ТЕХНИЧЕСКИЕ НАУКИ

CC BY

УДК 004.056.55 : 004.43

Метод повышения надежности стеганографии с помощью порогового разделения секрета: реализация и тестирование

Н.С. Могилевская, О.В. Терещенко
Южный федеральный университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Основной недостаток традиционных стеганографических методов — утрата скрытого сообщения при повреждении заполненного контейнера. В данной работе исследуется задача обеспечения целостности стеганографических сообщений при модификации контейнера. Встраиваемое сообщение делится на доли в соответствии с (k,n)-пороговой схемой разделения секрета Шамира, после чего эти доли внедряются в различные непересекающиеся области изображения-контейнера с использованием метода Куттера-Джордана-Боссена. Для восстановления исходного сообщения достаточно любых k из n долей, что позволяет воссоздать информацию даже при частичной потере или искажении контейнера. Целью работы стала разработка и тестирование программного средства, реализующего предложенный подход. Описаны алгоритмы встраивания и извлечения данных, алгоритм восстановления секрета, а также особенности программной реализации. Экспериментально продемонстрирована работоспособность метода и его устойчивость к таким воздействиям, как наложение водяного знака; осветление изображения и наложение фильтра шума.

Ключевые слова: стеганография, пороговое разделение секрета, схема Шамира, метод Куттера-Джордана-Боссена, отказоустойчивость, стегоконтейнер, программная реализация

Для цитирования. Могилевская Н.С., Терещенко О.В. Метод повышения надежности стеганографии с помощью порогового разделения секрета: реализация и тестирование. *Молодой исследователь Дона.* 2026;11(3):90–96.

A Method for Improving Reliability of Steganography Using Threshold Secret Sharing: Implementation and Testing

Nadezhda S. Mogilevskaya, Oleg V. Tereshchenko
Southern Federal University, Rostov-on-Don, Russian Federation

Abstract
The main vulnerability of traditional steganographic techniques lies in the possibility of losing a hidden message in case of damaging the container file. The article investigates the problem of ensuring steganographic message integrity in case of modification of a container file. The embedded message is fragmented according to Shamir's (k, n) - threshold secret sharing scheme, afterwards the fragments are embedded in different non-overlapping regions of the container image using the Kutter-Jordan-Bossen technique. Any k of n fragment is sufficient to recover the original message, which makes it possible to recover the message even in case of partial loss or distortion of the container file. The study aims at developing and testing a software, which would implement the proposed approach. The algorithms for embedding and extracting data, a secret recovery algorithm, and software implementation features have been defined. The operability of the method and its resilience to such impacts as watermark application, image dodging, and noise filter imposing have been experimentally demonstrated.

Keywords: steganography, threshold secret sharing, Shamir's Secret Sharing Scheme, Kutter-Jordan-Bossen technique, fault tolerance, stego-container, software implementation

For Citation: Mogilevskaya NS, Tereshchenko OV. A Method for Improving Reliability of Steganography Using Threshold Secret Sharing: Implementation and Testing. *Young Researcher of Don.* 2026;11(3):90–96.

© Могилевская Н.С., Терещенко О.В., 2026

Введение. Для защиты данных широко применяется стеганография. Её используют не только для скрытой передачи информации, но и для решения других задач — например, предотвращения копирования, контроля распространения файлов в сетях и тому подобного [1, 2]. Методы стеганографии часто обладают существенным недостатком — они уязвимы к утрате внедрённых данных. Если стегоконтейнер, то есть изображение со встроенным сообщением, будет случайно повреждён или подвергнется целенаправленной атаке (например, сжатию с потерями или обрезке), то скрытая информация, скорее всего, окажется безвозвратно утраченной. Это существенно ограничивает практическую применимость стеганографии в системах, где требуется высокая надёжность и отказоустойчивость.

Исключить возможность модификации скрытого сообщения даже при изменении контейнера, можно, например, с помощью комбинации стеганографии и криптографической (k, n)-схемы порогового разделения данных ($k < n$). В пороговых схемах секрет разделяется на n частей (долей), и для его восстановления необходимо собрать k из них. Любое количество долей, меньшее k, не дает никакой информации об исходных данных.

Комбинирование методов порогового разделения данных и стеганографии может быть организовано следующим образом. Сообщение, разделенное каким-либо пороговым методом, стеганографически встраивается в n непересекающихся частей изображения-контейнера. Такой подход не только скрывает факт передачи, но и обеспечивает устойчивость к потере или повреждению до n-k долей сообщения. Далее для краткости описанную комбинацию методов порогового разделения данных и стеганографии будем называть гибридным методом защиты данных.

Повышение устойчивости стеганографического сообщения к искажениям контейнера с помощью порогового разделения секрета рассматривается, в частности, в исследованиях [3, 4]. Так, в работе [3] для встраивания в пространственную область мультимедийных файлов применяется метод SSRC, а в [4] — метод наименее значащего бита (НЗБ). В обеих работах используется схема Шамира.

Цель настоящей работы состоит в создании программного средства, реализующего гибридный метод защиты данных и предоставляющего возможность использовать в его составе стеганографический метод Куттера-Джордана-Боссена [1, 2] и пороговую схему Шамира разделения секрета. В статье также будут представлены некоторые результаты работы построенного программного средства, подтверждающие его работоспособность.

Алгоритм встраивания данных в изображение. Входными параметрами алгоритма встраивания данных являются: изображение-контейнер, встраиваемое сообщение (секрет), параметры используемой пороговой (k, n)-схемы разделения данных, а также параметры стеганографического метода встраивания.

Стеганографический метод Куттера-Джордана-Боссена (метод КДБ) встраивания и извлечения сообщений из неподвижных изображений параметризуется тремя значениями: q — энергия встраиваемого сигнала, r — число повторных встраиваний одного бита информации, а также *cross* — размер крестообразной окрестности пикселя с измененным битом (соседи с одинаковой координатой по горизонтали, либо по вертикали). С ростом q изменения пикселей в изображении заметнее, но устойчивость вложения растет. Рост параметра r увеличивает избыточность встраивания. Параметр *cross* применяется для извлечения бита данных из пикселя. В предлагаемой программной реализации параметры q, r и *cross* выбираются пользователем. Заметим, что выбор этих параметров значительно влияет на качество работы гибридного метода.

Схема Шамира порогового разделения секрета работает в полях Галуа GF(P) простой мощности P. В реализованном программном средстве поддерживается работа с простыми числами в диапазоне [257,3571]. Каждый символ секрета преобразовывается в число (байт), согласно кодировке Windows-1251, и в качестве секрета передается на вход схеме Шамира. Схема Шамира возвращает для переданного числа n долей. В (k, n)-пороговой схеме Шамира используется полином $f(x_i)$, $deg(f(x_i)) = k - 1$ над полем P, такой, что $f(0) = s$, где s — секрет. На выходе метода формируются n долей вида (x_i, y_i), где $x_i = i'$, $y_i = f(x_i) \in GF(\mathrm{P})$, $i \in [0, n)$, $i' \in [1, n]$. Из значений y_i, $i \in [0, n)$, формируется матрица Y, где количество строк равно общему числу долей (т.е. параметру n), а количество столбцов равно количеству символов в строке секрета (таким образом, каждый столбец матрицы — это набор долей (именно $y_i \in GF(\mathrm{P})$, $i \in [0, n)$) для одного символа секрета). В процессе построения долей, которые будут встраиваться в стегоконтейнер, итеративно для каждой строки матрицы выполняется: каждый элемент строки конкатенируются с числом i' — индексом строки матрицы, где находится элемент, затем конкатенируются все полученные подстроки. Таким образом формируются встраиваемые в стегоконтейнер доли:

$$D_i = i' \,||\, y_{i,0} \,||\, i' \,||\, y_{i,1} \,||\, i' \,||\, y_{i,2} \,||\, \ldots \,||\, i' \,||\, y_{i,S'-1},\ i \in [0, n), i' \in [1, n], \quad (1)$$

где S' — длина секрета в байтах, «||» является операцией конкатенации. В конец каждой такой доли дописывается рассчитанный CRC-код, построенный с использованием многочлена:

$$f(x) = x^8 + x^5 + x^4 + 1.$$

https://mid-journal.ru

Изображение-контейнер условно делится на n непересекающихся и равных по ширине полос, в каждую из которых, согласно алгоритму Куттера-Джордана-Боссена, побитно встраивается длина доли вида (1) с учетом контрольной суммы, затем сама доля с CRC-кодом. Если ширина изображения не делится нацело на n частей, то остается область, в которую ничего не внедряется. Биты информации встраиваются в синий цветовой канал случайных пикселей соответствующих полос (1 бит данных в 1 пиксель). Для выбора случайных позиций применяется генератор псевдослучайных чисел с заданным зерном *Z*.

Блок встраивания долей в стегоконтейнер возвращает в интерфейс программы параметр *P*. Схема работы алгоритма встраивания данных в изображение-контейнер представлена на рис. 1.

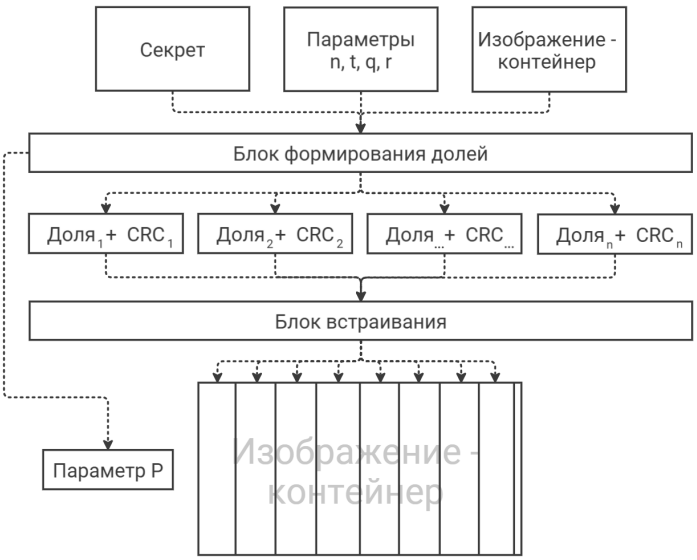

Рис. 1. Схема работы алгоритма встраивания долей секрета в файл-контейнер

Алгоритм извлечения данных. Этот алгоритм получает в качестве входных параметров заполненное изображение-контейнер, параметр n порогового метода разделения данных, параметры *r*, *cross* используемого стеганографического метода, а также число *P*, сгенерированное при выполнении алгоритма встраивания данных в контейнер.

Изображение условно делится на n равных по ширине полос, в каждой из которых итеративно происходит считывание бит данных. Нужные пиксели выбираются благодаря генератору псевдослучайных чисел с заданными зерно *Z*. Сначала считываются данные для восстановления длины доли, потом, согласно извлеченному значению, считываются биты самой доли. От полученной доли отделяются CRC-код, вычисленный при встраивании, рассчитывается новый CRC-код и сравнивается с извлеченным. На основе эквивалентности этих кодов выставляется флаг корректности извлеченной доли. Биты данных из пикселей извлекаются согласно алгоритму Куттера-Джордана-Боссена. Важно уточнить, что заполненный контейнер может быть сильно поврежден, ввиду чего извлекаемые длины долей могут быть «невозможными», например, их значения могут превышать количество пикселей в полосе. На этот случай в коде программы прописано условие, которое сравнивает значение извлеченного размера доли с количеством пикселей в полосе. Если значение длины доли превышает «пространство» полосы изображения, то алгоритм, даже не пытаясь извлечь саму долю, переходит к следующей полосе контейнера.

Алгоритм извлечения данных возвращает в интерфейс программы считанные доли с флагами, дописанными в конце соответствующих долей (флаги — «//true», «//false»), или сообщение «break part» для конкретной доли. Схема работы алгоритма извлечения данных из изображения-контейнера представлена на рис. 2.

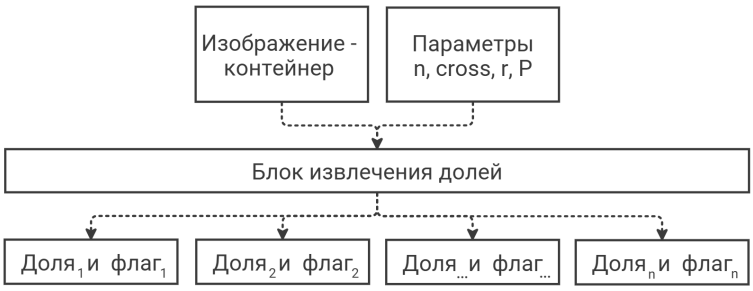

Рис. 2. Схема работы алгоритма извлечения долей

https://mid-journal.ru

Алгоритм восстановления секрета. Этот алгоритм получает в качестве входных параметров корректные извлеченные доли секрета (h штук, $k \le h \le n$) и параметр P, сгенерированный при встраивании данных в стегоконтейнер.

В процессе восстановления секрета условно восстанавливается матрица поддолей (Y), которая была получена в алгоритме формирования долей, встраиваемых в стегоконтейнер, и формируется матрица (X), состоящая из элементов $x_{(i,j)} = i'$, $i \in [0, h)$, $i' \in [1, h]$, $j \in [0, S')$, S' — размер секрета. На основе этих матриц, согласно схеме Шамира, восстанавливаются байты секрета. Полученная цепочка байт преобразуется в цепочку символов, согласно кодировке Windows-1251. Блок восстановления секрета возвращает в интерфейс программы восстановленный секрет. Схема работы алгоритма восстановления представлена на рис. 3.

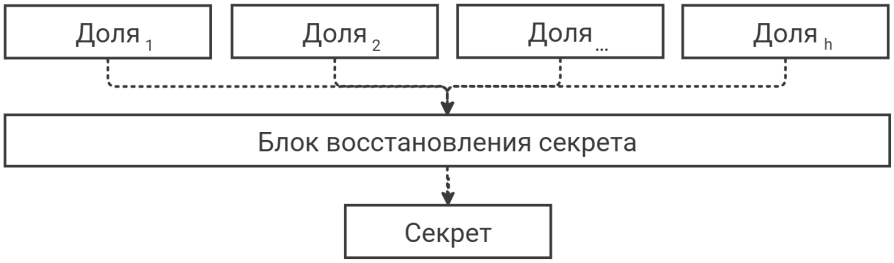

Рис. 3. Схема работы алгоритма восстановления секрета

О программной реализации. Описанные выше алгоритмы, реализующие гибридный метод защиты данных, программно реализованы в виде монолита на языке JavaFx Script с использованием среды разработки GigaIDE. Реализован ряд основных методов, среди которых: метод встраивания данных; метод извлечения данных; метод восстановления секрета; метод, реализующий (k, n)-пороговую схему Шамира; метод, возвращающий перемешанные координаты пикселей в i-й полосе изображения, $i \in [0, n)$; методы, отвечающие за работу с элементами поля Галуа $GF(P)$; метод, вычисляющий CRC-код для доли, а также некоторые другие вспомогательные методы. На построенное программное средство получено свидетельство о государственной регистрации [5].

Эксперименты. С использованием программного средства, реализующего гибридную схему защиты данных, был проведен ряд тестов, проверяющих степень устойчивости встроенной информации к повреждениям изображения-контейнера. В ходе экспериментов в качестве стегоконтейнера был использован набор из 9 разных изображений размером 1024×1024 пикселя формата PNG. В качестве встраиваемого сообщения выбирались случайные последовательности длиной 90 символов с помощью онлайн-сервиса [6]. Все тесты можно разделить на несколько групп, для каждой из которых параметры P (число элементов в поле), n (общее число долей), k (минимально необходимое число долей для восстановления секрета), r (количество повторных встраиваний одного бита данных) — вариативны. Параметры q (энергия встраиваемого сигнала) и *cross* (размер крестообразной окрестности пикселя) — фиксированы, равны соответственно 0,4 и 3.

Тесты проведены для 4 видов модификаций заполненного стегоконтейнера: обрезка изображения сверху и снизу, осветление изображения, наложение водяного знака, наложение шума. Для наложения водяного знака на изображение использовался онлайн-сервис [7], для осветления и наложения шума использовался онлайн-сервис [8]. В таблицах с результатами (таблица 2, таблица 3, таблица 4) зеленым и красным цветом помечена возможность или невозможность восстановления секрета по извлеченным долям соответственно. При занесении данных в таблицы результатов тестирования корректность извлечённых долей определялась по флагу.

В стегоконтейнеры внедрялись сообщения с разными параметрами встраивания данных, всего получилось 9 типов изображений с разным процентом модифицированных пикселей (таблица 1). Только для стегоконтейнера с параметрами $n = 32$, $k = 8$, $r = 16$, P — простое число в диапазоне [257,2039], для остальных случаев простое число P лежит в диапазоне [257,3571].

Таблица 1

Процент заполненности стегоконтейнера в зависимости от параметров встраивания

Сила встраивания	Количество встраиваний 1 бита данных	Процент измененных пикселей для $n = 8$, $k = 2$	Процент измененных пикселей для $n = 16$, $k = 4$	Процент измененных пикселей для $n = 32$, $k = 8$
0,4	4	6,7 %	12,2 %	26,7 %
0,4	8	13,3 %	24,5 %	49,0 %
0,4	16	24,5 %	49,0 %	97,9 %

https://mid-journal.ru

Первый тип тестов — обрезка изображения. Из-за того, что встраивание бит данных производится в случайные пиксели соответствующих полос, восстановление хоть какой-нибудь полезной информации даже при малом проценте обрезки (3,125 % — это 32768 пикселя) оказалось невозможным для всех заполненных стегоконтейнеров.

Второй тип тестов — осветление изображения. Результаты тестов показывают, что сообщение, встроенное гибридным методом защиты данных, устойчиво к применению эффекта осветления к стегоконтейнеру даже при высокой силе эффекта (таблица 2).

Таблица 2

Устойчивость данных, встроенных по гибридному методу, к осветлению изображения

Количество встраиваний одного бита данных	4				8				16			
Сила эффекта осветления	5	20	35	50	5	20	35	50	5	20	35	50
Количество восстановленных долей при $n = 8$, $k = 2$	8	7	0	0	8	6	6	6	8	8	8	8
Количество восстановленных долей при $n = 16$, $k = 4$	16	16	16	14	16	16	16	16	16	16	16	16
Количество восстановленных долей при $n = 32$, $k = 8$	30	30	20	15	32	32	32	32	32	32	32	32

Важно отметить, что стегоконтейнер с параметрами $n = 8$, $k = 2$, $r = 4$ имел много групп пикселей, являющихся оттенками белого и серого. При осветлении изображения с силой 35 и 50 все эти группы различных пикселей стали одинаково белыми — утратилась разница между ними. А так как при извлечении данных из стегоконтейнера метод КДБ восстанавливает бит данных путем предсказания исходного значения пикселя на основе значений соседних пикселей — утрата разницы между соседними пикселями приводит к потере данных.

Третий тип тестов — наложение водяного знака. Так же, как и в случае с осветлением изображения, данные, встроенные в контейнер по гибридному методу, устойчивы к «повреждению» контейнера водяным знаком (таблица 3).

Таблица 3

Устойчивость данных, встроенных по гибридному методу, к наложению водяного знака

Количество встраиваний одного бита данных	4				8				16			
Процент поврежденных пикселей	7,7	13,7	20,5	26,5	7,7	13,7	20,5	26,5	7,7	13,7	20,5	26,5
Количество восстановленных долей при $n = 8$, $k = 2$	8	8	8	8	8	8	8	8	8	8	8	8
Количество восстановленных долей при $n = 16$, $k = 4$	16	16	16	16	16	16	16	16	16	16	16	16
Количество восстановленных долей при $n = 32$, $k = 8$	32	32	32	32	32	32	31	32	32	32	32	32

Четвертый тип тестов — наложение фильтра шума. По результатам этих испытаний можно заключить, что, в целом, данные, встроенные в контейнер по гибридному методу, устойчивы к повреждению фильтром шума с силой примерно до 30 единиц (таблица 4).

Таблица 4

Устойчивость данных, встроенных по гибридному методу, к наложению фильтра шума

Количество встраиваний одного бита данных	4			8			16		
Сила эффекта	15	30	45	15	30	45	15	30	45
Количество восстановленных долей при $n = 8$, $k = 2$	8	8	0	8	8	1	8	8	7
Количество восстановленных долей при $n = 16$, $k = 4$	16	16	3	15	10	0	15	13	11
Количество восстановленных долей при $n = 32$, $k = 8$	30	23	0	32	15	4	32	32	7

Также, исходя из результатов тестов четвертого типа, можно предположить, что количество встраиваемых долей точно не прямо пропорционально количеству извлекаемых долей. Это видно из процентного соотношения восстановленных долей к общему числу встраиваемых долей для каждого эксперимента (таблица 5).

Таблица 5

Устойчивость данных, встроенных по гибридному методу, к наложению фильтра шума. Процентное соотношение восстановленных долей к общему числу встроенных долей

Количество встраиваний одного бита данных	4			8			16		
Сила эффекта	15	30	45	15	30	45	15	30	45
Процент восстановленных долей при $n = 8$, $k = 2$	100	100	0	100	100	13	100	100	88
Процент восстановленных долей при $n = 16$, $k = 4$	100	100	19	94	63	0	94	81	69
Процент восстановленных долей при $n = 32$, $k = 8$	94	72	0	100	47	13	100	100	22

Заключение. В результате работы создано программное средство, реализующее гибридный метод защиты данных, который объединяет пороговое разделение секрета и стеганографию. Цель разработки и апробации программы достигнута.

Программа [5] поддерживает схему Шамира с настраиваемыми параметрами, а также стеганографический метод Куттера-Джордана-Боссена. Это делает её эффективным инструментом для исследований. Работоспособность компонентов подтверждена экспериментально.

Список литературы

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. *Цифровая стеганография.* Москва: СОЛОН-Пресс; 2025. 262 с.

2. Шелухин О. И., Канаев С. Д. *Стеганография. Алгоритмы и программная реализация.* Москва: Горячая линия. Телеком; 2024. 592 с.

3. Вишневская Т.И., Уточкина Н.В. Стеганографический метод, устойчивый к повреждению данных. *Математические структуры и моделирование.* 2020;(1):37–43.

4. Мироненко А.Н. Метод применения (T, N) пороговой схемы в стеганографии. *Математические структуры и моделирование.* 2018;(2(46)):157–166. https://doi.org/10.25513/2222-8772.2018.2.157-166

5. Могилевская Н.С., Терещенко О.В. *StegoShare: программа стеганографического сокрытия данных с использованием пороговых схем разделения секрета.* Свидетельство о государственной регистрации программы для ЭВМ № 2025691720.

6. *Онлайн-сервис для генерации случайной последовательности символов.* Code More! URL: https://codemore.ru/2017/07/11/random.html (дата обращения: 31.01.2026).
7. *Онлайн-сервис для наложения водяного знака на изображение.* BatchTools.pro. URL: https://batchtools.pro/ru/watermark (дата обращения: 31.01.2026).
8. *Онлайн-сервис для осветления изображения и наложения фильтра шума.* Anytools.pro. URL: https://anytools.pro/ru/img/editor/noise (дата обращения: 31.01.2026).

Об авторах:

Надежда Сергеевна Могилевская, кандидат технических наук, доцент, доцент кафедры «Алгебра и дискретная математика» Института механики, математики и компьютерных наук Южного федерального университета (344090, Российская Федерация, г. Ростов-на-Дону, ул. Мильчакова, 8а), nmogilevskaya@sfedu.ru

Олег Витальевич Терещенко, магистрант кафедры «Алгебра и дискретная математика» Института механики, математики и компьютерных наук Южного федерального университета (344090, Российская Федерация, г. Ростов-на-Дону, ул. Мильчакова, 8а), teresh@sfedu.ru

Конфликт интересов: **авторы заявляют об отсутствии конфликта интересов.**

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Nadezhda S. Mogilevskaya, Master's Degree Student of the Department of Algebra and Discrete Mathematics, Institute of Mechanics, Mathematics, and Computer Science of the Southern Federal University (8a Milchakova Str., Rostov-on-Don, 344090, Russian Federation), teresh@sfedu.ru

Oleg V. Tereshchenko, Master's Degree Student of the Department of Algebra and Discrete Mathematics, Institute of Mechanics, Mathematics, and Computer Science of the Southern Federal University (8a Milchakova Str., Rostov-on-Don, 344090, Russian Federation), teresh@sfedu.ru

Conflict of Interest Statement: **the authors declare no conflict of interest.**

All authors have read and approved the final manuscript.