оценить, какую реальную выгоду они приносят для различных типов проектов.

Список использованных источников

1. ГОСТ Р ИСО 21500 - 2023. Управление проектами, программами и портфелями проектов. Контекст и основные понятия. – М.: Российский институт стандартизации, 2023.
2. Рассел С., Норвиг П. Искусственный интеллект: современный подход. – М.: Вильямс, 2021. – 1184 с.
3. Руководство к Своду знаний по управлению проектами (PMBOK Guide). 7-е изд. – М.: Олимп–Бизнес, 2021. – 756 с.
4. Три уровня искусственного интеллекта: ANI, AGI, ASI. Интерактивная платформа Neiroset.com // URL: https://neiroset.com/news/336-tri-urovnya-iskusstvennogo-intellekta-ani-agi-asi?ysclid=mh0uapwwdl625337099 (дата обращения 11.10.2025).
5. 14. Agile-манифест // URL: https://agilemanifesto.org/iso/ru/manifesto.html (дата обращения 07.10.2025).

УДК 004.56+003.26

М.Г. Савельева
Белорусский государственный технологический университет
Минск, Беларусь

АНАЛИЗ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ К БАЗОВОЙ КОРРЕЛЯЦИОННОЙ АТАКЕ ЗИГЕНТАЛЕРА

Аннотация. *Работа посвящена исследованию эффективности стегоанализа растрированных текстовых контейнеров (PNG-изображений страниц). Методы стеганографии LSB, DCT, DWT, MPV, GLM, PVD и авторские разработки, тестируются на устойчивость к базовой корреляционной атаке Зигенталера (BCA-атака). Результаты, выраженные в количестве статистических аномалий, показывают различную степень уязвимости методов, выявляя наименее и наиболее устойчивые из них для данного типа носителей.*

M.G. Saveleva
Belarusian State Technological University
Minsk, Belarus

ANALYSIS OF THE STABILITY OF STEGANOGRAPHIC METHODS TO THE BASIC SIEGENTHALER CORRELATION ATTACK

Abstract. *This paper examines the effectiveness of steganalysis of rasterized text containers (PNG page images). Steganographic methods such as LSB, DCT, DWT, MPV, GLM, PVD, and the author's own developments are tested for their resistance to the basic Siegenthaler correlation attack (BCA). The results, expressed as the number of statistical anomalies, demonstrate the varying degrees of vulnerability of the methods, identifying the least and most robust ones for a given type of media.*

Растущая потребность в стеганографии обусловлена требованием безопасной и незаметной передачи информации, а также защитой авторских прав на электронный контент в условиях усиливающегося контроля и угроз в киберпространстве. Существуют методы и инструменты стегоанализа, которые помогают поддерживать баланс между законным использованием стеганографии и предотвращением ее злоупотребления. Однако эффективность выявления скрытой информации в растрированных текстовых контейнерах остается практически не исследованной. Целью работы является оценка устойчивости растрированных текстов к базовой корреляционной атаке Зигенталера, а также эффективность стегоанализа.

Для исследования устойчивости методов стеганографических преобразований использованы 3 изображения-контейнера (растрированные страницы, являющиеся частью статей) формата PNG. Их характеристики рассмотрены в таблице 1.

Таблица 1 – Характеристики изображений-контейнеров

Контейнер	Разрешение	Пикселей всего, N	Размер, КБ
$C1$	2281×3197	7 292 357	396
$C2$	2135×3183	6 795 705	523
$C3$	2158×3133	6 761 014	776

Базовая корреляционная атака Зигенталера – это статистический метод обнаружения скрытых данных, основанный на выявлении аномальных корреляционных зависимостей между элементами стегоконтейнера (в данном случае, пикселями изображения), возникающих в процессе стеганографического преобразования. В

отличие от классического применения к криптоанализу поточных шифров, в стеганографии этот метод адаптирован для обнаружения искажений, которые вносит алгоритм скрытой передачи информации в статистические характеристики носителя. Метод основан на вычислении корреляционных коэффициентов между соседними пикселями и сравнении их с ожидаемыми значениями для контейнера: если корреляции превышают статистически значимый порог, устанавливаемый через доверительные интервалы или машинное обучение, делается вывод о наличии стеганографического преобразования [1–3].

В целях исследования работы атаки были проведены атаки на незаполненные контейнеры. Результат представлен в таблице 2.

Таблица 2 – Результат атаки на «пустые» контейнеры

Контейнер	Количество аномалий, «обнаруженных» в результате BCA-атаки
*C*1	39
*C*2	0
*C*3	18

Для внедрения сообщений были выбраны следующие методы: DCT (Discrete Cosine Transform – дискретное косинусное преобразование), DWT (Discrete Wavelet Transform – дискретное вейвлет-преобразование), LSB (Least Significant Bit – наименьший значащий бит), GML (Grey Level Modification – изменение уровня серого), PVD (Pixel Value Difference – разница между значениями) и MPV (Mid Position Value – значение средней позиции). А также предложенные ранее автором методы прямого и обратного стеганографических преобразований растрированных текстовых документов-контейнеров на основе модели RGB (метод 1), описан в [4], и на основе модификации полутоновых оттенков (метод 2), описан в [5].

Далее в каждый из контейнеров внедрялись 4 двоичных сообщения разной длины (вторая строка заголовка таблицы 3). Рассчитанная для каждого случая относительная стеганографическая емкость (ΔC – отношение длины сообщения M в битах к N) приведена в таблице 3.

Таблица 3 – Относительная стеганографическая емкость, полученная при различных атаках на стегоконтейнер

Контейнер	ΔC, бит/пиксель			
	1	2	3	4
*C*1	$0{,}77 \cdot 10^{-5}$	$6{,}91 \cdot 10^{-5}$	$6{,}86 \cdot 10^{-4}$	$2{,}06 \cdot 10^{-3}$

*C*2	$0{,}82\cdot10^{-5}$	$7{,}42\cdot10^{-5}$	$7{,}36\cdot10^{-4}$	$2{,}22\cdot10^{-3}$
*C*3	$0{,}83\cdot10^{-5}$	$7{,}45\cdot10^{-5}$	$7{,}35\cdot10^{-4}$	$2{,}22\cdot10^{-3}$

Результаты атаки на каждый из созданных стегоконтейнеров представлены в виде гистограмм на рис. 1 – рис. 3. Здесь первая горизонтальная строка под гистограммами обозначает данные для различных объемов внедренного сообщения, вторая горизонтальная строка – стегометод.

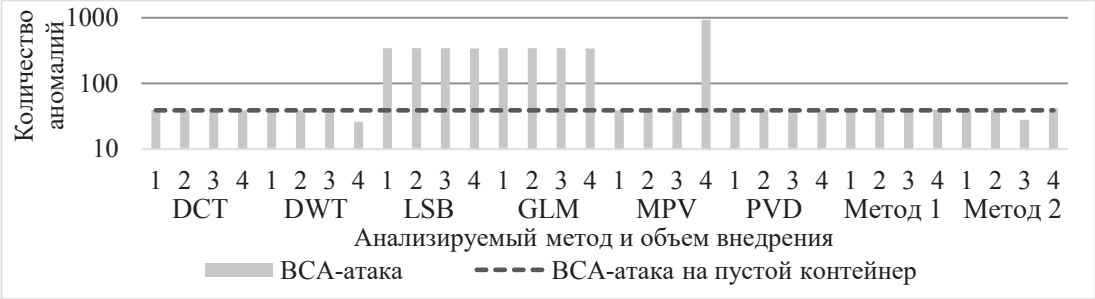

Рис. 1 – Результат ВСА-атаки на стегоконтейнер, полученный в результате преобразования *C*1

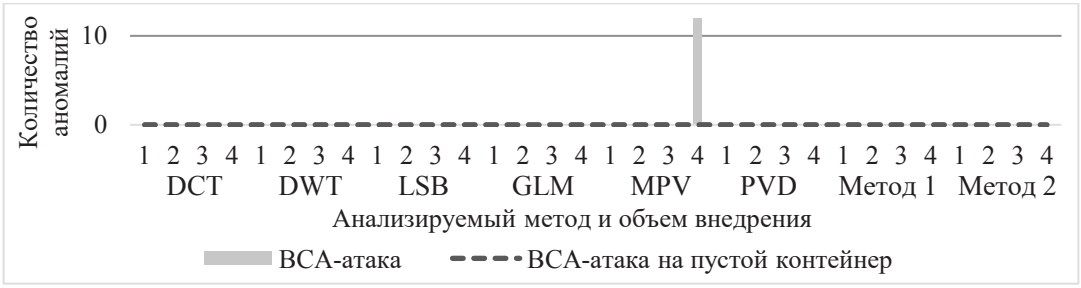

Рис. 2 – Результат ВСА-атаки на стегоконтейнер, полученный в результате преобразования C2

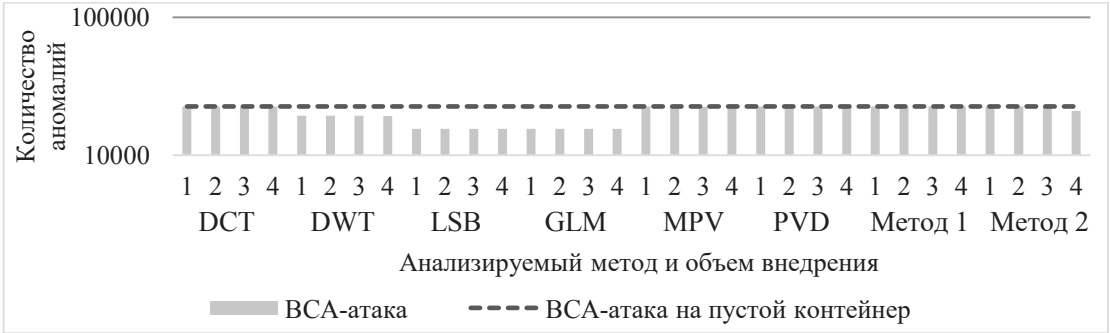

Рис. 3 – Результат ВСА-атаки на стегоконтейнер, полученный в результате преобразования C3

Результаты атаки ВСА выражены в абсолютном количестве выявленных статистических аномалий. Количество аномалий в базовой корреляционной атаке Зигенталера означает число статистически значимых отклонений в значениях пар соседних пикселей. Отклонения

появляются в результате неестественных пиков в определённых точках распределения и общих нарушений плавности статистических характеристик изображения. Большая концентрация аномалий указывает на вероятное наличие стеганографических преобразований, а их отсутствие или незначительное количество может означать отсутствие данных или применение адаптивных методов скрытия.

По проведенному исследованию можно отметить, что большая часть методов устойчива к BCA-атаке, в частности DCT, DWT, PVD, метод 1 и метод 2. При большом объеме сообщения результаты можно объяснить взаимодействием с особенностями контейнера, в том числе маскирующий эффект (маскируются естественные аномалии контейнера, приводя к заниженным оценкам).

Список использованных источников

1. Потий А., Избенко Ю. Исследование методов криптоанализа поточных шифров. – 2003.

2. Yang W. et al. Multi-channel fusion attacks //IEEE Transactions on Information Forensics and Security. – 2017. – Т. 12. – №. 8. – С. 1757-1771.

3. Thomas Siegenthaler. Decrypthing a class of stream chiphers using chipertext on-ly. IEEE Transactions on Computers, 34(1):81–85, January 1985.

4. Савельева М. Г., Урбанович П. П. Метод стеганографического преобразования web-документов на основе растровой графики и модели RGB // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – 2022. – № 2 (260). – С. 99–107.

5. Савельева М. Г., Урбанович П. П. Стеганографическое преобразование на основе модификации полутоновых оттенков растрированных документов // Информационно-управляющие системы. – 2024. – № 6. – С. 2–14.