и оптимизированные архитектуры, предоставляют новые возможности для решения вызовов, стоящих перед современной математикой и вычислительной техникой.

Список литературы

1. В. А. Головко, В. В. Краснопрошин. – Минск: БГУ, 2017. – 263 с. – (Классическое университетское издание).

УДК 004.056.5

ПРИМЕНЕНИЕ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

А. В. Попов
Полоцкий государственный университет имени Евфросинии Полоцкой, Новополоцк, Беларусь
Научный руководитель: И. Б. Бурачёнок к.т.н., доцент

Введение. В современном информационном мире как никогда возникает проблема защиты прав собственности на информацию, представленную в цифровом виде. Примерами такой информации могут послужить фотографии, аудио и видеозаписи и т. п. Представление и передача сообщений в цифровом виде безусловно дает современному человеку большие преимущества при обмене информацией. Однако представление информации в цифровом виде и распространение ее посредством современных технологий способствует не только ее модификации, но и ее воровства. Информация может быть легко скопирована и распространена без согласия правообладателя. Данная проблема повлекла за собой развитие современных методов защиты информации, представленной в электронном виде. Причем, если рассматривать одно из направлений защиты – медиаконтент, то данное направление повлекло за собой большое количество исследований в области стеганографии. Таким образом, исследование методов компьютерной стеганографии, применяемых в медиа-файлах на основе встраивания цифровых водяных знаков, является актуальным.

Цель работы исследовать метод стеганографии Куттера-Джордана-Боссена для защиты медиаконтента.

При использовании стеганографических методов, защита информации происходит на трех уровнях [3]:

1. неизвестен сам факт передачи скрытой информации;
2. неизвестен алгоритм помещения скрытой информации в контейнер (под контейнером подразумевается открытый текст, где скрыта зашифрованная информация);
3. неизвестен способ кодирования информации.

Стеганография предоставляет такие направления как: встраивание информации с целью её скрытой передачи, встраивание цифровых водяных знаков, встраивание идентификационных номеров, встраивание заголовков. Она бывает нескольких видов: текстовая, сетевых файлов, видео, аудио и изображений [1].

Для защиты авторских прав видео, аудио, текстов и изображений лучше всего подходит встраивание цифровых водяных знаков. Данный метод допустимо применять для защиты авторских прав, например на студенческие дипломные, курсовые, проектные работы или же звуко- или видеозаписи.

Цифровой водяной знак (далее ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом контролировать его использование [2].

Метод ЦВЗ основан на принципе, который используется для защиты документов от подделки. Особенность этого метода в том, что он позволяет внедрять цифровые водяные знаки, которые не видны глазу, в отличие от традиционных водяных знаков. Для расшифровки этих скрытых знаков нужен специальный декодер. Метод ЦВЗ применим к изображениям, а также к аудио- и видеофайлам. ЦВЗ, делятся на несколько типов: ЦВЗ, которые выдерживают любые изменения контейнера, ЦВЗ, которые ломаются или меняются при небольшой модификации контейнера, ЦВЗ, которые реагируют по-разному на разные воздействия. Их также можно называть: устойчивыми, хрупкими и полухрупкими. [3]

У метода стеганографии есть множество различных алгоритмов реализации этих трёх уровне, примером есть, метод Куттера-Джордана-Боссена (метод креста) []. Метод Куттера-Джордана-Боссена относится к классу алгоритмов, осуществляющих скрытие данных в пространственной области. В алгоритмах этого класса внедрение ЦВЗ выполняется за счет изменения яркостной либо цветовых компонент пикселя. В этом методе отдельные биты водяного знака многократно внедряются в изображение путём изменения значения синего канала в пикселе. Это изменение пропорционально яркостной компоненте пикселя и может принимать как положительные, так и отрицательные значения в зависимости от значения встраиваемого бита водяного знака.

Далее более подробно рассмотрим метод Куттера-Джордана-Боссена (метод креста), для этого введём некоторые обозначения [4]:

$B_{x,y}$ – яркость синего цвета пикселя с координатами (x, y);

$B_{x,y}$ * – изменённая яркость синего цвета пикселя;

$Y_{x,y}$ – яркость пикселя;

m_i – i-ый бит сообщения, которое мы хотим встроить;

f – коэффициент, задающий энергию встраиваемого бита данных (задаётся исходя из функционального назначения и особенности стегосистемы);

σ – размер области, по которой будет прогнозироваться яркость.

Для встраивания информации в контейнер используется одно из свойств зрительной системы человека. Это свойство заключается в том, что восприимчивость человека к изменениям яркости синего цвета по сравнению с красным и

зелёным – меньше всего. И так, для встраивания информации будет использоваться синий цвет заданного контейнера-изображения. Изображение будем рассматривать в цветовой модели RGB как показано на рисунке 1.

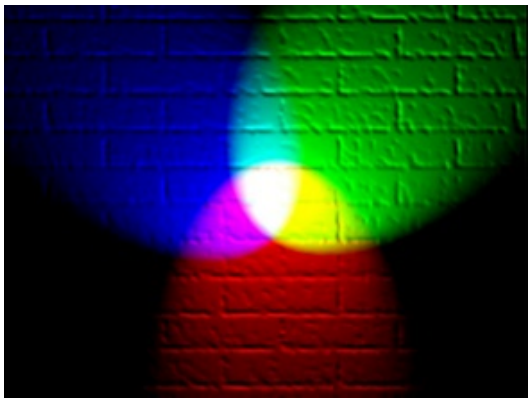

Рисунок 1 – Цветовая модель RGB

Встраивание информации будет производиться 1 бит сообщения в 1 пиксель контейнера. Секретный ключ задаёт координаты пикселей, в которые будет производиться встраивание. При встраивании яркости красного и зелёного цветов остаются без изменений, а яркость синего – изменяется по следующей формуле: [1]

$$B^*_{x,y} = \begin{cases} B_{x,y} + f * Y_{x,y}, \text{ при } m_i = 1 \\ B_{x,y} - f * Y_{x,y}, \text{ при } m_i = 0 \end{cases} \quad (1)$$

где $f = 0.1$, $Y_{x,y} = 0.3 * R_{x,y} + 0.59 * G_{x,y} + 0.11 * B_{x,y}$ [1]

Так как на принимающей стороне нет оригинального изображения, то гарантированно узнать в какую сторону изменилась яркость синего цвета мы не можем. Поэтому для извлечения прогнозируется значение яркости синего цвета как показано на рисунке 2:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\partial} (B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\partial}, \quad (2)$$

где $\partial = 1/3$.

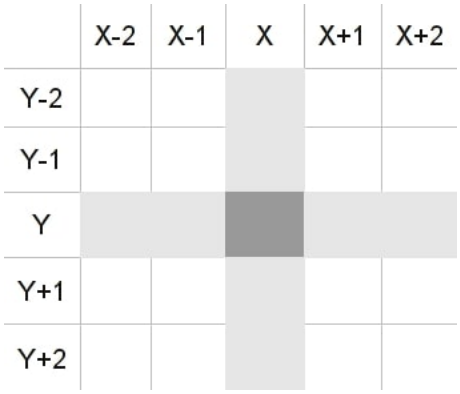

Рисунок 2 – Прогнозирование яркости синего цвета

Пиксель в центре – это пиксель, яркость синего цвета которого мы должны спрогнозировать, опираясь на пиксели, которые обозначены светло-серым цветом.

И наконец, для извлечения скрытого сообщения используется формула:

$$m_i = \begin{cases} 1, \text{ при } B_{x,y}{}^* > \overline{B_{x,y}} \\ 0, \text{ при } B_{x,y}{}^* < \overline{B_{x,y}} \end{cases} \quad [1]$$

Вывод. Таким образом, не вызывает сомнения актуальность данной тематики, стеганография имеет ряд преимуществ, например, что можно скрыть сам факт скрытия сообщения в контейнер, или же скрыть сам факт того, что кто-то пытался обойти подобную защиту и открыть содержимое или же конкретно скрыть сам файл. Всё это можно связать с защитой авторских прав. Однако следует заметить, что применение стеганографии в области авторского права является относительно новой технологией и кроме преимуществ она имеет и существенные недостатки, препятствующие ее массовому внедрению:

– отсутствие юридической поддержки при защите авторского права с помощью стеганографии (далеко не все органы власти и судебные органы на сегодня смогут принять в таком виде подтверждение авторства как доказательство);

– сложность защиты авторских прав на аудио- и видеоматериалы.

Исследованный алгоритм Куттера-Джордана-Боссена способен работать в режиме реального времени как для внесения скрытой информации в видео или же аудио поток, так и для ее извлечения, метод имеет ряд преимуществ перед другими методами, такими как простота реализации, незаметность внедрения, высокая устойчивость и гибкость. Метод может быть использован для различных целей, связанных с защитой и обработкой медиаконтента. Однако он слабо устойчив к шумовым искажениям, данный метод является эффективным и надежным способом применения компьютерной стеганографии для защиты информации на основе встраивания цифровых водяных знаков.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография: учебное пособие / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – Москва: СОЛОН-ПРЕСС, 2009. – 264 с.

2. Коробкин, А. И. Требования к цифровым водяным знакам для защиты цифровых изображений / А. И. Коробкин // Прикладные проблемы оптики, информатики, радиофизики и физики конденсированного состояния: материалы Шестой междунар. науч.-практ. конф., Минск, 20–21 мая 2021 г. / Ин-т приклад. физ. проблем Белорус. гос. ун-та ; редкол.: В. И. Попечиц [и др.]. – Минск, 2021. – с. 131-133.

3. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика». / Конахович Г.Ф., Пузыренко А.Ю. – М.: «МК-Пресс» 2006. – 288 с.

4. Kutter M., Jordan F., Bossen F. Digital watermarking of color images using amplitude modulation (англ.) : журнал. – 1998. – 1 April.

УДК 336.648

NFT КАК СОВРЕМЕННАЯ ЦИФРОВАЯ ТЕХНОЛОГИЯ

М. А. Ровнейко
Брестский государственный технический университет, Брест
Научный руководитель: С. И. Парфомук, кандидат технических наук, доцент

По данным английского словаря Collins, NFT – самое популярное слово нашей современности [3]. Этот факт объясняется тем, что у каждого пользователя в наши дни есть цифровые активы (документы в цифровом формате, бонусы в торговых сетях, сертификаты, страницы в социальных сетях, биткоины и др.). В связи с этим в настоящее время актуально предоставление возможности владения и управления цифровыми активами посредством блокчейн, которая наделяет невзаимозаменяемые ценности уникальными свойствами, индивидуализирует их [4].

Под токеном следует понимать единицу учёта для представления цифрового баланса в активе – таким образом токен выполняет функцию заменителя ценных бумаг и представляет собой запись в блокчейне, управляемую посредством смарт-контракта.

Аббревиатура NFT расшифровывается как «non-fungible token», то есть невзаимозаменяемый токен. NFT уникальны тем, что не обладают свойством взаимозаменяемости.

История NF-токенов ведёт отсчёт с 2013–2014 годов – в этот период проходили опыты с NFT на скриптовом языке блокчейна Bitcoin (проекты Colored Coins и Counterparty). В 2015 г. был начат NFT-проект Etheria – он был продемонстрирован на первой конференции разработчиков блокчейна Ethereum, которая проходила в Лондоне. Через год был запущен NFT-проект PixelMap, который хранит изображения непосредственно в блокчейне. В 2017 г. блокчейн Ethereum стал популярен по той причине, что в него было встроено создание и хранение токенов. В этом году был введён термин «невзаимозаменяемый токен» – NFT. В 2018 г. Decentraland (виртуальный мир, основанный на блокчейне) привлёк 26 млн долларов на первичном размещении монет. В течение 2020 г. на рынке NFT наблюдался быстрый рост, его стоимость достигла 250 млн долларов. Объём рынка 2021 г. оценивается в 2–3 млн долларов в месяц. Последние годы лидирующие позиции занял проект CryptoKitties.

К свойствам NF-токенов следует отнести уникальность, неделимость, быстроту операций, стандартизацию, свободную торговлю, ликвидность, программируемость, неизменность и доказуемый дефицит.