3. Сравнительный анализ доктринальных концепций правового регулирования смарт-контрактов в России и зарубежных странах / Л. Г. Ефимова, И. Е. Михеева, Д. В. Чуб. — Текст : непосредственный // Право. Журнал Высшей школы экономики. — 2020. — № 4. — С. 78-105.
4. Ante, Lennart, The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum. — URL: https://ssrn.com/abstract=3861106 (date of the application: 25.05.2022). — Text : electronic.
5. Ипполитов С. С. Интеллектуальная собственность и точки роста творческой индустрии в российской экономике: блокчейн, крипто-арт, NFT-токенизация / С. С. Ипполитов. — Текст : непосредственный // Культура и образование: научно-информационный журнал вузов культуры и искусств. — 2021. — № 2. — С. 5-18.
6. Вопросы электронного правительства в эпоху цифровой трансформации / В. А. Артамонов, Е. В. Артамонова. — Текст : непосредственный // Россия: тенденции и перспективы развития. — 2022. — № 17-1. — С. 31-39.
7. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты / пер. с англ. М. А. Райтмана. — Москва : ДМК Пресс, 2019. — 538 с.: ил. — Текст : непосредственный.
8. Mazur, Mieszko, Non-Fungible Tokens (NFT). The Analysis of Risk and Return. — URL: https://ssrn.com/abstract=3953535 (date of the application: 25.05.2022). — Text : electronic.

Д. В. Богданов, В. Ю. Швачко, М. Б. Атманских
Тюменский государственный университет, г. Тюмень

УДК 004.056

МЕТОДЫ ВНЕДРЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ВИДЕОРЯД КАК СРЕДСТВА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОГО ВИДЕОКОНТЕНТА

Аннотация. *В статье рассматриваются проблема утечек конфиденциальных данных в сфере создания медиаконтента и метод отслеживания подобных нарушений. Описаны некоторые методы нанесения цифрового водяного знака на видеоряд и особенности процедуры встраивания.*

Ключевые слова: *стеганография, цифровые водяные знаки, утечка, конфиденциальная информация.*

Введение. В настоящее время существует большое количество студий, участвующих в разработке контента для медийного бизнеса. В ходе студийной разработки обязательно присутствует процесс обмена наработками между командами или отдельными работниками студии, и, именно в ходе данного процесса может произойти утечка информации, несанкционированное распространение которой может повлечь для студии имиджевые потери или нарушить соглашение о неразглашении с заказчиком.

Для предотвращения подобных ситуаций необходимо вести строгий контроль производства и обеспечить должный уровень информационной безопасности. Однако в случае недостаточной компетентности ответственного работника, либо в случае отсутствия такового, утечка может произойти, и, необходимо заранее заручиться возможностью определить ее источник для упрощения расследования и применения дальнейших мер.

Для решения этой задачи предлагается использовать цифровые водяные знаки, встраиваемые в конфиденциальный видеоконтент, обмен которым происходит внутри студии. В ходе исследования будут рассмотрены следующие методы нанесения ЦВЗ: метод наименьшего значащего бита [1, 2], метод разности значений пикселей [3] и метод изменения уровня серого [4].

Проблема исследования. Существует ряд методов по нанесению цифровых водяных знаков. Необходимо выделить из них методики, подходящие под требования для встраивания в видеоконтент, для этого были поставлены следующие задачи:

1) выполнить обзор существующих методов внедрения ЦВЗ в изображение;

2) рассмотреть условия и особенности встраивания ЦВЗ в потоковое видео.

Методы исследования. Методами данного исследования стали: обзор, анализ, сравнение характеристик, описание работы и наглядная демонстрация исследуемых способов нанесения ЦВЗ.

Метод наименьшего значащего бита

Используя метод наименьшего значащего бита необходимо установить правило, согласно которому биты послания будут распределены по значащим пикселям в целевом кадре и определить размер

блоков для встраивания, на которые делится послание. От данной процедуры будет зависеть количество встраиваемых бит послания в байт цветности, иначе говоря — емкость. Заведомое определение данной закономерности обеспечит то, что процесс извлечения информации будет простым и получателю будет необходимо лишь извлечь биты послания из значений пикселей [1].

Пример встраивания ЦВЗ методом наименьшего значащего бита:

Установлено следующее правило: в один байт цветности можно разместить 3 бита послания. Имеем послание длиной 18 бит: 101000011011111000 и 24-битное растровое изображение. Необходимо выбрать пиксели-носители послания, в данном случае это будет следующая пара:

Пиксель 1 (10101100), (01011001), (10100100),
Пиксель 2 (10100010), (11100011), (00110111),

где в каждом пикселе первый байт — насыщенность красного оттенка, второй — насыщенность зеленого и третий — синего, соответственно. Далее необходимо поделить послание на трехбитовые блоки, которые будут помещаться в значения цветности:

101 | 000 | 011 | 011 | 111 | 000,

и, разместить их в значениях цветности выбранных пикселей, заменяя трехбитовыми блоками последние биты значения цветности по порядку:

Пиксель 1 (10101**101**), (01011**000**), (10100**011**),
Пиксель 2 (10100**011**), (11100**111**), (00110**000**).

Полученные пиксели необходимо поместить обратно в изображение. Для увеличения стойкости перед стегоанализом, в выходное изображение или кадр можно добавить искусственные помехи, при наличии которых, определить закономерность изменения НЗБ будет гораздо труднее [2].

Наглядная демонстрация результата работы алгоритма представлена на рис. 1 и 2.

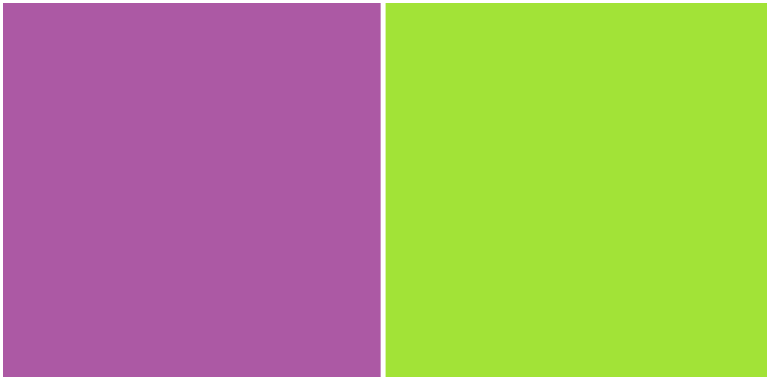

Рис. 1. Цвета пикселей до модификации

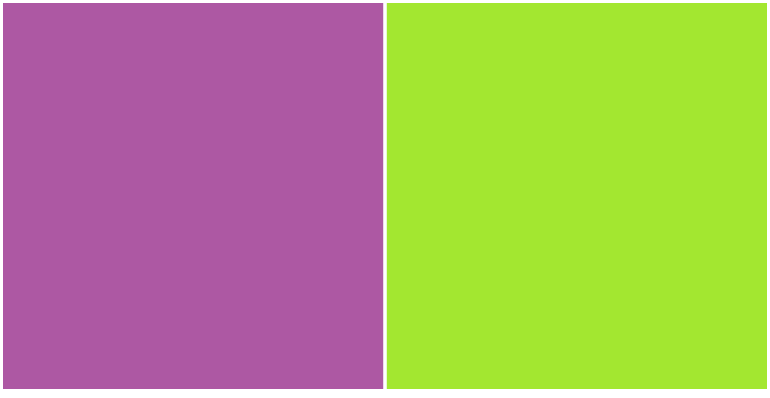

Рис. 2. Цвета пикселей после встраивания послания

Метод разности значений пикселей

В отличие от предыдущего рассмотренного метода, данный представляет возможность встраивания послания в черно-белое представление изображения. При встраивании ЦВЗ данным методом стоит учитывать особенность — в областях, где перепады пикселей небольшие, встраивание данных будет более заметным.

Встраивание происходит следующим образом: черно-белое изображение, выступающее контейнером делится на двухпиксельные блоки — g_j и g_{j+1}. Затем, вычисляется модуль разности значений

черного цвета между пикселями в блоке. Данное значение определяет размерность отрезка послания, которое возможно встроить в блок [3].

Согласно алгоритму, при встраивании каждой части послания в блок, шкала насыщенности черного (0...255) делится на диапазоны, шириной 2, возведенной в степень. Необходимо, чтобы сумма размеров диапазонов после всех преобразований составляла 256 количеству значений черного в пикселе черно-белого изображения. Авторы метода предлагают следующие наборы значений ширины w_i диапазона для разбиения шкалы: r = {8, 16, 32, 64, 128, 8} (бит) [3].

Определив диапазоны, вычислим, сколько бит послания возможно встроить. Для этого сравним модуль разности значений черного между пикселями — $|d|$, равный $(g_j - g_{j+1})$ и ширины w_i диапазонов из набора r. Первый по возрастанию диапазон r_i, где $w_i > |d|$ берем для дальнейшей работы, в противном случае, если такого диапазона нет, переходим к следующему блоку пикселей. Так, например, имея $|d| = 15$ и разбиение, предложенное авторами, для встраивания нам подойдет диапазон r_2, имеющий размер $w_2 = 16$ [3].

Имея диапазон r_2 с шириной $w_2 = 16$, вычисляется объем n_i послания, который возможно встроить. Для этого необходимо найти значение $n_i = log_2 w_i$. В данном случае, при $w_2 = 16$, $n_2 = 8$ — столько бит послания возможно встроить в имеющийся набор пикселей.

Выяснив диапазон r_i с нижней границей l_i и шириной w_i, в который будет встраиваться часть послания, определяется новая разность значений серого между пикселями d'_j:

$$d'_j = \begin{cases} l_i + b_k & для\ d \geq 0, \\ -(l_i + b_k) & в\ противном\ случае \end{cases} \quad (1)$$

где l_i — нижняя граница диапазона, а b_k — десятичное представление встраиваемой части послания. Новые значения пикселей g_j и g_{j+1} — g'_j и g'_{j+1} вычисляются следующим образом:

$$(g'_j, g'_{j+1}) = \begin{cases} (g_j - \lceil m_j \rceil, g_{j+1} + \lfloor m_j \rfloor) & \text{если } d_j \text{ - чётное} \\ (g_j - \lfloor m_j \rfloor, g_{j+1} + \lceil m_j \rceil) & \text{если } d_j \text{ - нечётное} \end{cases} \quad (2)$$

где $m_j = (d'_j - d_j)/2$. В случае, если новые значения пикселей меньше 0, либо больше 255, послание не встраивается в блок и происходит выбор нового. На рис. 3 представлена схема работы алгоритма.

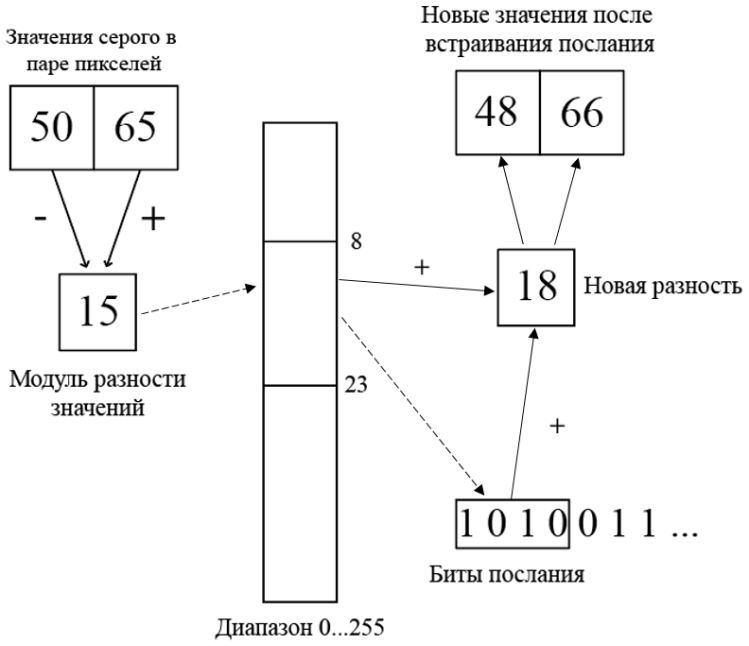

Рис. 3. Алгоритм работы метода разности значений пикселей

Метод изменения уровня серого

Данный метод равно, как и предыдущий направлен на встраивание ЦВЗ в черно-белое изображение.

Первый шаг внедрения — заменить все нечетные значения черного в пикселях четными путем изменения их на 1. Далее, необходимо установить соответствие четности значения черного и бита послания. В случае совпадения четности N-го бита цветности, приведенного к четному виду и N-го бита послания N бит цветности пикселя не изменяется, в противном случае, если N бит послания не является четным — бит уровня черного в изображении-контейнере изменяется на нечетный [4].

Операция в обратной последовательности производится при извлечении послания из контейнера. Имея заранее установленный набор пикселей, в которые встроено послание, производится проверка четности битов цветности, содержащих часть послания. В случае если значение пикселя четное — бит послания равен 0, в случае, если нечетное — 1.

Результаты

Особенности встраивания в потоковый видеоряд

Поскольку рассмотренные методы являются пространственными и нацелены на манипуляцию с конкретными кадрами видеоряда, необходимо предусмотреть практические нюансы применения ЦВЗ в видео, содержащемся в современных видеоконтейнерах.

Не каждая команда, взаимодействующая с видео, использует loseless-кодеки, а также мала вероятность того, что конфиденциальный видеофайл утечет в неизменном виде и не будет являться экранной записью с агрессивным сжатием или низким битрейтом. Для предотвращения потерь информации, которую несет изображение предлагается разбить кадры на крупные группы размером 1/100 от общего количества пикселей, в значения пикселей которых будет встраиваться одна и та же информация, а при извлечении учитываться все значения и браться превалирующее. Таким образом возможно избежать помех из-за единичных искажений значений цветности пикселей с посланием.

Заключение. Были изучены 3 метода внедрения ЦВЗ в изображение, подходящие под задачи, а также рассмотрены практические аспекты их применения при встраивании в потоковое видео. Подготовлена теоретическая почва для разработки прототипа программного комплекса.

СПИСОК ЛИТЕРАТУРЫ

1. blogspot.com : сайт. — URL: https://ghostbasenji.blogspot.com/2018/08/steganography-method-LSB.html (дата обращения: 14.05.2022). — Текст : электронный.
2. Назаренко Ю. Л. Стегоанализ метода сокрытия информации в изображении замены наименьшего значащего бита (LSB) / Ю. Л. Назаренко. — Текст : электронный // European science. — 2018. — № 3. — С. 35-40. — URL: https://cyberleninka.ru/article/n/stegoanaliz-metoda-sokrytiya-informatsii-v-izobrazhenii-zameny-naimenshego-znachaschego-bita-lsb (дата обращения: 15.05.2022).
3. Da-Chun Wu. A steganographic method for images by pixel-value differencing / Da-Chun Wu, Wen-Hsiang Tsai. — Text : direct // Pattern Recognition Letters. — 2003. — № 24.
4. Potdar V. M. Grey Level Modification Steganography for Secret Communication / V. M. Potdar, E. Chang. — Text : direct // IEEE International Conference on Industrial Informatics. — 2004. — № 2.