ТЕХНИЧЕСКИЕ НАУКИ

УДК 003.26

Оценка стеганографических методов сокрытия информации

Э.Г. Товмасян, Н.А. Галичев, Д.А. Штепа, И.А. Алферова
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Рассматриваются стеганографические методы сокрытия информации и возможности использования их для обеспечения целостности стеганосообщений. Особое внимание уделяется методу наименьшего значащего бита и методу оценки числа переходов значений младших бит в соседних элементах изображения.

Ключевые слова: стеганография, информационная безопасность, шифрование, кодирование

Для цитирования. Алферова И.А., Галичев Н.А., Штепа Д.А., Товмасян Э.Г. Аналитический обзор стеганографических методов сокрытия информации. *Молодой исследователь Дона.* 2025;10(2):77–81.

Evaluation of Steganography Methods of Information Concealment

Elina G. Tovmasyan, Nikita A. Galichev, Darya A. Shtepa, Irina A. Alferova
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
This article discusses steganography methods of information concealment and the possibility of using them to ensure the integrity of stegan messages. Special attention is paid to the method of the least significant bit and the method of estimating the number of transitions of the values of the least significant bits in neighboring image elements.

Keywords: steganography, information security, encryption, coding

For Citation. Tovmasyan EG, Galichev NA, Shtepa DA, Alferova IA. Evaluation of Steganography Methods of Information Concealment. *Young Researcher of Don.* 2025;10(2):77–81.

Введение. Одной из чрезвычайно важных задач является защита информации, которая может включать интеллектуальную собственность, авторские права и конфиденциальные данные. Существует два принципиально различных способа передачи секретных данных по открытому каналу: шифрование и стеганография [1]. Криптографические методы, применяемые для шифрования сообщений, подразумевают изменение текста таким образом, чтобы доступ к сообщению имел ограниченный круг лиц, даже в случае перехвата данных в канале связи. Текст, полученный после такого изменения, называется шифртекстом. Решением задач шифрования сообщений занимается наука, именуемая криптографией [2]. Стеганография, в свою очередь, действует совершенно иным образом. С целью защиты информации от несанкционированного чтения, стеганографические методы обеспечивают защиту данных путем их интеграции в шумовые данные, скрывающие сам факт передачи. Это достигается внедрением секретных символов в контейнер. Открытый текст, видоизмененный подобным образом, может быть обнаружен злоумышленником в канале связи. Тем не менее, злоумышленник не догадывается о факте передачи сообщения, так как передаваемая информация выглядит легитимно для постороннего наблюдателя [3]. Несмотря на наличие серьезно проработанных математических основ криптографии, стеганография все еще не обладает такой же глубиной разработки. На сегодняшний день технологические аспекты этой науки хорошо отработаны, однако задача построения и анализа математических моделей остается актуальной. Цель данной работы заключается в оценке стеганографических методов сокрытия информации с использованием гистограмм. Основная часть. Стеганография представляет собой дисциплину, изучающую способы скрытой передачи информации, при которых факт существования передаваемых данных остается незамеченным. В отличие от криптографии, которая фокусируется на защите содержания сообщений, стеганография дополняет ее, позволяя скрывать сам процесс передачи данных. Применение стеганографических методов значительно уменьшает вероятность обнаружения скрываемой информации. Для повышения уровня защиты можно также использовать шифрование, что обеспечит дополнительную защиту.

Стеганографию можно рассматривать как способ создания тайных каналов связи, акцентируя внимание на ее роли в организации скрытых коммуникаций. Главной задачей данного подхода является осуществление сокрытия информации таким образом, чтобы потенциальный злоумышленник не только не мог расшифровать ее, но даже не подозревал о ее наличии. Важной характеристикой стеганографических методов является внедрение секретного сообщения в контейнер — открытый объект, который не вызывает подозрений. Затем данный контейнер передается получателю через обычный канал связи. Ключевое отличие стеганографии от криптографии заключается в том, что зашифрованные данные в криптосистемах могут быть распознаны, даже если они остаются нерасшифрованными, тогда как в стеганографии скрыто само существование сообщения.

Современные стеганографические системы (или стегосистемы) определяются как совокупность методов и инструментов, предназначенных для создания тайного канала передачи информации. При их разработке необходимо учитывать, что злоумышленник может обладать знаниями о принципах работы системы. Однако единственным неизвестным для него остается ключ, который используется для выявления и извлечения скрытого сообщения. Таким образом, надежность всей системы защиты данных при передаче информации во многом зависит от секретного ключа, который должен быть заранее согласован между отправителем и получателем.

Стеганография делится на три основных направления [4]. Классическая стеганография включает методы, не использующие вычислительные устройства и реализуемые вручную. Компьютерная стеганография, являясь продолжением классических методов, применяет свойства цифровых систем, такие как скрытие информации в неиспользуемых областях файлов, текстовая стеганография и модификация имен файлов. Цифровая стеганография представляет собой разновидность компьютерной стеганографии, основанную на внедрении информации в мультимедийные объекты (изображения, аудио, видео), которые изначально имели аналоговую природу. С развитием компьютерных технологий и появлением различных способов передачи данных возникли новые стеганографические методики, учитывающие особенности цифровых сетей, форматов файлов и других средств обработки информации. Например, данные могут быть скрыты внутри текстовых или графических файлов с помощью специализированного программного обеспечения. Тем не менее, современные технологии пока не обеспечивают абсолютной защиты передаваемой информации, что стимулирует дальнейшие исследования в стеганографии и методов ее анализа.

В общем случае стеганографическую систему можно рассматривать как систему, обеспечивающую скрытый канал связи. Она в большинстве случаев включает следующие ключевые элементы: анализатор формата — программные средства для оценки контейнера на его применимость в стеганографических целях (оценка формата, потенциального размера внедряемого содержания); прекодер — программное обеспечение, предназначенное для кодирования сообщения в форму, удобную для внедрения в контейнер, что чаще всего включает архивирование, помехоустойчивое кодирование или шифрование вложений; стеганокодер — средство, осуществляющее внедрение стегановложения с учетом особенностей контейнера; стеганоконтейнер — контейнер, модифицируемый стеганоалгоритмом для последующей передачи; ключ — секретный параметр стеганоалгоритма и/или криптографического алгоритма; вложение — информация, подлежащая сокрытию (обычно это текст или файл); стеганодетектор — средства, проверяющие наличия стегановложения в контейнере; стеганодекодер — программное средство для восстановления стегановложения (без дешифровки и/или деархивации); постдекодер — программное средство, осуществляющее дешифрование и/или деархивацию, восстанавливающее первоначальный вид скрытого вложения [5].

Стеганографическая система считается надежной лишь в том случае, если злоумышленник не способен доказать наличие скрытого сообщения в контейнере. Процесс компрометации такой системы включает несколько последовательных этапов. Первый из них — обнаружение скрытой информации, который направлен на выявление факта наличия сообщения. Второй — извлечение замаскированных данных, чтобы получить доступ к скрытому содержимому. Третий этап связан с модификацией скрытых данных, где осуществляется изменение или подмена информации. Четвертый этап включает блокировку передачи данных, при которой предотвращается передача как открытой, так и скрытой информации. Первые два этапа относятся к пассивным атакам, направленным на анализ и извлечение данных без вмешательства в процесс передачи. Последние два этапа представляют собой активные атаки, предполагающие прямое воздействие на контейнер или канал передачи.

Атаки на стеганосистемы можно классифицировать аналогично методам криптоанализа. Существуют атаки на основе известного заполненного контейнера, когда злоумышленник располагает контейнерами с уже внедренными скрытыми сообщениями, целясь в выявление наличия стеганографического канала и извлечение данных. Атака на основе известного встроенного сообщения актуальна для систем защиты авторских прав, где скрытое сообщение может выступать в виде известного цифрового водяного знака (например, логотипа). Задача злоумышленника — получить ключ, что затруднительно без доступа к заполненному контейнеру. Атака на основе

выбранного скрытого сообщения возможна, если злоумышленник может передавать свои сообщения и анализировать получаемые контейнеры. Это позволяет выявлять закономерности, связанные с внедрением данных. Адаптивная атака на основе выбранного сообщения является усложненной версией предыдущей атаки, где злоумышленник адаптирует свои действия, основываясь на анализе ранее полученных контейнеров. Атака на основе выбранного заполненного контейнера часто применяется в системах цифровых водяных знаков, когда злоумышленник использует детектор для анализа заполненных контейнеров, изучая продетектированные сообщения с целью раскрытия ключа или алгоритма внедрения.

Таким образом, атаки на стеганосистемы могут варьироваться от пассивного анализа до активного вмешательства, и их успех во многом зависит от доступной злоумышленнику информации и способности адаптироваться к защитным механизмам системы. Помимо перечисленных методов, злоумышленники могут применять подходы, не имеющие аналогов в традиционном криптоанализе. Например, атака с использованием известного пустого контейнера предполагает, что злоумышленник сравнивает его с подозрительным контейнером, выявляя отклонения, которые могут указывать на наличие стеганографического канала. Для противодействия таким атакам разработаны теоретические основы, включая методы создания устойчивых стеганосистем, даже если контейнер известен лишь приблизительно, например, с добавлением случайного шума.

Атака с использованием выбранного пустого контейнера возможна, если злоумышленник может навязать использование определенного контейнера для передачи данных. В таком случае он может создать контейнер с однородными областями, что значительно усложняет сокрытие сообщения. Подобные манипуляции затрудняют внедрение данных, так как однородные структуры оставляют меньше возможностей для скрытия информации без заметных искажений. Применение атаки на основе известной математической модели контейнера заключается в использовании знаний о его математической модели или ее части для выявления отклонений в подозрительном сообщении. Например, определенные биты контейнера могут обладать статистической корреляцией, которая нарушается при внедрении скрытого сообщения. Задача стеганографа в такой ситуации — сохранить статистические свойства контейнера, чтобы избежать обнаружения. Успех атаки во многом зависит от точности математической модели, которой владеет злоумышленник.

Цель атаки на стеганосистему во многом схожа с целью атак на криптосистемы, однако в стеганографии значительно возрастает роль активных атак. Извлечение скрытого сообщения может быть крайне сложным даже при наличии возможности проведения атаки. Одной из ключевых проблем остается идентификация наличия скрытой информации в произвольном контейнере. Поэтому стеганоанализ зачастую сводится не к поиску самого сообщения, а к попытке обнаружения стеганографического ключа или выявлению специфических признаков стеганопреобразования. Этот процесс более узконаправлен, но более реалистичен в условиях ограниченных ресурсов и информации.

Метод наименьшего значащего бита (НЗБ) является одним из простейших и наиболее распространенных методов стеганографии, используемых для сокрытия информации. Метод LSB (Least Significant Bit) изменяет значения последних значащих бит контейнера. В качестве контейнера могут использоваться аудиофайлы, видеофайлы, изображения и любые другие формы представления информации, состоящие из множества однородных численных значений. Удобство использования таких форматов заключается в том, что можно пренебречь точностью значений, из которых состоит контейнер, и, тем самым, проще скрыть информацию внутри него, не оставляя следов. При этом требуется, чтобы различия между пустыми и заполненными контейнерами были незаметны для человеческого восприятия.

Рассмотрим метод НЗБ на конкретном примере с 8-битным черно-белым изображением. В данном случае черный цвет обозначается как 00h или 00000000b в 8-битном представлении, а белый цвет — как FFh или 11111111b. Имея 8 бит, каждое из которых может принимать значения 0 или 1, количество различных комбинаций равно 256 (2^8). Представим, что все пиксели до внедрения имели черный цвет: 00000001 00000011 00000010 00000011. Можно подсчитать изменение цвета каждого из пикселей: первый пиксель изменится на 1/255, второй на 2/255, третий на 2/255, а четвертый на 3/255. Подобные изменения не заметны для человеческого глаза и могут не фиксироваться на оборудовании с низкой чувствительностью. Преимуществом такого подхода является простота реализации. Этот метод применим для большого количества форматов, использующих наборы чисел для описания данных, отражающих характеристики блоков (видео, музыка, изображения и так далее). Для его применения необходимо, чтобы формат данных хранил массив значений, который затем преобразуется для восприятия человеческими органами чувств. Однако этот метод может быть обнаружен при помощи анализа энтропии наименьших значащих бит контейнера. Для борьбы с этим можно использовать предварительную обработку сообщения, помогающую придать ему статистические свойства, характерные для конкретного контейнера или его типов. Несмотря на это, метод LSB остается одним из наиболее известных и классических алгоритмов сокрытия информации благодаря своей простоте и универсальности.

При оценке данного метода стоит учитывать связи между младшими битами соседних элементов и их взаимодействие с остальными битами контейнера. В формате BMP для анализа используются наименьшие значащие биты цветовых компонентов соседних пикселей изображения. Пусть n — длина последовательности. В таком случае изменение значения i-ого элемента на значение i+1 элемента этой последовательности будет определяться как «переход», где i изменяется в диапазоне от 1 до n−1. Использование двоичного формата позволяет вручную перебрать все возможные переходы. В результате получаются четыре типа переходов: из 1 в 1, из 0 в 0, из 1 в 0 и из 0 в 1. На основе собранной статистики создается гистограмма, которая даёт возможность сделать вывод о наличии скрытого сообщения в анализируемом контейнере. Для каждого бита формируются четыре столбца, которые соответствуют переходу, как показано на рис. 1 и 2.

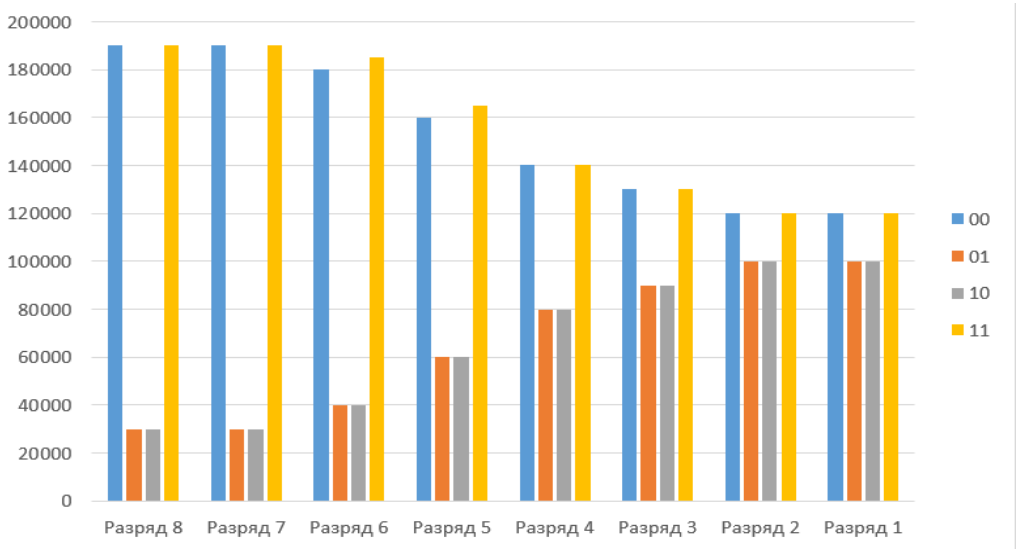

Рис. 1. Гистограмма пустого контейнера

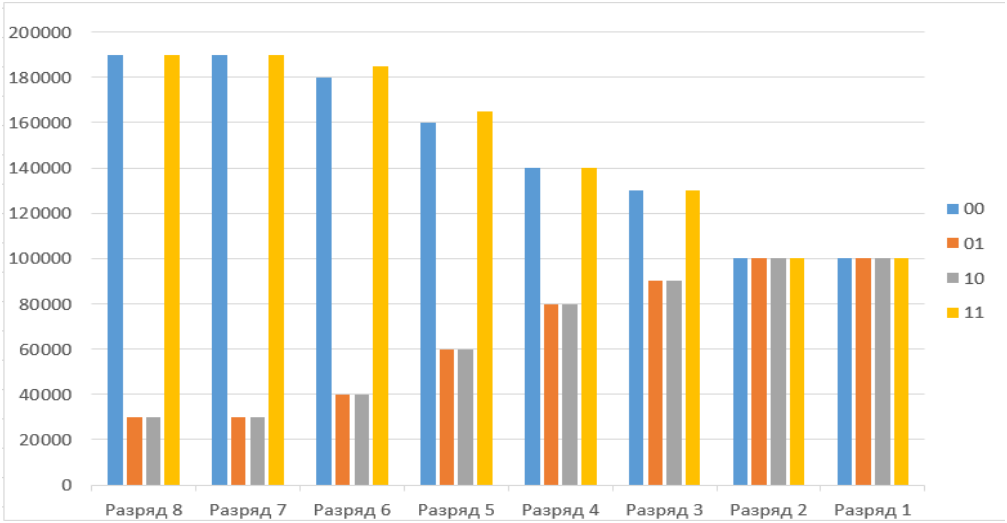

Рис. 2. Гистограмма контейнера с секретной информацией

Гистограмма пустого контейнера будет иметь разное число переходов в каждом разряде, так как распределение наименее значимых бит (НЗБ) имеет случайный характер, как показано на рис. 1.

Гистограмма контейнера, содержащего секретную информацию, будет иметь примерно равные состояния, что не свойственно пустому контейнеру.

В работе [6] был предложен метод подсчёта статистики:

$$\theta = \frac{m_{00} - m_{01}}{2} - \frac{m_{11} - m_{10}}{2},$$

где m_{ij} — количество переходов НЗБ из значения i в значение j.

Экспериментально необходимо будет найти критерий θ, который будет отвечать за принятие решения о наличии или отсутствии вложения в изображение.

Заключение. Стеганография обладает богатой историей, но, несмотря на это, остается еще недостаточно исследованной областью. Существование известных методов и формирование общей теоретической базы создают возможности для применения стеганографических технологий в практических задачах. Однако наличие множества нерешенных вопросов и отсутствие строгих теоретических основ подчеркивают необходимость проведения дополнительных исследований в этой сфере. В частности, важно разработать четкие математические модели для оценки различных методов, применяемых для сокрытия информации. С учетом полученных данных был выбран метод, который станет основой дальнейшего исследования и разработки программных инструментов. В частности, акцент сделан на использовании нечетких зашумленных битов (НЗБ) для встраивания информации в контейнеры, представляющие собой изображения в формате BMP. Этот формат предпочтителен, поскольку он не подвержен сжатию, что способствует сохранению качества и целостности скрываемой информации.

Список литературы

1. Артёхин Б.В. Стеганография. *Защита информации. Конфидент.* 1996;(4):47–50.

2. Швидченко И.В. Анализ криптостеганографических алгоритмов. *Проблемы управления и информатики.* 2007;4:149–155.

3. Барсуков В.С., Романцов А.П. Компьютерная стеганография: вчера, сегодня, завтра. Технологии информационной безопасности XXI века. *Специальная техника.* 1988;(4–5). URL: https://skte.narod.ru/lib034.htm (дата обращения: 21.03.2025).

4. Генне О.В. Основные положения стеганографии. *Защита информации. Конфидент.* 2000;(3):20–24. URL: https://citforum.ru/internet/securities/stegano.shtml (дата обращения: 21.03.2025).

5. Грибунин В.Г., Оков И.Н., Туринцев И.В. *Цифровая стеганография.* Москва: Солон-Пресс; 2003. 263 с.

6. Конахович Г.Ф., Пузыренко А.Ю. *Компьютерная стеганография. Теория и практика.* Киев: МК-Пресс; 2006. 288 с.

Об авторах:

Никита Александрович Галичев, студент кафедры кибербезопасности информационных систем Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), galichevnikita@yandex.ru

Дарья Андреевна Штепа, студент кафедры кибербезопасности информационных систем Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), dasha.shtepa15@gmail.com

Элина Гаиковна Товмасян, студент кафедры кибербезопасности информационных систем Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), elina.tovmasyan04@mail.ru

Ирина Александровна Алферова, старший преподаватель кафедры кибербезопасности информационных систем Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), irenphil@ya.ru

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

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Nikita A. Galichev, Student of the Information Systems Cybersecurity Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), galichevnikita@yandex.ru

Darya A. Shtepa, Student of the Information Systems Cybersecurity Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), dasha.shtepa15@gmail.com

Elina G. Tovmasyan, Student of the Information Systems Cybersecurity Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), elina.tovmasyan04@mail.ru

Irina A. Alferova, Senior Lecturer of the Information Systems Cybersecurity Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), irenphil@ya.ru

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

All authors have read and approved the final manuscript.