изображения;

2) метод Коха и Жао [Демидчук, 2012; Koch, 1995; Zhao, 1995] – более сложный подход, использующий модификацию коэффициентов дискретного косинусного преобразования (ДКП) для внедрения скрытой информации;

3) метод расширения спектра [Иванова, Семенов, 2021] – метод, основанный на принципах расширения спектра, где информация распределяется по всему спектру частот изображения.

Эти методы широко используются в области защиты цифровых изображений и представляют собой различные подходы к внедрению и извлечению скрытой информации.

В качестве объектов исследования использовались спутниковые снимки размером 400x400 (рис. 1). В качестве контрольной информации был использован цифровой водяной знак (ЦВЗ) [Гонсалес, 2006], представляющий собой QR-код размером 50x50 (рис. 2).



Рис. 1. Цифровые изображения
Fig. 1. Digital images

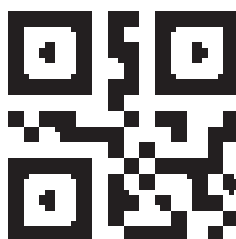


Рис. 2. ЦВЗ
Fig. 2. Digital watermark

Метод наименьшего значащего бита является наиболее широко используемым и простым методом стеганографии в пространственной области. Его главное преимущество заключается в том, что для его реализации не требуется значительных вычислительных ресурсов, что делает его доступным для использования даже на устройствах с ограниченной производительностью. Процесс извлечения контрольной информации с помощью метода LSB также отличается простотой: для

восстановления скрытых данных достаточно иметь только стегоконтейнер (изображение, содержащее встроенную информацию). Это упрощает процесс восстановления и делает метод LSB особенно привлекательным для задач, где важна быстрота и простота обработки.

Метод Коха и Жао считается одним из наиболее популярных методов стеганографии в частотной области. Однако, в отличие от простого в реализации метода LSB, этот метод требует более сложного подхода. Он основан на разбиении исходного изображения на блоки размером 8×8 , что накладывает ограничения на размер и форму изображения: оно должно быть квадратным и иметь размеры, кратные восьми.

Сложность реализации метода Коха и Жао обусловлена несколькими факторами. Во-первых, внедрение информации происходит путем выбора двух коэффициентов ДКП из средних частот. Во-вторых, используется защитная маркировка, которая заключается в сравнении модулей значений выбранных коэффициентов. Если необходимо, значение одного из коэффициентов изменяется в зависимости от бита встраиваемого ЦВЗ. Для маркировки блока битом водяного знака применяются определенные условия, и, если они не выполняются, коэффициенты корректируются для обеспечения надежности внедрения [Шелухин, Канаев, 2024].

Для извлечения контрольной информации в методе Коха и Жао требуется наличие как самого стегоконтейнера, так и защитной маркировки, которая представляет собой массив координат. Этот массив координат играет ключевую роль, так как он указывает, какие именно коэффициенты ДКП были изменены в процессе внедрения информации. Наличие защитной маркировки является критическим условием для успешного извлечения данных, поскольку без нее становится крайне сложно или даже невозможно определить, какие именно части изображения содержат скрытую информацию.

Метод расширения спектра считается одним из наиболее популярных методов стеганографии в области цифровой обработки сигналов. Однако из всех вышеуказанных данный метод самый сложный и требует значительных вычислительных ресурсов для внедрения. Метод расширения спектра также имеет ограничения на размер и форму изображения: оно должно быть квадратным и иметь размер, кратный размеру ЦВЗ.

В методе расширения спектра прямой последовательностью информационный сигнал модулируется с помощью функции, принимающей псевдослучайные значения в заданных пределах. Эта функция умножается на константу, представляющую собой частоту (скорость) следования элементарных посылок сигнала. В результате получается псевдослучайный сигнал, который содержит составляющие на всех частотах, что приводит к расширению спектра и распределению энергии сигнала в широком диапазоне частот [Шелухин, Канаев, 2024].

Для модуляции в данном методе используется алгоритм, в котором каждый бит сообщения представляется в виде базисной функции, размерность которой соответствует размеру изображения.

Для эффективного скрытия информации требуется значительное количество базисных функций, ортогональных к типичным изображениям. Однако кодирование изображений требует меньшего количества базисных функций, что приводит к конфликту при компрессии. Идеальная схема компрессии не способна полностью отобразить базисы, использованные для скрытия, что может привести к потере информации.

Для извлечения контрольной информации в методе расширения спектра требуется как наличие самого стегоконтейнера, так и знание общего количества базисных функций, использованных при внедрении, что является размером ЦВЗ.

Оценка устойчивости стегоконтейнеров к шуму: методология, критерии и результаты

Пусть $\hat{f}_{i,k}$ представляет собой исходный стегоконтейнер. Зашумленный стегоконтейнер $\hat{f}_{i,k}^*$ может быть описан следующим образом:

$$\hat{f}_{i,k}^* = \hat{f}_{i,k} + \eta, \quad (1)$$

где η – распределенный шум, определяемый как:

$$\eta = b \cdot rand(X, Y), \quad (2)$$

где X, Y – размеры изображения;

b – амплитуда накладываемого шума, которая рассчитывается по формуле:

$$b = \sqrt{\frac{\sum_i \sum_k \hat{f}_{i,k}}{X \cdot Y} \cdot k^2}, \quad (3)$$

где k – уровень зашумленности.

На основе приведенного выше отношения (1) было произведено наложение шума на стегоконтейнеры с различными уровнями зашумленности (3). После этого из зашумленных стегоконтейнеров извлекалась контрольная информация. Основная цель исследования – определить вероятность ошибки P_Δ на каждом уровне зашумленности путем побитового сравнения векторов исходной и извлеченной контрольной информации:

$$P_\Delta = \left(\frac{\Delta}{L}\right), \quad (4)$$

где L – длина извлеченного вектора с контрольной информацией:

$$\Delta = \sum_{i=1}^L 1_{\vec{x} \neq \vec{x}^*}, \quad (5)$$

где $\vec{x}$ и $\vec{x}^*$ – исходный и извлеченный вектор с контрольной информацией соответственно.

Для сохранения качества изображения и его «читаемого внешнего вида» был определен предел зашумленности. Для этого использовались следующие метрики:

1. PSNR (Peak Signal-to-Noise Ratio [Tanchenko, 2014; Mohammad, Al-Halabi, Monthy, 2019]:

$$PSNR = 10 \cdot \log_{10} \left(\frac{255^2}{MSE} \right), \quad (6)$$

где MSE – среднеквадратичная ошибка между исходным изображением и зашумленным изображением:

$$MSE = \frac{1}{X \cdot Y} \sum_{x=1}^X \sum_{y=1}^Y (\hat{f}_{i,k}(x, y) - \hat{f}_{i,k}^*(x, y))^2; \quad (7)$$

2. SSIM (Structural Similarity Index [Mohammad, Al-Halabi, Monthy, 2019; Wang, Bovik, Sheikh, Simoncelli, 2004]:

$$SSIM = \frac{(2\mu_{f_{i,k}}\mu_{f_{i,k}^*} + C_1)(2\sigma_{f_{i,k}f_{i,k}^*} + C_2)}{(\mu_{f_{i,k}}^2 + \mu_{f_{i,k}^*}^2 + C_1)(\sigma_{f_{i,k}}^2 + \sigma_{f_{i,k}^*}^2 + C_2)}, \quad (8)$$

где $\mu_{f_{i,k}}$ и $\mu_{f_{i,k}^*}$ – средние значения пикселей исходного и зашумленного стегоконтейнера соответственно;

$\sigma_{f_{i,k}}^2$ и $\sigma_{f_{i,k}^*}^2$ – дисперсии исходного и зашумленного стегоконтейнера;

$\sigma_{f_{i,k}f_{i,k}^*}$ – ковариация между исходным и зашумленным стегоконтерами;

C_1 и C_2 – константы, которые добавляются для стабильности вычислений:

$$\begin{aligned} C_1 &= (0,01 \cdot 255)^2 \\ C_2 &= (0,03 \cdot 255)^2; \end{aligned} \quad (9)$$

3. Визуальный осмотр.

По общепринятым критериям для оценки качества метрики должны иметь следующие значения: PSNR не менее 30 дБ; SSIM не менее 0,9 [Avcibas, Sankur, Sayood, 2002].

Результаты вычисления предела уровня зашумленности представлены в табл. 1. Из таблицы следует, что предельным уровнем зашумленности, при котором стегоконтейнер сохраняет свое качество, является уровень 10^{-5} .

Таблица 1
Table 1

Результаты вычисления предела уровня зашумленности
The results of calculating the noise level limit

Уровень зашумленности	Метрики	Цифровые изображения		
		автомагистраль	рельефы	кварталы
10^{-3}	<i>PSNR</i>	5,2596	5,22	5,8603
	<i>SSIM</i>	0,19709	0,089148	0,21383
	<i>Визуальный осмотр</i>	Не читаемо	Не читаемо	Не читаемо
10^{-4}	<i>PSNR</i>	20,6967	23,6248	19,1981
	<i>SSIM</i>	0,89361	0,86158	0,91205
	<i>Визуальный осмотр</i>	Появляется рябь	Появляется рябь	Появляется рябь
10^{-5}	<i>PSNR</i>	40,4674	43,3896	38,9593
	<i>SSIM</i>	0,99819	0,99789	0,9988
	<i>Визуальный осмотр</i>	Четкое изображение	Четкое изображение	Четкое изображение

На основе вычисленных вероятностей ошибки на различных уровнях зашумленности были построены графики зависимости, которые наглядно демонстрируют устойчивость методов стеганографии к внешним воздействиям. Эти графики представлены на рис. 3–6.

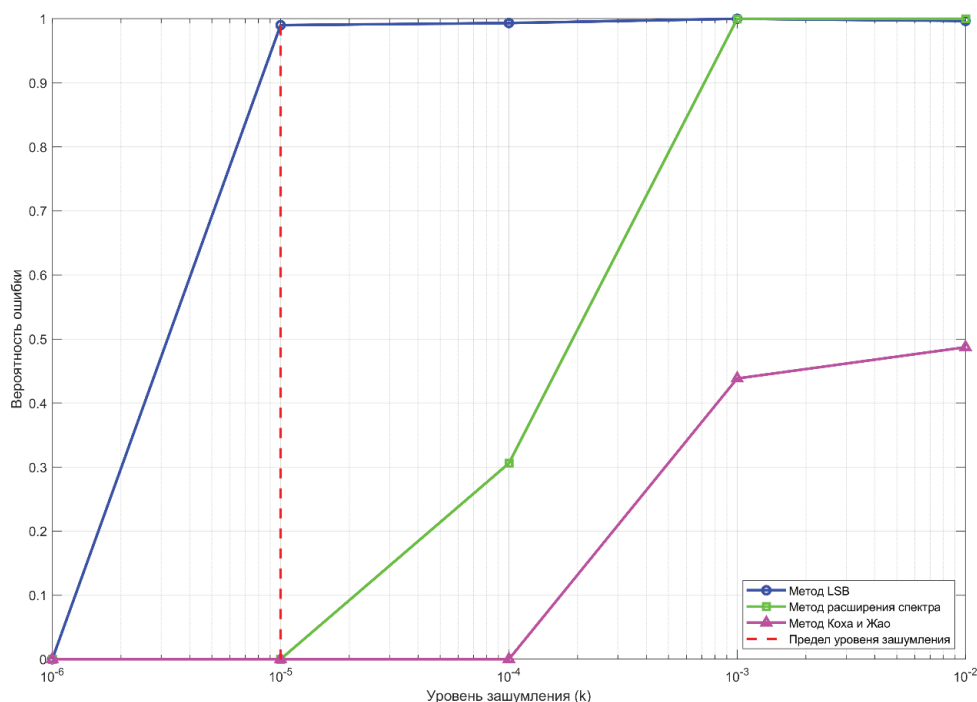


Рис. 3. График зависимости (автомагистраль)
Fig. 3. Dependency schedule (motorway)

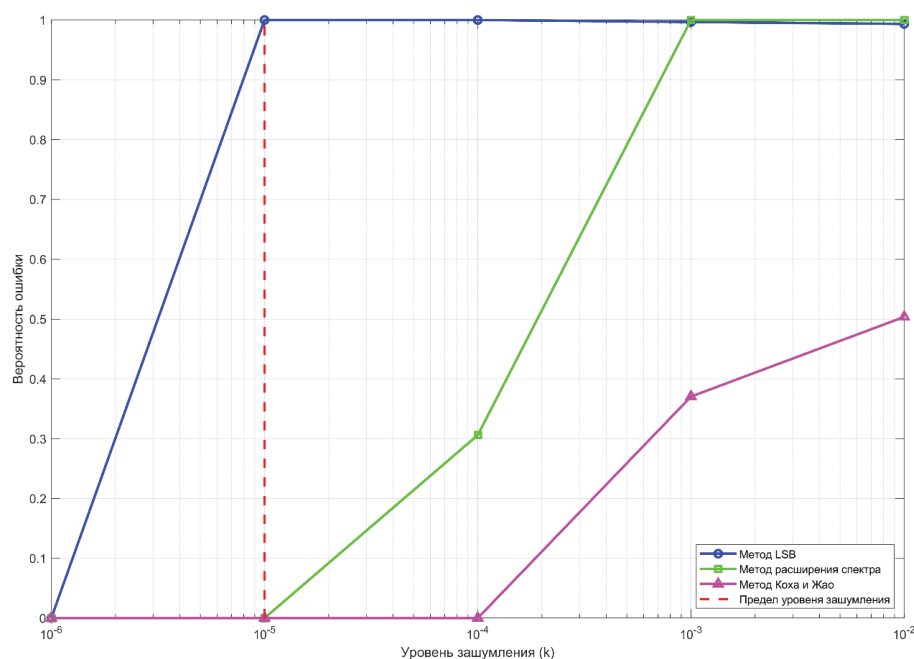


Рис. 4. График зависимости (Рельефы)
Fig. 4. Dependency graph (Reliefs)

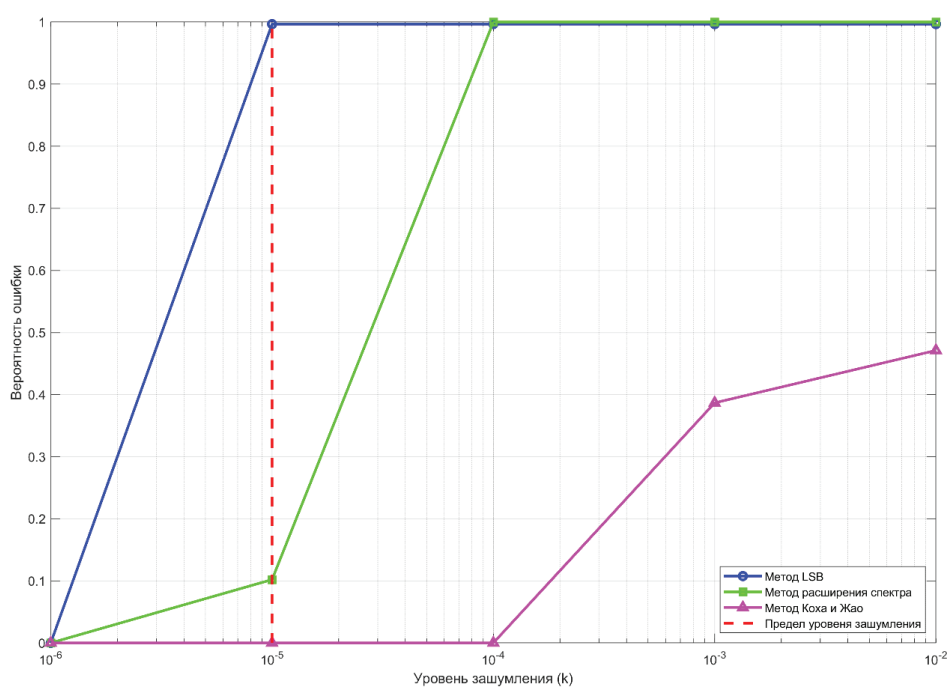


Рис. 5. График зависимости (Кварталы)
Fig. 5. Dependency graph (Neighborhoods)

Закключение

Настоящее исследование представляет детальный анализ эффективности различных методов стеганографии в условиях наложения шума на цифровые изображения. Основываясь на полученных результатах, можно сделать следующие выводы:

1. Метод Коха и Жао продемонстрировал наибольшую устойчивость к внешним воздействиям среди всех исследованных методов. Даже при высоких уровнях зашумленности, не превышающих установленный предел, вероятность ошибок извлечения контрольной

информации в некоторых случаях составляла 0. Максимальная вероятность ошибки не превышала 0,5, что свидетельствует о высокой надежности этого метода. Таким образом, метод Коха и Жао является наиболее подходящим выбором для приложений, требующих высокой степени защиты информации в условиях потенциального воздействия шума.

2. Метод расширения спектра также показал хорошие результаты, особенно в контексте конкретных изображений. В двух из трех случаев этот метод продемонстрировал высокую эффективность, что указывает на его потенциал в определенных условиях. Однако его успешность в значительной степени зависит от характеристик самого изображения, что может ограничивать его применение в более широком контексте. Это подчеркивает важность тщательного подбора параметров метода в зависимости от конкретных условий и характеристик изображений.

3. Метод наименьшего значащего бита оказался наименее эффективным в условиях зашумленности. Его низкая устойчивость к внешним воздействиям приводит к высокой вероятности ошибок извлечения информации. Это делает метод LSB непригодным для использования в ситуациях, где высока вероятность воздействия шума или других искажений.

Результаты исследования подчеркивают важность выбора подходящего метода стеганографии в зависимости от конкретных условий и требований к защите информации. Для обеспечения надежной защиты в условиях потенциального воздействия шума рекомендуется использовать метод Коха и Жао. В случаях, когда характеристики изображения позволяют, метод расширения спектра также может быть эффективным.

Дальнейшие исследования могут быть направлены на разработку более устойчивых и эффективных методов стеганографии, а также на адаптацию существующих методов к новым вызовам в области защиты цифровых изображений. Это может включать в себя разработку гибридных подходов, сочетающих преимущества различных методов, а также использование современных технологий, таких как машинное обучение, для повышения устойчивости и эффективности стеганографических методов.

Список литературы

- Гонсалес Р., Вудс Р. 2006. Цифровая обработка изображений; пер. с англ. П.А. Чочиа. М.: Техносфера, 1070 с.
- ГОСТ Р 7.0.1-2003. ЗНАК ОХРАНЫ АВТОРСКОГО ПРАВА Общие требования и правила оформления. <https://docs.cntd.ru/document/1200032004>
- Грибунин В.Г., Оков И.Н., Туринцев И.В. 2009. Цифровая стеганография. М.: СОЛОН-ПРЕСС, 265 с.
- Демидчук А.И., Чернявский Ю.А. 2012. Алгоритм поиска в изображениях скрытых данных, встроенных методом Коха-Жао. *Информатика*, 1(33): 39–46.
- Иванова Л.В., Семенов Н.С. 2021. Применение метода расширения спектра в системе связи на основе прямой последовательности. *Журнал связи*, 25(2): 45–50
- Конахович Г.Ф. Пузыренко А.Ю. 2006. Компьютерная стеганография. Теория и практика: Учебно-практическое пособие. К.: МК-Пресс, 288 с.
- Левин В.А. 2021. Стеганография и цифровые водяные знаки. Научный мир, 150–175.
- Федосенко М.Ю. 2023. Обзор перспектив использования стеганографии в качестве инструмента обмена скрытыми данными в процессе осуществления правонарушений. Сборник тезисов докладов конгресса молодых ученых. Электронное издание. – СПб: Университет ИТМО. URL: <https://kmu.itmo.ru/digests/article/9974>
- Шелухин О.И., Канаев. С.Д. 2024. Стеганография. Алгоритмы и программная реализация. М.: Горячая линия – Телеком, 592 с.
- Avcibas I., Sankur B., Sayood K. 2002. Statistical evaluating of image quality measures. *Journal of Electronic Imaging*, 11(2): 206–223.
- Koch E., Zhao J. 1995. Towards Robust and Hidden Image Copyright Labeling. IEEE Workshop on Nonlinear Signal and Image Processing, P. 123–132.
- Mohammad A.B., Al-Halabi T., Monthy M. 2019. Comparative Analysis of PSNR and SSIM for Image Quality Assessment. *Journal of Mathematics and Computer Science*, 54–62.
- Tanchenko A. 2014. Visual-PSNR measure of image quality. *Journal of Visual Communication and Image Representation*, 25(5): 874–878.



- Zhao J., Koch E. 1995. Embedding Robust Labels into Images for Copyright Protection. Proc. of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies. Munich, Vienna, P. 242–252.
- Wang Zh., Bovik A.C., Sheikh H. R., Simoncelli E.P. 2004. Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE transactions on image processing*, 13(4):600–12. doi: 10.1109/tip.2003.819861.

References

- Gonzalez R., Woods R. 2006. Digital image processing; translated from English by P.A. Choc. M.: Technosphere, 1070 p.
- GOST R 7.0.1-2003. COPYRIGHT PROTECTION MARK General requirements and design rules. <https://docs.cntd.ru/document/1200032004>
- Gribunin V.G., Okov I.N., Turintsev I.V. 2009. Digital steganography, Moscow: SOLON PRESS, 265 p.
- Demidchuk A.I., Chernyavsky Yu.A. 2012. An algorithm for searching hidden data embedded in images using the Koch-Zhao method. *Informatics*, 1(33): 39–46.
- Ivanova L.V., Semenov N.S. 2021. Application of the spectrum expansion method in a direct sequence communication system. *Communication journal*. 25(2): 45–50
- Konakhovich G.F. Puzyrenko A.Yu. 2006. Computer steganography. Theory and practice: An educational and practical guide. K.: MK-Press, 288 p.
- Levin V.A. 2021. Steganography and digital watermarks. Scientific World, 150–175.
- Fedosenko M.Y. 2023. Review of the prospects of using steganography as a tool for exchanging hidden data in the process of illegal actions. Collection of abstracts of the Congress of Young Scientists. Electronic edition. – St. Petersburg: ITMO University. URL: <https://kmu.itmo.ru/digests/article/9974>
- Shelukhin O.I., Kanaev S.D. 2024. Steganography. Algorithms and software implementation. Moscow: Hotline – Telecom, 592 p.
- Avcibas I., Sankur B., Sayood K. 2002. Statistical evaluating of image quality measures. *Journal of Electronic Imaging*, 11(2): 206–223.
- Koch E., Zhao J. 1995. Towards Robust and Hidden Image Copyright Labeling. *IEEE Workshop on Nonlinear Signal and Image Processing*, P. 123–132.
- Mohammad A.B., Al-Halabi T., Monthy M. 2019. Comparative Analysis of PSNR and SSIM for Image Quality Assessment. *Journal of Mathematics and Computer Science*, 54–62.
- Tanchenko A. 2014. Visual-PSNR measure of image quality. *Journal of Visual Communication and Image Representation*, 25(5): 874–878.
- Zhao J., Koch E. 1995. Embedding Robust Labels into Images for Copyright Protection. Proc. of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies. Munich, Vienna, P. 242–252.
- Wang Zh., Bovik A.C., Sheikh H. R., Simoncelli E.P. 2004. Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE transactions on image processing*, 13(4):600–12. doi: 10.1109/tip.2003.819861.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.

Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 03.04.2025

Поступила после рецензирования 23.05.2025

Принята к публикации 04.06.2025

Received April 3, 2025

Revised May 23, 2025

Accepted June 04, 2025

ИНФОРМАЦИЯ ОБ АВТОРЕ

Чурсин Дмитрий Сергеевич, специалист по внедрению программных продуктов, ООО «ЦЕНТРОГРАММСИСТЕМ», г. Белгород, Россия

INFORMATION ABOUT THE AUTHOR

Dmitry S. Chursin, Software Product Implementation Specialist, CENTERPROGRAMSYSTEM LLC, Belgorod, Russia