

Черноморец Андрей Алексеевич, доктор технических наук, профессор,
профессор кафедры прикладной информатики и информационных
технологий, Белгородский государственный национальный
исследовательский университет, Россия, г. Белгород

Кривчикова Анастасия Сергеевна, магистрант, Белгородский
государственный национальный исследовательский университет, Россия, г.
Белгород

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ СТЕГАНОГРАФИЧЕСКОГО СКРЫТИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИИ

Аннотация. Настоящая статья посвящена сравнительной оценке современных стеганографических методов внедрения данных в изображения. Анализ охватывает как пространственные подходы (метод LSB, псевдослучайные перестановки), так и частотные (ДКП, ДВП) подходы, а также специализированные алгоритмы (Куттера-Джордана-Боссена, Коха-Жао). В качестве основного инструмента для объективной оценки был использован метод анализа иерархий, с помощью которого удалось выявить преимущества и недостатки каждого из рассмотренных методов. Результаты проведенного анализа помогают систематизировать критерии выбора оптимального стеганографического метода для конкретных практических задач в области защиты информации.

Annotation. This article is devoted to a comparative evaluation of modern steganographic methods for embedding data in images. The analysis covers both spatial approaches (LSB, pseudorandom permutations) and frequency-based approaches (DCT, DWT), as well as specialized algorithms (Kutter-Jordan-Bossen, Koch-Zhao). The analytic hierarchy process was used as the primary tool for an objective evaluation, revealing the advantages and disadvantages of each of the methods considered. The results of the analysis help systematize the criteria for

selecting the optimal steganographic method for specific practical tasks in the field of information security.

Ключевые слова: стеганография, метод LSB, метод псевдослучайной перестановки, метод замены палитры, дискретное косинусное преобразование (DCT), дискретное вейвлет-преобразование (DWT), метод анализа иерархий.

Keywords: steganography, LSB method, pseudorandom permutation method, palette substitution method, discrete cosine transform (DCT), discrete wavelet transform (DWT), analytic hierarchy process.

На сегодняшний день разработано значительное количество разнообразных методов сокрытия информации в графических контейнерах. Каждый из них характеризуется своими преимуществами и недостатками. Поэтому целью данной статьи является анализ и сопоставление основных методов стеганографического сокрытия информации.

Метод наименее значащего бита известный (LSB) – это один из наиболее распространённых алгоритмов замены среди методов замены в пространственной области. Его принцип основан на том, что младший бит пикселя несет минимальную информационную нагрузку для визуального восприятия. Человеческий глаз, как правило, не фиксирует искажений, вызываемых модификацией этих битов. Фактически, LSB рассматривает в качестве цифрового шума, что открывает возможность для внедрения данных путем прямой замены этих битов на биты скрываемого сообщения. В контексте черно-белых изображений скрываемый объем может достигать 1/8 от исходного размера файла-контейнера. [2]

Метод псевдослучайных перестановок – это подход при котором биты секретного сообщения не записываются последовательно, а хаотично размещаются по всему изображению. Алгоритм работы метода следующий: генератор псевдослучайных чисел создает последовательность уникальных индексов пикселей (j_1, j_2, \dots, j_N). Каждый k -й бит сообщения j_k . При этом функция перестановки должна быть псевдослучайной, то есть, она должна

обеспечивать выбор бит контейнера приблизительно случайным образом. Это обеспечивает равномерное распределение битов, скрываемых данных по всему битовому пространству изображения-контейнера. [4]

Метод замены палитры. Данный метод основан на использовании специфических особенностей формата контейнера и предназначен для скрытия текстовой информации в графических файлах, которые используют цветовые палитры. К таким файлам относятся, например, BMP, GIF и PCX. Суть метода замены палитры заключается в том, что искажаются не сами цвета, а их номера. Однако, благодаря, предварительно отсортированной палитре, цвет точки заменяется на схожий, который практически невозможно отличить от исходного цвета из-за их малого различия. [4]

Метод блочного сокрытия. Данный метод предполагает разделение исходного изображения на отдельные, непересекающиеся области различной формы. Для каждой из этих областей рассчитывается контрольная сумма, определяющая ее четность. Внутри каждого блока внедряется один бит скрываемой информации. Если рассчитанный бит четности не соответствует внедряемому секретному биту, то происходит изменение одного из младших битов пикселей в блоке. Выбор конкретного блока для внедрения информации может осуществляться случайным образом, опираясь на стегоключ. [8]

Метод Куттера–Джордана–Боссена – это стеганографический способ, опирающийся на то, что человеческий глаз не очень чувствителен к трансформациям синей составляющей цвета. Принцип работы заключается в целенаправленной корректировке интенсивности синего цвета пикселей, при этом значения красного и зеленого каналов остаются без изменений. Процедура внесения информации контролируется параметром, который определяет соотношения между незаметностью модификаций и их устойчивостью к потенциальным дефектам. Для восстановления скрытых данных применяется алгоритм, исследующий соседние пиксели в квадратной области 7 на 7 точек. Это позволяет вернуть изначальные значения и выделить внедренную информацию. [3]

Метод Дармстедтера-Делейгла-Квисквотера-Макка. Суть метода: конфиденциальные сведения кодируются как бинарный вектор. В каждый фрагмент изображения внедряется ровно один бит информации (стандартно используется блок 8 на 8 пикселей). Сильная сторона данного стеганографического подхода – это ее невосприимчивость к дефектам, обусловленная резервированием данных при внедрении. [6]

Стеганографический метод на основе дискретного косинусного преобразования (DCT) предполагает сокрытие информации в коэффициентах средней частоты блоков размером 8 на 8 пикселей, полученные после преобразования. Выбор этих коэффициентов обусловлен их оптимальными характеристиками: изменения в них не так явно различимы, как во фрагментах с низкой частотой, но при этом менее подвержены влиянию сжатия, чем высокочастотные составляющие. Процесс внедрения данных осуществляется путем изменения наименее значимых битов или посредством сопоставления пар коэффициентов. [9]

Дискретное вейвлет-преобразование. В случае дискретного вейвлет-преобразования, после субдискретизации изображение разделяется на четыре поддиапазона Низкочастотный поддиапазон по горизонтали и вертикали (LL), низкочастотный поддиапазон по горизонтали и высокочастотный по вертикали (LH), высокочастотный поддиапазон по горизонтали и низкочастотный по вертикали (HL) и высокочастотный поддиапазон по горизонтали и вертикали (HH). В каждом из диапазонов содержатся коэффициенты ДВП, для встраивания чаще всего, как и в дискретно косинусном преобразовании используют высокочастотные диапазоны, так как их изменение менее заметно для восприятия человеком. [7]

Метод Фридрих. Метод Фридриха (Fridrich) – это один из классических алгоритмов стеганографии, основанный на использовании дискретного косинусного преобразования (ДКП) и применяемый для скрывания данных в JPEG-изображениях. Его ключевая особенность заключается в том, что

внедрение информации происходит не в пиксели, а в квантованные коэффициенты ДКП, что делает метод устойчивым к сжатию с потерями. [4]

Метод Коха-Жао реализует стеганографию в частотной области через модификацию коэффициентов ДКП (DCT). Изображение разбивается на блоки 8×8 пикселей, где для кодирования бита используется разность между двумя заданными коэффициентами. Если разность не превышает порог, коэффициенты корректируются добавлением/вычитанием константы. После обратного преобразования DCT изменения визуально незаметны, сохраняя качество изображения. Метод обеспечивает хорошую скрытность данных при сохранении приемлемого визуального качества контейнера. [1]

Таким образом, после выполненного обзора методов стеганографического скрытия информации следует перейти к их сравнительному анализу.

Для сравнительного анализа методик методов стеганографического скрытия информации в изображении был использован метод анализа иерархий [5].

Первым этапом в решении задачи принятия решения были выделены критерии, по которым будет происходить сравнение методов стеганографического скрытия информации, а также построена матрица парных сравнений для них (таблица 1).

Таблица 1 – Матрица парных сравнений для уровня критериев

	Скрытность	Устойчивость к атакам	Вместимость	Сложность реализации	Скорость работы	Вектор локальных приоритетов	Нормализованный вектор локальных приоритетов
Скрытность	1	2	3	3	7	2,631	0,426
Устойчивость к атакам	1/2	1	2	2	3	1,431	0,232
Вместимость	1/3	1/2	1	2	3	1,000	0,162
Сложность реализации	1/3	1/2	1/2	1	3	0,758	0,123
Скорость работы	1/7	1/3	1/3	1/3	1	0,351	0,057
Сумма по столбцам	2,310	4,333	6,833	8,333	17,000	6,170	1,000
	L_{max}	4,102	ИС	0,022	ОС	0,019	

Как видно из таблицы 1, рассмотренные выше методики профориентации будут оцениваться по следующим критериям:

- скрытность: способность метода оставаться незаметным для стегоанализа (обнаружения скрытых данных);
- устойчивость к атакам: сопротивление метода к искажениям (сжатию, шумам, фильтрации или другим преобразованиям файла);
- вместимость: объем данных, который можно скрыть в файле без заметных искажений;
- сложность реализации: трудность программирования метода;
- скорость работы: быстрдействие алгоритма при встраивании и извлечении данных.

Кроме того, критерий скрытности является наиболее значимым.

Отношение согласованности (ОС) равно 1,9%. Считается нормальным, если $ОС < 10\%$ [5]. Таким образом, матрицу можно считать согласованной.

Затем были составлены матрицы парных сравнений альтернатив по всем критериям.

Сравнение решений по критерию «Скрытность» представлено в таблице 2.

Таблица 2 – Сравнение решений по критерию «Скрытность»

	LSB	Псевдослучайные	Замена палитры	Блочное сокрытие	Куттера-Джордана	Дармстедтер и др	DCT	DWT	Фридрих	Кох-Жао	Вектор локальных приоритетов	Нормализованный вектор локальных приоритетов
LSB	1	1/3	1/5	1/7	1/7	1/7	1/5	1/7	1/3	1/5	0,227	0,016
Псевдослучайные	3	1	1/3	1/5	1/5	1/5	1/3	1/5	1	1/3	0,422	0,031
Замена палитры	5	3	1	1/3	1/3	1/3	1	1/3	3	1	0,943	0,068
Блочное сокрытие	7	5	3	1	1/3	1/3	3	1/3	5	3	1,676	0,122
Куттера-Джордана	7	5	3	3	1	1/3	5	1/3	5	3	2,197	0,159
Дармстедтер и др	7	5	3	3	3	1	5	1/3	5	3	2,737	0,199
DCT	5	3	1	1/3	1/5	1/5	1	1/5	3	1	0,809	0,059
DWT	7	5	3	3	3	3	5	1	5	3	3,410	0,247
Фридрих	3	1	1/3	1/5	1/5	1/5	1/3	1/5	1	1/3	0,422	0,031
Кох-Жао	5	3	1	1/3	1/3	1/3	1	1/3	3	1	0,943	0,068
Сумма по столбцам	50	31 1/3	15 7/8	11 1/2	8 3/4	6	21 6/7	3 2/5	31 1/3	15 7/8	13 4/5	1
			Л _{max}	11	ИС	0,116	ОС	0,078				

Наилучшим вариантом по критерию «скрытность» является метод дискретного вейвлет-преобразования (DWT).

Сравнение решений по критерию «Устойчивость к атакам» представлено в таблице 3.

Таблица 3 – Сравнение решений по критерию «Устойчивость к атакам»

	LSB	Псевдослучайные	Замена палитры	Блочное сокрытие	Куттера-Джордана	Дармстедтер и др	DCT	DWT	Фридрих	Кох-Жао	Вектор локальных приоритетов	Нормализованный вектор локальных приоритетов
LSB	1	1/3	1/5	1/7	1/7	1/7	1/5	1/7	1/3	1/5	0,227	0,016
Псевдослучайные	3	1	1/3	1/5	1/5	1/5	1/3	1/5	1	1/3	0,422	0,031
Замена палитры	5	3	1	1/3	1/3	1/3	1	1/3	3	1	0,943	0,068
Блочное сокрытие	7	5	3	1	1/3	1/3	3	1/3	5	3	1,676	0,122
Куттера-Джордана	7	5	3	3	1	1/3	5	1/3	5	3	2,197	0,159
Дармстедтер и др	7	5	3	3	3	1	5	1/3	5	3	2,737	0,199
DCT	5	3	1	1/3	1/5	1/5	1	1/5	3	1	0,809	0,059
DWT	7	5	3	3	3	3	5	1	5	3	3,410	0,247
Фридрих	3	1	1/3	1/5	1/5	1/5	1/3	1/3	1	1/3	0,444	0,032
Кох-Жао	5	3	1	1/3	1/3	1/3	1	1/3	3	1	0,943	0,068
Сумма по столбцам	50,000	31,333	15,867	11,543	8,743	6,076	21,867	3,543	31,333	15,867	13,809	1
			Л _{max}	11,125	ИС	0,125	ОС	0,084				

Наилучшим вариантом по данному критерию является метод дискретного вейвлет-преобразования (DWT).

Сравнение решений по критерию «Вместимость» представлено в таблице 4.

Таблица 4 – Сравнение решений по критерию «Вместимость»

	LSB	Псевдослучайные	Замена палитры	Блочное сокрытие	Куттера-Джордана	Дармстедтер и др	DCT	DWT	Фридрих	Кох-Жао	Вектор локальных приоритетов	Нормализованный вектор локальных приоритетов
LSB	1	3	5	3	5	7	3	5	1/3	7	2,979	0,216
Псевдослучайные	1/3	1	3	1	3	5	1	3	1/5	5	1,463	0,106
Замена палитры	1/5	1/3	1	1/3	1	3	1/3	1	1/7	3	0,628	0,046
Блочное сокрытие	1/3	1	3	1	3	5	1	3	1/5	5	1,463	0,106
Куттера-Джордана	1/5	1/3	1	1/3	1	3	1/3	1	1/7	3	0,628	0,046
Дармстедтер и др	1/7	1/5	1/3	1/5	1/3	1	1/5	1/3	1/9	1	0,293	0,021
DCT	1/3	1	3	1	3	5	1	3	1/5	5	1,463	0,106
DWT	1/5	1/3	1	1/3	1	3	1/3	1	1/7	3	0,628	0,046
Фридрих	3	5	7	5	7	9	5	7	1	9	5,032	0,365
Кох-Жао	1/7	1/5	1/3	1/5	1/3	1	1/5	1/3	1/9	1	0,293	0,021
Сумма по столбцам	5 8/9	12,400	24,667	12,400	24,667	42,000	12,400	24,667	2,584	42,000	14,872	1,000
			Лмах	11,320	ИС	0,147	ОС	0,098				

Наилучшие варианты по критерию «Вместимость»: метод Фридрих, метод наименее значащего бита известный (LSB), метод псевдослучайной перестановки и метод блочного сокрытия.

Сравнение решений по критерию «Сложность реализации» представлено в таблице 5.

Таблица 5 – Сравнение решений по критерию «Сложность реализации»

	LSB	Псевдослучайные	Замена палитры	Блочное сокрытие	Куттера-Джордана	Дармстедтер и др	DCT	DWT	Фридрих	Кох-Жао	Вектор локальных приоритетов	Нормализованный вектор локальных приоритетов
LSB	1	1/3	1/5	1/7	1/7	1/7	1/5	1/7	1/3	1/5	0,227	0,016
Псевдослучайные	3	1	1/3	1/5	1/5	1/5	1/3	1/5	1	1/3	0,422	0,031
Замена палитры	5	3	1	1/3	1/3	1/3	1	1/3	3	1	0,943	0,068
Блочное сокрытие	7	5	3	1	1/3	1/3	3	1/3	5	3	1,676	0,122
Куттера-Джордана	7	5	3	3	1	1/3	5	1/3	5	3	2,197	0,159
Дармстедтер и др	7	5	3	3	3	1	5	1/3	5	3	2,737	0,199
DCT	5	3	1	1/3	1/5	1/5	1	1/5	3	1	0,809	0,059
DWT	7	5	3	3	3	3	5	1	5	3	3,410	0,247
Фридрих	3	1	1/3	1/5	1/5	1/5	1/3	1/5	1	1/3	0,422	0,031
Кох-Жао	5	3	1	1/3	1/3	1/3	1	1/3	3	1	0,943	0,068
Сумма по столбцам	50,000	31,333	15,867	11,543	8,743	6,076	21,867	3,410	31,333	15,867	13,787	1
			Лмах	11,042	ИС	0,116	ОС	0,078				

Наилучшими вариантами по данному критерию являются метод дискретного вейвлет-преобразования (DWT) и метод Дармстедтера-Делейгла-Квисквотера-Макка.

Сравнение решений по критерию «Скорость работы» представлено в таблице 6.

Таблица 6 – Сравнение решений по критерию «Скорость работы»

	LSB	Псевдослучайные	Замена палитры	Блочное сокрытие	Куттера-Джордана	Дармстедтер и др	DCT	DWT	Фридрих	Кох-Жао	Вектор локальных приоритетов	Нормализованный вектор локальных приоритетов
LSB	1	3	5	3	5	7	3	5	3	7	3,712	0,269
Псевдослучайные	1/3	1	3	1	3	5	1	3	1	5	1,719	0,125
Замена палитры	1/5	1/3	1	1/3	1	3	1/3	1	1/3	3	0,683	0,050
Блочное сокрытие	1/3	1	3	1	3	5	1	3	1	5	1,719	0,125
Куттера-Джордана	1/5	1/3	1	1/3	1	3	1/3	1	1/3	3	0,683	0,050
Дармстедтер и др	1/7	1/5	1/3	1/5	1/3	1	1/5	1/3	1/5	1	0,311	0,023
DCT	1/3	1	3	1	3	5	1	3	1	5	1,719	0,125
DWT	1/5	1/3	1	1/3	1	3	1/3	1	1/3	3	0,683	0,050
Фридрих	1/3	1	3	1	3	5	1	3	1	5	1,719	0,125
Кох-Жао	1/7	1/5	1/3	1/5	1/3	1	1/5	1/3	1/5	1	0,311	0,023
Сумма по столбцам	3,219	8,400	20,667	8,400	20,667	38,000	8,400	20,667	8,400	38,000	13,259	1,000
			Lmax	9,843	ИС	0,017	ОС	0,012				

Наилучшие варианты по критерию скорости работы: метод наименее значащего бита известный (LSB), метод псевдослучайной перестановки, метод блочного сокрытия, сокрытия информации с помощью дискретного косинусного преобразования и метод Фридрих.

Проведя все сравнения для иерархии, можно перейти к результатам ранжирования методов стеганографического сокрытия информации в изображении. Матрица сравнения результатов представлена в таблице 7.

Таблица 7 – Матрица сравнения результатов

	Скрытность	Устойчивость к атакам	Вместимость	Сложность реализации	Скорость работы	Вес критерия
LSB	0,016	0,016	0,216	0,016	0,269	0,063
Псевдослучайные	0,031	0,031	0,106	0,031	0,125	0,048
Замена палитры	0,068	0,068	0,046	0,068	0,050	0,064
Блочное сокрытие	0,122	0,122	0,106	0,122	0,125	0,119
Куттера-Джордана	0,159	0,159	0,046	0,159	0,050	0,135
Дармстедтер и др	0,199	0,199	0,021	0,199	0,023	0,160
DCT	0,059	0,059	0,106	0,059	0,125	0,070
DWT	0,247	0,247	0,046	0,247	0,050	0,203
Фридрих	0,031	0,032	0,365	0,031	0,125	0,091
Кох-Жао	0,068	0,068	0,021	0,068	0,023	0,058
Сумма по столбцам	1,000	1,000	1,000	1,000	1,000	1,000

Рейтинг методик стеганографического сокрытия информации в изображении представлена в таблице 8.

Таблица 8 – Рейтинг методик стеганографического скрытия информации в изображении

Место	Название	Рейтинг
1	Метод дискретного вейвлет-преобразования	20,3%
2	Метод Дармстедтера-Делейгла-Квисквотера-Макка	16,0%
3	Метод Куттера–Джордана–Боссена	13,5%
4	Метод блочного сокрытия	11,9%
5	Метод Фридрих	9,1%
6	Метод скрытия информации с помощью дискретного косинусного преобразования	7,0%
7	Метод замены цветовой палитры	6,4%
8	Метод наименее значащего бита известный (LSB)	6,3%
9	Метод относительной замены величин коэффициентов ДКП (метод Коха и Жао)	5,8%
10	Метод псевдослучайных перестановок	4,8%

На основе примененного метода анализа иерархий для выбора альтернативы, было выявлено, что наилучшими вариантами по всем критериям являются метод дискретного вейвлет-преобразования, метод Дармстедтера-Делейгла-Квисквотера-Макка и метод Куттера–Джордана–Боссена. Но тем не менее, представленные методики обладают довольно сложной реализацией и низкой скоростью работы.

Список литературы

1. Грачев, Я.Л. Стегоанализ методов скрытия информации в графических контейнерах [Электронный ресурс] / Я. Л. Грачев, В. Г. Сидоренко // Надежность. – 2021. – Т. 21, №3. – С. 39-46. – URL: <https://www.dependability.ru/jour/article/viewFile/431/710> (дата обращения 10.12.2025).

2. Грибунин, В. Г. Цифровая стеганография. [Текст] / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – Москва : Солон-Пресс. – 262 с.
3. Жигалов, И.Е. Применение метода Куттера – Джордана – Боссена для сокрытия данных в пространственной области изображения [Электронный ресурс] / И. Е. Жигалов, М. И. Озерова, А. В. Евстигнеев // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2023. – URL: <https://vestnik.susu.ru/ctcr/article/view/13489> (дата обращения 10.12.2025).
4. Коханович, Г. Ф. Компьютерная стенография. Теория и практика. [Текст] / Г. Ф. Коханович, А. Ю. Пузыренко. – Киев : «МК-Пресс», 2006. – 288 с.
5. Ломакин, В.В. Алгоритм повышения степени согласованности матрицы парных сравнений при проведении экспертных опросов [Текст] / В.В. Ломакин, М.В. Лифиренко // Фундаментальные исследования. – 2013. – № 1. – С.1798-1803.
6. Методики сокрытия информации в файлах формата jpeg [Электронный ресурс]. – URL: <https://goo.su/3YEA3U> (дата обращения 10.12.2025).
7. Попов, А.Е. Методы стеганографического скрывания информации в изображениях [Электронный ресурс] / А. Е. Попов. – 2024. – URL: <https://clk.li/sKOR> (дата обращения 10.12.2025).
8. Применение стеганографических методов по защите данных [Электронный ресурс]. – URL: <https://www.bibliofond.ru/view.aspx?id=607720> (дата обращения 10.12.2025).
9. Стеганография [Электронный ресурс]. – URL: <https://chalab.ru/post.php?id=13> (дата обращения 10.12.2025).

References

1. Grachev, Ya.L. Stegoanalysis of information hiding methods in graphic containers [Electronic resource] / Ya. L. Grachev, V. G. Sidorenko // Reliability. – 2021. – Vol. 21, No. 3. – pp. 39-46. – URL: <https://www.dependability.ru/jour/article/viewFile/431/710> (accessed 12/10/2025).

2. Gribunin, V. G. Digital steganography. [Text] / V. G. Gribunin, I. N. Okov, I. V. Turintsev. Moscow : Solon Press, 262 p.
3. Zhigalov, I.E. Application of the Cutter–Jordan–Bossen method for hiding data in the spatial area of an image [Electronic resource] / I. E. Zhigalov, M. I. Ozerova, A.V. Evstigneev // Bulletin of the South Ural State University. Series: Computer technology, control, radio electronics. - 2023. – URL: <https://vestnik.susu.ru/ctcr/article/view/13489> (accessed 12/10/2025).
4. Kokhanovich, G. F. Computer shorthand. Theory and practice. [Text] / G. F. Kokhanovich, A. Y. Puzyrenko. – Kiev : MK-Press, 2006. – 288 p.
5. Lomakin, V.V. Algorithm for increasing the degree of consistency of the matrix of paired comparisons during expert surveys [Text] / V.V. Lomakin, M.V. Lifirenko // Fundamental research. – 2013. – No. 1. – pp.1798-1803.
6. Methods of hiding information in jpeg files [Electronic resource]. – URL: <https://goo.su/3YEA3U> (accessed 12/10/2025).
7. Popov, A.E. Methods of steganographic information hiding in images [Electronic resource] / A. E. Popov. – 2024. – URL: <https://clk.li/sKOR> (accessed 10.12.2025).
8. Application of steganographic methods for data protection [Electronic resource]. – URL: <https://www.bibliofond.ru/view.aspx?id=607720> (accessed 12/10/2025).
9. Steganography [Electronic resource]. – URL: <https://chalab.ru/post.php?id=13> (accessed 10.12.2025).