Научая статья

УДК 004.63
DOI 10.25205/1818-7900-2024-22-2-33-43

Метод цифровой подписи изображений без дополнительных файлов, с устойчивостью к JPEG-сжатию и удалению метаданных

Евгений Константинович Мазайшвили[1]
Елена Юрьевна Авксентьева[2]

Университет ИТМО, Санкт-Петербург, Россия

[1]evgenij997@yandex.ru
[2]avksentievaelena@rambler.ru

Аннотация

Рассмотрен метод цифровой подписи изображений, не использующий метаданные или дополнительные файлы. Цифровой подписью подписывается массив блоков 8 × 8 пикселей с примененным дискретным косинусным преобразованием, из которых состоит JPEG-файл. В качестве алгоритма подписи может быть использован любой известный алгоритм, например, RSA.

Полученная цифровая подпись преобразуется из бинарного вида в изображение. Метод преобразования основан на кодировании каждых нескольких бит подписи одной из 64 базисных функций дискретного косинусного преобразования. Далее базисная функция преобразуется в изображение обратным дискретным косинусным преобразованием. Полученная подпись, закодированная в виде изображения, присоединяется к исходному изображению справа, чтобы сформировать подписанное изображение.

Цифровая подпись обладает устойчивостью к JPEG-сжатию в регулируемых пределах. Для достижения устойчивости к сжатию используется следующий метод. Поскольку значения в блоках могут измениться при сжатии, используется квантизация – уменьшение точности значений. Она устроена таким образом, чтобы при квантизации сжатого и несжатого изображений значения в блоках после квантизации совпадали, что позволяет проверить валидность цифровой подписи. Квантизация также включает в себя шаг проверки четности полученного значения для исключения неверной трактовки значений при сильном сжатии.

Шаг квантизации не применяется к части изображения, содержащей цифровую подпись. Это связано с тем, что эта часть состоит из базисных функций дискретного косинусного преобразования, и даже при сильном сжатии соответствующая базисная функция все равно сохранит большой коэффициент и будет однозначно трактуема.

Ключевые слова

JPEG, дискретное косинусное преобразование, цифровая подпись, сжатие, изображение

Для цитирования

Мазайшвили Е. К., Авксентьева Е. Ю. Метод цифровой подписи изображений без дополнительных файлов, с устойчивостью к JPEG-сжатию и удалению метаданных // Вестник НГУ. Серия: Информационные технологии. 2024. Т. 22, № 2. С. 33–43. DOI 10.25205/1818-7900-2024-22-2-33-43

Digital Signature Method for Images without Additional Files, Robust to JPEG Compression and Metadata Removal

Evgeniy K. Mazaishvili[1], Elena Yu. Avksentieva[2]

ITMO University, Saint Petersburg, Russian Federation

[1]evgenij997@yandex.ru
[2]avksentievaelena@rambler.ru

Abstract

The article discusses a method of digitally signing images that does not use metadata or additional files. The object for signature is an array of 8x8 pixel blocks with a discrete cosine transformation applied, which make up a JPEG file. Any known algorithm can be used as a signature algorithm, for example, RSA.

The resulting digital signature is converted from a binary form to an image. The conversion method is based on encoding every few bits of the signature of one of the 64 basic functions of the discrete cosine transform. Next, the basic function is transformed into an image by an inverse discrete cosine transformation. The resulting signature, encoded as an image, is attached to the original image on the right to form a signed image.

The digital signature is resistant to JPEG compression within adjustable limits. The following method is used to achieve compression resistance. Since the values in the blocks can change during compression, quantization is used – reducing the accuracy of the values. It is designed in such a way that when quantizing compressed and uncompressed images, the values in the blocks after quantization are becoming the same, which allows you to verify the validity of the digital signature. Quantization also includes a step of checking the parity of the received value to avoid misinterpretation of values when compression is strong.

The quantization step does not apply to the part of the image containing the digital signature. This is due to the fact that this part consists of the basic functions of the discrete cosine transform, and even with strong compression, the corresponding basic function will still retain a large coefficient and will be unambiguously interpreted.

Keywords

JPEG, Discrete cosine transform, Digital signature, Compression, Image

For citation

Mazaishvili E., Avksentieva E. Digital signature method for images without additional files, robust to JPEG compression and metadata removal. *Vestnik NSU. Series: Information Technologies*, 2024, vol. 22, no. 2, pp. 33–43 (in Russ.) DOI 10.25205/1818-7900-2024-22-1-33-43

Введение

Цифровая подпись представляет собой математическую схему, позволяющую верифицировать подлинность и целостность документа, представленного в цифровом виде [1]. Современный криптографический алгоритм цифровой подписи может быть применен к любому цифровому файлу. Большинство реализаций предполагают создание дополнительного файла таким образом, что подписанным документом будет считаться оригинальный файл + файл цифровой подписи. Многие форматы файлов, как, например, PDF, поддерживают встраивание цифровой подписи внутрь исходного файла [2]. В этом случае подписанным документом будет считаться исходный файл со встроенной цифровой подписью.

Однако для цифровых изображений в двух самых популярных форматах – JPEG и PNG – не существует схемы хранения цифровой подписи внутри исходного файла. Таким образом, существует лишь два варианта реализации цифровой подписи изображения.

1. Встраивание подписи в метаданные изображения, например, dSIG-чанки для изображений в формате PNG и метаданные EXIF для изображений в формате JPEG.
2. Сохранение отдельного файла цифровой подписи в дополнение к исходному файлу.

Обе реализации имеют недостаток в виде невозможности передачи подписанных изображений через загрузку в популярные социальные сети, мессенджеры и на популярные хостинги изображений. Причина заключается в том, что вышеперечисленные среды выполняют перекодирование изображений, удаляя метаданные. Многие из них выполняют JPEG-сжатие в дополнение к удалению метаданных.

JPEG (Joint Photographic Experts Group) – это спецификация для сжатия цифровых изображений с потерями, основанная на дискретном косинусном преобразовании – discrete cosine transform, далее DCT [3]. Использование DCT позволяет перевести изображение из пространственного представления (массива пикселей) в частотное представление (сумму косинусных функций разной частоты). Удаление самых высокочастотных функций и обратное преобразование в пространственное представление приводит к большому коэффициенту сжатия без видимого ухудшения качества изображения.

Целью данной работы является создание метода встраивания цифровой подписи в изображение формата JPEG для передачи через среды, выполняющие перекодирование изображений (рис. 1).

Рис. 1. Ожидаемая схема работы цифровой подписи
Fig. 1. Scheme of expected digital signature method

Предлагаемый метод выполняет модификацию самого изображения в виде добавления на его правую грань дополнительных пикселей, содержащих подпись. Подпись должна быть устойчива к JPEG-сжатию в определенных пределах.

1. Предлагаемый метод

Главная проблема при реализации ЭЦП для подписи изображений с устойчивостью к сжатию – это отсутствие гарантии, что после сжатия цвета пикселей изображения останутся без изменений. Соответственно, в качестве объекта подписи нельзя использовать массив всех пикселей. Также нельзя использовать приблизительные значения пикселей как объект цифровой подписи. В этом случае злоумышленник имеет возможность изменять цвета пикселей в определенных пределах, формируя неправильное изображение, не нарушая подписи.

1.1. Подпись изображения

Предлагаемый метод подписи состоит из шести шагов.

1. Вычисление массива DCT-блоков из черно-белого исходного изображения.
2. Квантизация DCT-блоков на фиксированную величину.
3. Вычисление таблицы четности для каждого DCT-блока. Эта таблица позволит цифровой подписи остаться валидной при небольших изменениях в DCT-блоке, например, при сжатии.
4. Цифровая подпись массива DCT-блоков алгоритмом RSA.
5. Кодирование полученной подписи и таблиц четности в отдельное изображение (далее по тексту: изображение-подпись, см. рис. 8, справа) методом, дающим изображению-подписи устойчивость к JPEG-сжатию.
6. Присоединение изображения-подписи к исходному изображению.

1.2. Верификация подписанного изображения

Метод верификации подписи состоит также из шести шагов.

1. Разделение подписанного изображения на исходное изображение и изображение-подпись.
2. Расшифровка данных из изображения-подписи – получение подписи в готовом для верификации виде и таблиц четности.
3. Вычисление массива DCT-блоков из исходного изображения.
4. Квантизация DCT-блоков на фиксированную величину
5. Внесение поправок в DCT-блоки из таблиц четности.
6. Проверка: совпадает ли прочитанная на шаге 2 цифровая подпись с хешем массива DCT-блоков.

Предлагаемый метод имеет ограничение в виде возможности верифицировать только черно-белые изображения.

Метод имеет некоторую схожесть со стеганографией, основанной на сокрытии данных в DCT-коэффициентах [4]. Коэффициенты анализируются, и результат этого анализа выявляет скрытую изначально информацию – является подпись валидной или нет. Однако данный метод не предназначен для сокрытия информации внутри JPEG-изображений. При взгляде на итоговое изображение будет видно, что оно состоит из двух частей – само изображение и его подпись.

Второстепенной проблемой в данном методе является то, что цифровая подпись должна сама являться изображением и быть присоединенной к подписываемому изображению. Это сделает ее подверженной JPEG-сжатию, которое нарушит подпись. Соответственно, подпись должна устойчиво читаться при сжатии изображения в определенных пределах.

2. Создание подписи

Исходное изображение может быть как сжатым без потерь, например, в формате PNG, так и сжатым с потерями в формате JPEG. Далее будет описан процесс для изображения, сжатого без потерь. Процесс сжатия файла формата JPEG отличается лишь отсутствием необходимости вычислять массив DCT-блоков, так как он уже содержится в файле.

2.1. Вычисление массива DCT-блоков из исходного изображения

Дискретное косинусное преобразование (DCT) – алгоритм, преобразующий изображение из пространства пикселей в частотное пространство, где каждому блоку 8 × 8 пикселей ставится в соответствие блок 8 × 8 коэффициентов [5]. Пример DCT-блока представлен на рис 2.

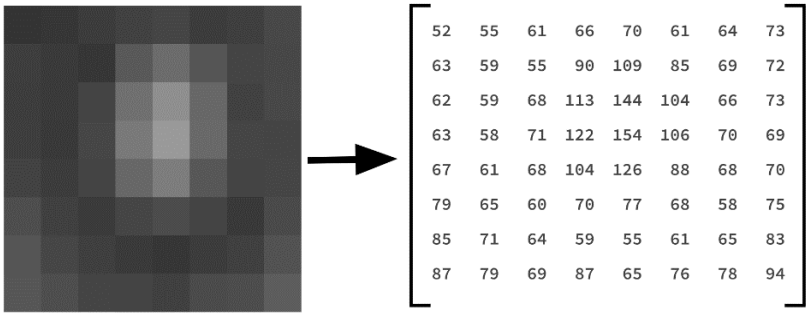

Рис. 2. Дискретное косинусное преобразование участка 8 × 8 пикселей
Fig. 2. Discrete cosine transform of block 8 by 8 pixels

Значения в DCT-блоке имеют диапазон от –1023 до 1023 с шагом 1. Большему значению соответствует большая амплитуда соответствующей косинусной функции и большая яркость определенных пикселей, зависящих от функции.

С точностью до ошибок округления DCT является алгоритмом преобразования без потерь – таблицу можно преобразовать обратно в исходный массив пикселей.

На этом шаге метода исходное изображение преобразуется в массив DCT-блоков.

2.2. Квантизация DCT-блоков на заданную величину

Квантизация является вторым шагом метода. Этот шаг делает значения в DCT-блоках более грубыми, выполняя квантизацию с определенным шагом. Квантизация представляет собой преобразование, где каждое значение внутри DCT-блока преобразуется по формуле:

$$value_i = floor(\frac{value_i}{Q_i}) * Q_i, \quad (1)$$

где Q_i – значение шага квантизации из таблицы шагов квантизации.

В методе используется переменное значение шага в зависимости от места значения в таблице: шаг увеличивается к нижнему правому углу таблицы. Это сделано по причине того, что алгоритм сжатия JPEG вносит более сильные искажения в значения ближе к нижнему правому углу DCT-блока, где представлены более мелкие детали изображения. Поскольку мы хотим точнее сохранить более явные детали, то для значений ближе к левому верхнему углу таблицы используются меньшие шаги квантизации. Значение в левом верхнем углу имеет больший шаг, так как его изменение приводит лишь к изменению общей яркости блока в итоговом изображении. Используемые значения шага обозначены на рис. 3.

$$\begin{bmatrix} 40 & 25 & 25 & 25 & 25 & 40 & 40 & 80 \\ 25 & 25 & 25 & 25 & 40 & 40 & 80 & 80 \\ 25 & 25 & 25 & 40 & 40 & 80 & 80 & 90 \\ 25 & 25 & 40 & 40 & 80 & 80 & 90 & 90 \\ 25 & 40 & 40 & 80 & 80 & 90 & 90 & 90 \\ 40 & 40 & 80 & 80 & 90 & 90 & 90 & 90 \\ 40 & 80 & 80 & 90 & 90 & 90 & 90 & 90 \\ 80 & 80 & 90 & 90 & 90 & 90 & 90 & 90 \end{bmatrix}$$

Рис. 3. Значение шага квантизации в зависимости от места значения в блоке
Fig. 3. Quantization step value for different places in a block

Смысл квантизации можно представить как уход от точных значений в блоке и работу с диапазонами значений. Например, значение 529 в блоке при 60%-м сжатии исказится до 521, но при шаге квантизации 10, они оба будут попадать в интервал 520–530. Аналогично при шаге 50: оба значения будут попадать в интервал 500–550. Нижнее значение диапазона является результатом квантизации с определенным шагом, как на рис. 4.

```
До квантизации:
[[ -98 -227  118  -45   72  -68   48  -24]
 [-197 -165  -42   41   -2   -2   -4   -4]
 [  96   81    3  -24  -15    4   -1    6]
 [ -28  -13   34   37   11    5    4    0]
 [  -8  -19  -26  -13   -1   -3   -6    2]
 [  11   14    4   -7  -12    0    5    0]
 [  -5   -2   10   19   15    4   -1    2]
 [   2   -4  -11  -12   -9    0    3    2]]

После квантизации:
[[-120 -250  100  -50   50  -80   40  -80]
 [-200 -175  -50   25  -40  -40  -80  -80]
 [  75   75    0  -40  -40    0  -80    0]
 [ -50  -25    0    0    0    0    0    0]
 [ -25  -40  -40  -80  -80  -90  -90    0]
 [   0    0    0  -80  -90    0    0    0]
 [ -40  -80    0    0    0    0  -90    0]
 [   0  -80  -90  -90  -90    0    0    0]]
```

Рис. 4. Значения в одном из DCT-блоков до и после квантизации (используются шаги квантизации с рис. 3)
Fig. 4. Values in one of DCT blocks before and after quantization (using quantization steps from fig. 3)

Квантизованные блоки не переводятся обратно в пиксели и не сохраняются в итоговом подписанном изображении. Они нужны только для этапа вычисления их хеша. Именно хеш от всех квантизованных блоков является объектом цифровой подписи.

Если бы в качестве объекта подписи вместо квантизованных, т. е. приблизительных значений DCT-блоков, использовались приблизительные значения пикселей с заданной погрешностью, злоумышленник мог бы изменять их в пределах этой погрешности, вырисовывая нужные детали на изображении. В данной работе используются приблизительные значения, но не пикселей, а DCT-блоков, изменение которых злоумышленником приведет лишь к изменению малозаметных деталей на изображении.

2.3. Вычисление таблицы четности для каждого DCT-блока

При квантизации блока может оказаться, что некоторые значения находятся на границе интервала квантизации или близко к границе. Например, для квантизации с шагом 10 значение 50 будет находиться на границе интервалов 40–50 и 50–60. В этом случае даже небольшое искажение при сжатии может сместить значение в неправильный интервал, делая подпись невалидной.

Для того чтобы избежать этой проблемы, каждому из интервалов, определяемых шагом квантизации, присваивается четность как на рис. 5.

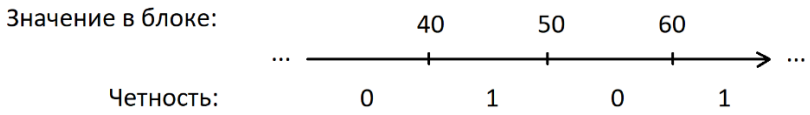

Рис. 5. Вычисление четности для каждого значения в квантизованном блоке
Fig. 5. Parity calculation for every value in quantized block

Вместе с цифровой подписью сохраняется четность каждого значения для каждого блока в виде одного бита. Например, при шаге квантизации 10 значение 51 находится в нечетном интервале 50–60, а значение 49 – в четном интервале 40–50.

Таким образом, к каждому квантизованному блоку рассчитывается соответствующая ему таблица четности. Эта таблица позволяет на этапе расшифровки делать поправки в значения блока, если значение при сжатии случайно преодолеет границу интервала. Пример таблицы четности приведен на рис. 6.

```
[[1 0 0 0 0 0 1 1]
 [0 1 0 1 1 1 1 1]
 [1 1 0 1 1 0 1 0]
 [0 1 0 0 0 0 0 0]
 [1 1 1 1 1 1 1 0]
 [0 0 0 1 1 0 0 0]
 [1 1 0 0 0 0 1 0]
 [0 1 1 1 1 0 0 0]]
```

Рис. 6. Таблица четности для значений из нижнего блока на рис. 4
Fig. 6. Parity table for values in bottom block from fig. 4.

Таблица занимает 64 бита на каждый участок изображения 8 × 8 пикселей.

2.4. Цифровая подпись хеша массива DCT-блоков алгоритмом RSA

Массив всех квантизованных блоков + массив таблиц четности хешируются алгоритмом SHA-256, и получаемый хеш подписывается закрытым ключом согласно алгоритму RSA.

В результате четвертого шага получается всего два артефакта, необходимых для верификации подписи: подписанный хеш размером 2048 бит (при использовании RSA-2048) и массив таблиц четности размером 64 бит × количество блоков 8 × 8 пикселей в изображении.

2.5. Кодирование полученной подписи и таблиц четности в изображение-подпись

Подписанный хеш и таблицы четности должны храниться непосредственно в изображении, и для этого они должны быть устойчивыми к JPEG-сжатию.

Для того чтобы достичь устойчивости к сжатию, была исследована одна из особенностей работы дискретного косинусного преобразования. DCT-блок представляет собой блок 8 × 8 значений, от –1023 до 1023. Блок, состоящий только из максимальных и минимальных значений, будет демонстрировать устойчивость к сжатию, так как сжатие такого блока приведет к тому, что в значения будут внесены лишь незначительные искажения. Например, значение –1023

может стать значением –990 после сжатия. Однако близость его к минимальному значению позволит однозначно считать его минимальным значением. Таким образом, изображение, составленное из DCT-блоков с максимальным и минимальным значением, будет устойчиво к очень высокому уровню сжатия.

В данной работе используется три значения: –1023, 0 и 1023. Таким образом, в одном значении DCT-блока в изображении-подписи хранится 2,5 бит полезной информации. Пример такого блока представлен на рис. 7.

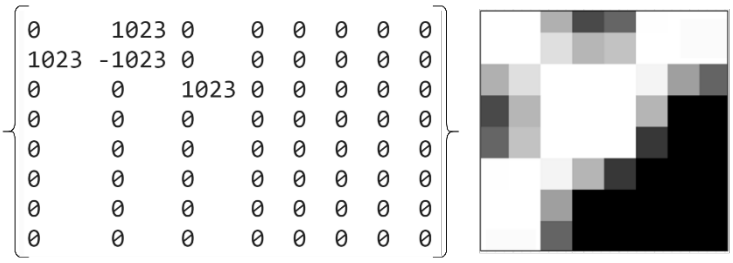

Рис. 7. Искусственно созданный DCT-блок (слева) и соответствующий ему блок пикселей (справа), который будет включен в финальное изображение-подпись
Fig. 7. Artificialy crafted DCT block (left) and corresponding pixel block (right), that will be included into the final image-signature

Таким образом, кодируя 64 × 2,5 бита в картинку 8 × 8 пикселей, все таблицы четности уместятся в зону, занимающую не более 1/3 изображения.

2.6. Присоединение изображения-подписи к исходному изображению

После кодирования изображение-подпись, содержащее подписанный хеш и таблицы четности, присоединяется к исходному изображению (см. рис. 8).

Рис. 8. Слева направо: исходное изображение, изображение с цифровой подписью
Fig. 8. Left to right: original image, image with digital signature

Размер области с подписью всегда составляет фиксированную часть изображения, так как количество таблиц четности линейно зависит от размера изображения, а подписанный хеш имеет фиксированную длину.

На этом шаге процесс подписи завершается.

3. Верификация ЭЦП

Входные данные для этапа верификации – изображение с цифровой подписью. Изображение не содержит метаданных из исходного файла и, вероятно, было сжато алгоритмом JPEG.

3.1. Разделение подписанного изображения на исходное и изображение-подпись

Поскольку размер цифровой подписи известен, разделение изображений на исходное и подпись является тривиальным.

3.2. Расшифровка данных из изображения-подписи – получение подписи в готовом для верификации виде и таблиц четности

Для расшифровки изображения-подписи каждый участок 8 × 8 пикселей переводится в DCT-блок, значения которого округляются до ближайшего: 1023; 0 или –1023.

Таким образом, восстанавливаются подписанный хеш и таблицы четности.

3.3. Вычисление массива DCT-блоков из исходного изображения.

Шаг аналогичен первому шагу при подписывании изображения.

Вычисление DCT не требуется, если файл уже находится в формате JPEG, в таком случае достаточно лишь прочитать готовые DCT-блоки из файла.

3.4. Квантизация DCT-блоков на фиксированную величину

Шаг квантизации полностью повторяет таковой при подписи изображения. Цель этого шага – получить такие же квантизованные блоки, какие были в изображении на момент подписи, чтобы подпись была валидной.

3.5. Внесение поправок в DCT-блоки из таблиц четности

На этом шаге происходит расчет таблиц четности для квантизованных блоков, аналогично шагу подписи. Однако, в отличие от аналогичного шага при подписи, при верификации происходит сравнение таблиц, и уже по результатам сравнения происходит корректировка значений блоков: те значения, которые могли выйти за границу своего интервала, поскольку находились близко к ней, возвращаются в свой интервал.

Если рассчитанная четность значения в блоке не совпадает с соответствующей четностью, записанной в таблице четности в подписи, выполняется коррекция.

Алгоритм данной коррекции описывается формулой:

$$v_i = \begin{cases} |\hat{v}_i - v_i| > \frac{Q_i}{2}: & v_i + \frac{Q_i}{2} \\ \text{else:} & v_i - \frac{Q_i}{2} \end{cases}, \quad (2)$$

где Q_i – таблица шагов квантизации, v – квантизованое значение в блоке, $\hat{v}$ – значение в блоке до квантизации.

Формула описывает следующее преобразование. Если значение ближе к нижней границе интервала, то оно считается ошибочно попавшим в него из нижестоящего интервала. Интервал в квантизованной таблице меняется на нижестоящий. Если же значение ближе к верхней границе интервала, то оно считается ошибочно попавшим в него из вышестоящего интервала. Интервал в квантизованной таблице меняется на вышестоящий.

3.6. Проверка – совпадает ли прочитанная на шаге 2 цифровая подпись с рассчитанным хешем

Последним шагом происходит хеширование массива DCT-таблиц и таблиц четности из подписи по той же схеме, что и при подписывании изображения, после чего полученный хеш сравнивается с тем, что находится в цифровой подписи. Совпадение хешей указывает на то, что подпись верна. Несовпадение указывает либо на слишком сильное сжатие, либо на намеренное искажение изображения.

Заключение

В работе рассмотрен метод цифровой подписи изображений в формате JPEG, а также в любом формате сжатия без потерь, например, PNG. Метод обладает устойчивостью к JPEG-сжатию, благодаря использованию в качестве объекта подписи квантизованых DCT-блоков. Устойчивость к сжатию достигается за счет хранения данных цифровой подписи в виде изображения, состоящего из базовых функций DCT максимальной амплитуды.

Метод может использоваться как упрощенная схема верификации изображений, не требующая ничего, кроме самого контента изображения.

В качестве перспективы развития метода можно увеличить плотность данных в изображении-подписи, чтобы оно занимало меньшую часть основного изображения.

Список литературы

1. **Bellare M., Goldwasser S.** Lecture Notes on Cryptography, 2008, с. 168
2. PDF (Portable Document Format), версия 1.7, ISO 32000-1, 2008 // Библиотека Конгресса. URL: https://www.loc.gov/preservation/digital/formats/fdd/fdd000277.shtml (дата обращения: 11.01.2024).
3. **Buchanan W. J.** DCT (Дискретное косинусное преобразование) // Теоретические и практические аспекты криптографии. URL: https://asecuritysite.com/comms/dct2 (дата обращения: 24.12.2023).
4. **Abdelhamid A. A., Mona F. M., Mursi A., Alsammak A. K.** Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3 // Инженерный журнал Ain Shams. 2018.

5. **Griffin J.** Полное руководство JPEG, включая сжатие и кодирование // Веб-мастер блог. URL: https://www.thewebmaster.com/jpeg-definitive-guide/ (дата обращения: 10.12.2023).

References

1. **Bellare M., Goldwasser S.** *Lecture Notes on Cryptography*, 2008, p. 168
2. PDF (Portable Document Format), version 1.7, ISO 32000-1, 2008. *Library of Congress*. URL: https://www.loc.gov/preservation/digital/formats/fdd/fdd000277.shtml (accessed: 11.01.2024).
3. **Buchanan W. J.** DCT (Discrete Cosine Transform). *Theoretical and practical aspects of cryptography*. URL: https://asecuritysite.com/comms/dct2 (accessed: 24.12.2023).
4. **Abdelhamid A. A., Mona F. M., Mursi A., Alsammak A. K.** Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3. *Ain Shams Engineering Journal*, 2018.
5. **Griffin J.** The Ultimate Guide to JPEG Including JPEG Compression & Encoding. URL: https://www.thewebmaster.com/jpeg-definitive-guide/ (accessed: 10.12.2023)

Сведения об авторах

Мазайшвили Евгений Константинович, аспирант

Авксентьева Елена Юрьевна, PhD

Information about the Authors

Evgeniy K. Mazaishvili, PhD Student

Elena Yu. Avksentieva, PhD

Статья поступила в редакцию 10.04.2024;
одобрена после рецензирования 16.04.2024; принята к публикации 16.04.2024

The article was submitted 10.04.2024;
approved after reviewing 16.04.2024; accepted for publication 16.04.2024