УДК 528.71
DOI 10.33764/2618-981X-2023-6-182-185

Н. Г. Нестеров[1], А. В. Чуваков[1]*

Стеганографический метод защиты информации в графическом файле формата GIF

[1] Самарский государственный технический университет, г. Самара, Российская Федерация
*e-mail: nesterovnikita0906@gmail.com

Аннотация. В данной статье исследуем, как можно улучшить стеганографию путем включения невзаимозаменяемых токенов (NFT) в изображения GIF, чтобы обеспечить дополнительный уровень защиты конфиденциальной информации. Стеганография — это метод сокрытия конфиденциальной информации в другом файле или носителе без изменения ее видимого содержимого. Изображения в формате GIF (Graphics Interchange Format) обычно используются в качестве носителей для стеганографических сообщений из-за простоты их передачи и широкого распространения в Интернете.

Ключевые слова: технологии NFT (Non-Fungible Token), стеганография, изображение GIF, авторские права, невзаимозаменяемый токен

N. G. Nesterov[1], A. V. Chuvakov[1]*

Steganographic Method of Protecting Information in a GIF Graphic File

[1] Samara State Technical University, Samara, Russian Federation
*e-mail: nesterovnikita0906@gmail.com

Annotaion. In this article, we explore how steganography can be improved by including non-fungible tokens (NFTs) in GIF images to provide an additional layer of protection for sensitive information. Steganography is a method of hiding sensitive information in another file or medium without changing its visible content. GIF (Graphics Interchange Format) images are commonly used as media for steganographic messages due to their ease of transmission and wide distribution on the Internet.

Keywords: technologies NFT (Non-Fungible Token), steganography, GIF image, copyright, non-fungible token

Введение

С ростом распространенности кибератак потребность в безопасных методах передачи информации стала первостепенной. Стеганография позволяет передавать конфиденциальную информацию по скрытым каналам, не привлекая к ней внимания. Скрывая информацию в изображениях GIF, можно передавать сообщения незамеченными для перехватчиков. Однако с появлением NFT (Non-Fungible Token) теперь можно усовершенствовать стеганографические методы и обеспечить дополнительный уровень безопасности [1, 2]. NFT – это уникальные цифровые активы, которые хранятся в блокчейне. Каждый NFT уникален и не может быть воспроизведен или обменен на другой токен. NFT становятся все более популярными для различных приложений, включая цифровое искусство, предметы коллекционирования и игры [3].

Стеганографические методы

Существует несколько стеганографических методов, которые могут использоваться для защиты информации в графическом файле GIF, включая:

– метод Least Significant Bit (LSB) – этот метод заключается в том, чтобы заменить наименее значимый бит каждого пикселя в изображении на биты информации, которую нужно скрыть. Данные скрываются в младших разрядах каждого пикселя, что делает их почти незаметными для человеческого глаза. Этот метод является одним из самых простых и широко используемых методов стеганографии в изображениях;

– метод маскировки – в этом методе используется маска, которая накладывается на изображение для скрытия данных. Это делается путем замены определенных цветовых пикселей на другие цвета, которые представляют биты информации. Таким образом, данные могут быть скрыты в маске, которая используется для скрытия их в изображении;

– метод частотного преобразования – в этом методе данные скрываются в высокочастотных компонентах изображения. Данные могут быть встроены в компоненты, такие как дискретное косинусное преобразование (DCT) или вейвлет-преобразование. Этот метод обычно используется в JPEG-изображениях, но также может быть применен к GIF-изображениям.

– метод встраивания NFT-элементов – этот метод заключается в встраивании информации в изображение, используя NFT-элементы. Это делается путем сокрытия метаданных NFT в младших разрядах каждого пикселя или путем встраивания самого NFT в изображение. Этот метод может быть использован для передачи конфиденциальной информации, такой как ID токена, информация о владельце, история транзакций и т.д. [4, 5].

В данной статье исследуются два метода усиления стеганографии с помощью NFT-элементов в GIF-изображениях: сокрытие метаданных NFT в младших разрядах каждого пикселя и встраивание самого NFT в изображение. Оба метода могут использоваться для передачи конфиденциальной информации в GIF-изображениях.

Методы встраивания NFT элементов

Путем включения элементов NFT в изображения GIF можно повысить безопасность стеганографии. Один из методов заключается в сокрытии метаданных NFT в младших разрядах каждого пикселя. В этом методе метаданные NFT (например, ID токена, информация о владельце, история транзакций и т.д.) могут быть сокрыты в младших разрядах каждого пикселя в GIF-изображении. Данные могут быть сокрыты с использованием метода Least Significant Bit (LSB), путем замены наименее значимого бита каждого пикселя на биты метаданных NFT. Это позволяет сохранить визуальное качество изображения, при этом скрытая информация остается защищенной от нежелательных глаз [5, 6].

Данный метод предлагает усиленную стеганографию с использованием NFT-элементов в GIF-изображениях. Такой подход может быть использован в

различных областях, таких как в электронной коммерции, где GIF-изображения могут быть использованы для передачи информации о товарах и услугах, а также в медицинских областях, где GIF-изображения могут быть использованы для передачи конфиденциальной информации о пациентах [7].

Другой метод включает встраивание NFT в само изображение GIF. В этом методе сам NFT может быть встроен в GIF-изображение. Для этого необходимо определить определенный участок изображения, который будет использоваться для встраивания NFT. В этом участке можно использовать определенные пиксели для представления битов информации NFT. После встраивания NFT в изображение оно может быть сохранено в формате GIF и передано получателю [7].

Этот метод также предоставляет усиленную стеганографию с использованием NFT-элементов в GIF-изображениях. Этот подход может быть использован в качестве дополнительного слоя защиты, что делает его особенно полезным для передачи конфиденциальной информации, такой как ID токена, информация о владельце, история транзакций и т.д. [4].

Оба этих метода демонстрируют возможности усиленной стеганографии в GIF-изображениях с использованием NFT-элементов. В данной статье будет произведено сравнение этих методов на основе критериев, таких как качество изображения, стойкость к атакам и скорость встраивания/извлечения данных [8].

Сравнение методов

Для сравнения двух методов рассмотрены следующие критерии: качество изображения, стойкость к атакам и скорость встраивания/извлечения данных.

Качество изображения. Оба метода позволяют сохранить качество изображения на высоком уровне. Однако, при использовании метода встраивания NFT в изображение, может потребоваться выделить определенную область изображения, что может повлиять на общее качество изображения.

Стойкость к атакам. Метод сокрытия метаданных NFT в младших разрядах каждого пикселя имеет более высокую стойкость к атакам, чем метод встраивания самого NFT в изображение. Это связано с тем, что второй метод может быть подвержен атакам, которые могут изменять выбранный участок изображения и портить данные NFT.

Скорость встраивания/извлечения данных. Метод сокрытия метаданных NFT в младших разрядах каждого пикселя обычно требует больше времени на встраивание и извлечение данных, так как данные должны быть встроены в каждый пиксель. Метод встраивания самого NFT в изображение, в свою очередь, может быть выполнен быстрее, так как данные NFT могут быть легко встроены в определенный участок изображения [9].

Исходя из этих критериев, можно сделать вывод, что оба метода имеют свои преимущества и недостатки в зависимости от конкретной ситуации, в которой они могут быть использованы. Например, метод сокрытия метаданных NFT в младших разрядах каждого пикселя может быть полезен в случае, когда стойкость к атакам является приоритетной задачей. Метод встраивания самого NFT в изображение может быть более подходящим в случае, когда необходимо

быстро встроить данные NFT в изображение и сохранить высокое качество изображения [9, 10].

Заключение

В заключение можно сказать, что включение элементов NFT в стеганографию в изображениях GIF обеспечивает дополнительный уровень безопасности для защиты конфиденциальной информации. Встраивая метаданные NFT в LSB каждого пикселя или создавая уникальный NFT для представления изображения GIF, можно передавать сообщения скрытно и безопасно. Однако стеганографию, усиленную NFT, следует использовать в сочетании с другими мерами безопасности, чтобы обеспечить максимальную защиту конфиденциальной информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Луговой В. Е. Non-Fungible Token (NFT). В сборнике: информационные технологии, системный анализ и управление (ИТСАУ-2021). Ростов-на-Дону – Таганрог, 2021. С. 173-175.

2. Тройнин Р. А., Корниленко О. И., Денисенко В. В. Обзор технологии NFT, ее структура и особенности. Инновации. Наука. Образование. 2022. № 52. С. 515-520.

3. Анненко А. И., Кочетков П. С. Правовая природа NFT с точки зрения права интеллектуальной собственности. В сборнике: дни науки факультета права НИУ «Высшая школа экономики». Сборник докладов VI Ежегодной научно-практической конференции. Москва, 2022. С. 95-100.

4. Ванцовская А. А. Цифровое искусство на блокчейне и NFT-рынок. StudNet 2021. Т. 4 № 7. С. 25.

5. Петрова А. Цифровое искусство на примере NFT. Проблемы распределения прав при обращении NFT на блокчейн-платформах. В сборнике: Правовая защита интеллектуальной собственности: проблемы теории и практики. Сборник материалов X Международного юридического форума (IP Форум). 2022. С. 312-316.

6. Исааков Г. Н., Соколова Е. С. В сборнике: Молодежь в науке 2023. Сборник статей Международного научно-исследовательского конкурса. г. Петрозаводск, 2023. С. 179-183.

7. Лаптева И. Е. Применение технологии NFT в области создания цифрового контента. Академическая публицистика. 2022. № 6-1. С. 126-139.

8. Зобов А. NFT-токены: Правовой статус и их роль в IP. В сборнике: Правовая защита интеллектуальной собственности: проблемы теории и практики. Сборник материалов X Международного юридического форума (IP форум). 2022. С. 234-237.

9. Мисиченко Н. Ю., Асанов А. Р. Особенности технологии (NFT). В сборнике: Теория и практика менеджмента: состояние и перспективы. Сборник материалов международной научно-практической конференции профессорско-преподавательского состава, молодых ученых и студентов. Ростовский государственный экономический университет (РИНХ). 2022. С. 75-81.

10. Чикалова Ю. А. NFT и криптоискусство, влияние технологии NFT на арт-рынок. Инновации. Наука. Образование. 2021. № 48. С. 2659-2663.