СРАВНЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ РАЗЛИЧНЫХ МЕТОДОВ НАНЕСЕНИЯ ВОДЯНЫХ ЗНАКОВ

COMPARISON OF THE PERFORMANCE OF DIFFERENT WATERMARKING METHODS

УДК 004

Муртазалиева Индира Амировна, магистрант, МГТУ им. Баумана, г. Москва

Murtazalieva Indira Amirovna, Graduate Student, Bauman Moscow State Technical University, Moscow, email: murtazaieva97@bk.ru

Аннотация

Развитие технологий обработки и передачи цифровой информации в настоящее время привело к появлению проблемы защиты авторских прав на мультимедийные данные. Один из подходов к решению этой проблемы основан на встраивании в цифровые объекты цифровых водяных знаков (ЦВЗ) – специальных и обычно невидимых меток, которые содержат в себе информацию о владельцах объектов. В этой статье рассмотрены основные характеристики ЦВЗ, процессы встраивания и извлечения, а также преимущества и недостатки методов, используемых при нанесении ЦВЗ на изображения.

Annotation

With the development of technologies for processing and transmitting digital information, the problem of copyright for multimedia data has arisen [1,2]. One of the approaches to solving this problem is based on the use of digital watermark objects - special and usually invisible tags containing information about the owners of the objects [3,4]. This article discusses the main characteristics of a digital watermark, the

embedding and extraction processes, and the advantages and disadvantages of the methods used when applying a digital watermark to images.

Ключевые слова: цифровые водяные знаки, сингулярное разложение, ДКП, ДВП, ДПФ.

Keywords: digital watermark, DCT, DFT, DWT, SVD.

Введение

Сегодня вся информация доступна в электронном виде в Интернете. Доступность данных позволяет пользователям обмениваться и получать доступ ко всем файлам и информации в цифровой форме, что нарушает закон об авторском праве. Цифровые водяные знаки позволяют добавлять видимые или невидимые логотипы на цифровой контент для подтверждения подлинности. Цифровые водяные знаки могут выполнять различные задачи, такие как защита авторских прав, снятие отпечатков пальцев, аутентификация изображений и контента, защита от несанкционированного доступа и многие другие [1]. Алгоритмы встраивания цифровых водяных знаков должен поддерживать качество исходного изображения, а также должены встраивать цифровой водяной знак таким образом, чтобы изображение с ЦВЗ было устойчиво к различным атакам, например таким как гауссовский шум, сжатие JPEG или атаки поворота [2]. Водяные знаки можно встраивать в любой текст, изображение, аудио или видео. В этой статье будет рассмотрены методы встраивания ЦВЗ в изображения.

Водяные знаки могут быть встроены в пространственную или частотную области изображения. Наибольшей популярностью обладают частотные методы, так как обладают большей надежностью. Есть различные частотные методы разложения изображения, такие как дискретное косинусное преобразование (ДКП), дискретное вейвлет преобразование (ДВП), дискретное преобразование Фурье (ДПФ), избыточное дискретное вейвлет преобразование (ИДВП) и многие другие. Исследователи использовали эти методы для преобразования изображений в различные области. У каждого из этих методов есть свои достоинства и недостатки. В пространственной области для встраивания

используются младшие значащие биты (LSB) изображений, но они не устойчивы к различной обработке изображений, например, к таким атакам, как поворот, обрезка, сжатие JPEG и геометрические атаки. Поэтому большинство исследователей используют частотную область для встраивания.

В разделе 1.1 описана процедура нанесения водяных знаков, а в разделе 1.2 показаны ее характеристики. В разделе 1.3 рассмотрены различные методы преобразования изображения, выделены основные преимущества и недостатки.

1 Процедура нанесения водяных знаков

Цифровые водяные знаки позволяют скрывать важную информацию в исходном изображении, аудио, тексте или видео, которые служат контейнером для встраивания. При маркировании контента цифровыми водяными знаками, задействованы два процесса. Первый процесс называется встраиванием, второй – извлечением. Встраивание выполняется непосредственно владельцем контента, чтобы добавить право собственности на контент, а извлечение производится на принимающей стороне для подтверждения прав собственности. Эти процессы противоположны друг другу, но также связаны между собой, так как встраивание должно выполняться таким образом, чтобы извлекать информацию могли только авторизованные пользователи. Рассмотрим эти процессы поподробнее.

Этап 1. Встраивание водяного знака: при встраивании, ЦВЗ сначала вставляется в исходное изображение-контейнер C с использованием некоторого алгоритма и сгенерированного ключа, который также используется во время извлечения. Далее изображение со встроенным ЦВЗ будет доступно для пользователей. На маркированное изображение могут быть применены различные атаки обработки изображений, а также такие, которые полностью меняют изображение, содержащее водяной знак WC на WC′. В этом случае наложенный шум может быть рассчитан путем нахождения разницы между маркированным изображением WC и изображением, из которого извлекли водяной знак W', с использованием различных метрик измерения, таких как NC, BER, CC. На рисунке 1 изображена процедура встраивания.

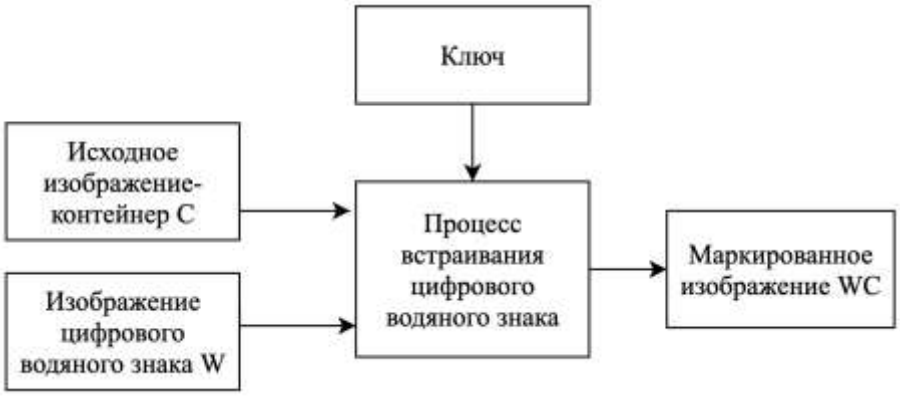


Рисунок 1 - Процесс встраивания ЦВЗ

Этап 2. Извлечение водяных знаков: извлечение основано на процессе встраивания и является функцией, зависящей от маркированного, оригинального изображений и ключа [3]. Полный процесс извлечения водяного знака показан на рис. 2, который включает ключ, алгоритм извлечения и маркированное изображение. В некоторых случаях может также понадобиться исходное изображение.



Рисунок 2 - Процесс извлечения водяного знака

Процесс извлечения водяных знаков бывает трех типов.

1. Неслепой подход: во время извлечения требуется оригинальное изображение ЦВЗ, а также изображение-контейнер.

2. Полуслепой подход: при извлечении не требуется исходного изображения-контейнера, но необходим ключ, используемый для встраивания, исходное изображение ЦВЗ и маркированное изображение.

3. Слепой подход: слепой подход извлекает изображение ЦВЗ только на основе WC и ключа, и не требует изображения-контейнера C или исходного изображения ЦВЗ. Этот подход более безопасен, чем другие, потому что в этом случае получатель не имеет никакой информации об исходных данных.

2 Характеристики водяных знаков

Алгоритмы встраивания ЦВЗ должны обладать необходимыми характеристиками (рисунок 3), такими как:

1. **Надежность.** Надежность проверяет, насколько устойчивы ЦВЗ при воздействии различных типов атак. Эта характеристика используется для сопоставления исходного и извлеченного ЦВЗ. Чем больше сходства между ними, тем надежнее будет схема. ЦВЗ называется надежным, если остается неизменным до и после применения атак. Одним из наиболее часто используемых параметров измерения устойчивости является нормализованная корреляция (NC), которая определяет соотношение между извлеченным и исходным водяным знаком. Значение коэффициента NC находится между 0 и 1, чем больше значение, близкое к 1, тем выше его надежность. Если $W = W'$, то схема является надежной и извлеченный водяной знак (W') равен исходному (W).

2. **Незаметность.** Незаметность определяет сходство между исходным и маркированным изображениями [4]. ЦВЗ бывают двух типов: видимые, которые используются в качестве логотипов и невидимые, которые защищают права на контент. Пользователи не должны иметь возможность просматривать невидимый ЦВЗ, встроенный в изображения. Эта характеристика показывает невидимость содержания ЦВЗ в маркированном изображении. Одна из основных проблем ЦВЗ - найти баланс между незаметностью и надежностью, поскольку эти две характеристики противоположны друг другу. Увеличение значения одной уменьшает другую, поэтому поиск компромисса между ними является сложной задачей.

3. **Безопасность.** Одной из основных характеристик ЦВЗ является безопасность, которая заключается в поддержании целостности и

конфиденциальности водяного знака против различных атак, совершаемых некоторыми неавторизованными лицами. Таким образом, безопасность обеспечивает защиту маркированного изображения от несанкционированного обнаружения, изменения или внедрения данных. Преобразование Арнольда — это один из методов, обеспечивающих безопасность данных путем добавления секретного ключа к маркированному изображению. Также могут использоваться и другие алгоритмы шифрования, например метод шифрования DES (стандарт шифрования данных).

4. **Емкость.** Емкость определяет, какой объем информации может быть встроен в изображение-контейнер. Изображение должно выдерживать нагрузку данных ЦВЗ или, другими словами, емкость определяет объем информации, которую может вместить конкретный носитель данных. Увеличение объема данных ЦВЗ в изображении-контейнер ухудшит его незаметность и снизит устойчивость к различным атакам. Поэтому должен быть баланс между емкостью, надежностью и незаметностью [5].

5. **Прозрачность.** После процесса встраивания, ЦВЗ не должен влиять на качество исходного изображения, кроме некоторых изменений его контрастности или яркости изображения-контейнера. Некоторые исследователи использовали свойство зрительной системы человека HVS (Human Visual System) [6] при внедрении водяных знаков. Характеристика HVS в схеме водяных знаков используется для определения подходящей области, которая не оказывает значительного эффекта искажения на исходное изображение.

6. **Вычислительные затраты.** Алгоритм, который используется для встраивания водяного знака, не должен быть сложным, так как это увеличивает вычислительные затраты. «Вычислительные затраты» — это стоимость или время, затрачиваемое алгоритмом на вычисление изображения с водяным знаком и на извлечение встроенного водяного знака. Стоимость внедрения и извлечения водяного знака должна соответствовать потребностям владельца изображения. Чем сложнее алгоритм, тем больше будет его стоимость с точки зрения времени, необходимого для запуска этого алгоритма.

7. **Уровень ложноположительных результатов.** Уровень ложноположительных результатов (ЛПР) подразумевает обнаружение водяного знака на маркированном изображении, даже если оно не содержит ЦВЗ [7]. Некоторые исследователи использовали метод SVD (разложение по сингулярным значениям) для встраивания водяного знака, но этот метод не обеспечивает устранение проблемы ложного срабатывания, поэтому используются гибридные методы в сочетании с SVD.



Рисунок 3 – Характеристики цифровых водяных знаков

3 Типы водяных знаков

Существуют различные классификации ЦВЗ, например, по способам встраивания и извлечения. Рассмотрим один из вариантов классификации методов стеганографии для изображений. На рисунке 4 представлена схема классификации.



Рисунок 4 – Классификация методов встраивания скрытых сообщений

По способу внедрения ЦВЗ существующие методы можно разделить на следующие группы [8]:

- линейные, основанные на линейной модификации изображения;
- нелинейные, использующие векторное или скалярное квантование;
- другие (в том числе использующие фрактальные преобразования).

По области встраивания скрытых данных существующие методы можно разделить на две группы:

- пространственные, основанные на встраивании бит ЦВЗ в результате изменений яркостных или цветовых составляющих изображения;
- спектральные, основанные на декомпозиции маркируемых областей изображения.

Рассмотрим методы, классифицируемые по области встраивания скрытых данных.

1. Пространственные, основанные на встраивании бит ЦВЗ в результате изменений яркостных или цветовых составляющих изображения. Этот метод прост в реализации, но информацию, встроенную в значение пикселя, могут легко

обнаружить злоумышленники. Водяные знаки, встроенные с помощью этой схемы, обеспечивают большую незаметность по сравнению с надежностью, так как эти схемы открыты для различных типов атак. К преимуществам данного метода следует отнести способность скрыть большую емкость данных. Рассмотрим некоторые методы, в которых для нанесения водяных знаков используется пространственная область изображений:

- LSB (наименьший значащий бит): это один из простейших методов встраивания в пространственную область, с помощью которого изображение преобразуется в 8-битную плоскость, а 8-й бит LSB используется для встраивания водяного знака, так как он несет незначительную информацию и имеет меньшее влияние на качество изображения. Одно из преимуществ использования метода LSB является то, что если размер водяного знака очень мал, то в исходное изображение можно добавить несколько водяных знаков, так что, если некоторые из водяных знаков будут потеряны из-за воздействия атак, оставшиеся могут помочь в защите авторских прав на контент. Этот метод менее устойчив к различным атакам, таких как вращение, отсечение, медианная фильтрация и фильтрация среднего значения для изображения с водяными знаками.

- Метод на основе корреляции: вместо того, чтобы внедрять водяной знак в изображение-контейнер, ЦВЗ преобразуется в некоторую псевдослучайную шумовую последовательность (PNS), а затем на нее умножается вес, и взвешенная PNS добавляется в изображение обложки, используя следующие уравнение:

$$CW(i,j) = C(i,j) + k * W'(i,j), \quad (4)$$

где $CW(i,j)$ – изображение со встроенным ЦВЗ в области i,j, $C(i,j)$ - исходное изображение обложки в области i,j,k - вес или коэффициент прироста. Здесь значение k определяет его надежность и незаметность, увеличение значения k увеличивает надежность, но снижает его незаметность, и наоборот.

- Аддитивный метод: в аддитивном методе к изображению добавляется псевдослучайный шум на основе интенсивности пикселя [9]. Этот шум

добавляется к исходному изображению с помощью некоторого ключа, который будет использоваться во время его извлечения для обнаружения водяного знака.

2. Спектральные, основанные на декомпозиции маркируемых областей изображения. В этом случае ЦВЗ встраивается в частотное преобразование основного изображения, что делает его более надежным, чем в методах пространственной области. Основным недостатком таких методов является вычислительная сложность. ДКП, ДВП, ДПФ — это некоторые из методов, используемых для преобразования изображения в частотную область. Рассмотрим наиболее популярные из них:

- **Дискретное косинусное преобразование (ДКП):** ДКП используется для преобразования изображения из пространственной области в частотную область путем преобразования его в сумму серий косинусоидальных волн на различных частотах. ДКП может быть выполнен в различных измерениях, таких как 1D, 2D и 3D, в случае изображений 2D ДКП выполняется для преобразования его в косинусный ряд. Преобразование ДКП может применяться к полному изображению или путем разделения изображения на различные блоки определенного размера [10]. Изображение преобразуется в различные полосы, а затем в эти полосы встраивается водяной знак. Выбор диапазона выполняется на основе его информационного содержания, чтобы можно было достичь устойчивости к различным шумовым атакам. Если для внедрения водяного знака выбран высокочастотный коэффициент, то фильтр может удалить его, фильтруя высокочастотные коэффициенты, поэтому, в качестве мест внедрения для водяного знака выбираются компоненты средней частоты, что делает его более надежным, чем метод пространственной области, выбор областей внедрения является одной из основных проблем техники ДКП. ДКП — это наиболее часто применяемое линейное ортогональное преобразование в цифровой обработке сигналов [11]. ДКП применяется в обработке изображений, сжатии, нанесении водяных знаков и т. д. [12]. 1D ДКП и 2D ДКП представлены с помощью формул 5 и 6.

1D-ДКП вычисляется по формуле:

$$f(i) = F(u) \qquad (5)$$

2D-ДКП задается как:

$$F(u,v) = \alpha(u)\alpha(v)\sum_{i=0}^{M-1}\sum_{j=0}^{M-1} f(i,j)\cos\frac{(2i+1)u\pi}{2M}\cos\frac{(2j+1)v\pi}{2M} \qquad (6)$$

где $u, v = 0,1,2 \dots M-1, M$ – размер последовательности, $f(i,j)$ - изображение в пространственной области, $F(u,v)$ – изображение в частотной области.

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{M}}, & u = 0 \\ \frac{2}{\sqrt{M}}, & u \neq 0 \end{cases} \qquad (7)$$

Обратный ДКП задается как,

$$f(i,j) = \sum_{i=0}^{M-1}\sum_{j=0}^{M-1} \alpha(u)\alpha(v)F(u,v)\cos\frac{(2i+1)u\pi}{2M}\cos\frac{(2j+1)v\pi}{2M} \qquad (8)$$

- **Дискретное преобразование Фурье (ДПФ):** преобразование Фурье раскладывает изображение на две составляющие, называемые амплитудой и фазой. Встраивание ЦВЗ выполняется в компоненты фазовой модуляции. ДПФ используется для преобразования изображения в 4 поддиапазона HL, LH, HH и низкочастотную составляющую LL [13]. Вычисления выполняются с использованием быстрого преобразования Фурье (БПФ). Одним из свойств ДПФ является инвариантность преобразования. Преимущество использования ДПФ, заключается в том, что он имеет меньший визуальный эффект и устойчив к шумовым атакам. ДПФ вычисляется по формуле:

$$F(u,v) = \frac{1}{M*N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} f(i,j)e^{-2\pi(\frac{ui}{M}+\frac{vj}{N})j} \qquad (9)$$

- **Дискретное вейвлет-преобразование (ДВП):** ДВП — это быстрый и простой подход к преобразованию, который переводит изображение из пространственной области в спектральную. ДВП разбивает изображение на иерархии с помощью математических инструментов [14]. Это преобразование основано на вейвлет функциях. Термин вейвлет подразумевает компоненты с разными масштабами. Таким образом, он предоставляет детали изображения как в частотной, так и в пространственной области. ДВП раскладывает изображение на высокочастотные и низкочастотные коэффициенты. Высокочастотные компоненты содержат мелкие детали, которые отвечают за четкость и резкость изображения, в то время как низкочастотные коэффициенты содержат основную информацию сигнала, поэтому дальнейшее разложение выполняется для низкочастотных компонентов. Этот метод преобразует изображение в различные поддиапазоны, называемые LL, LH, HL и HH, где LL представляет собой поддиапазон низкочастотных коэффициентов, HL – высоконизкочастотные, LH – низковысокочастотные, а HH – высокочастотные коэффициенты изображения. Существуют различные масштабы, используемые для ДВП, такие как 1D, 2D, 3D, которые преобразуют изображение в различные уровни поддиапазонов.

ДПФ и ДКП представляют сигнал либо в пространственную область, либо в частотную область, в то время как ДВП может представлять сигнал, как и в пространственной, так и в частотной области. ДВП используется в JPEG2000. Основная концепция ДПФ - сегментировать изображение на различные блоки, а затем скрывать данные в этих блоках. Большинство исследователей использовали ДВП для преобразования основного изображения на различные поддиапазоны, а затем выбирали любой подходящий диапазон для встраивания. Для встраивания выбираются в основном высокочастотные компоненты, чтобы обеспечить незаметность, но они не устойчивы к атакам, поскольку могут быть отфильтрованы различными фильтрами. Одна из основных проблем ДВП заключается в том, что имеется проблема инвариантности сдвига, которая приводит к понижающей дискретизации, поэтому многие исследователи

использовали избыточное ДВП, которое эту устраняет проблему, а также увеличивает емкость для встраивания водяных знаков.

- Разложение по сингулярным значениям (SVD): SVD — это эффективный метод работы с матрицами, который используется для обработки различных типов изображений. При применении SVD к изображению, образуются 3 матрицы [11]: A, U и A^T, в которых матрица U называется диагональной матрицей, а U и V - ортогональные матрицы. Этот метод используется во многих областях, таких как сжатие, обработка и маркирование изображений. Разложение по сингулярным значениям матрицы A представлено в формуле 10. Большинство исследователей использовали диагональные компоненты матрицы U для встраивания, поскольку в ней содержится основная часть информации изображения, но также известно, что страдает от проблемы ложного срабатывания. Одним из решений проблемы ложного срабатывания является встраивание водяного знака в основной компонент (A * S), поскольку основной компонент имеет уникальную функцию и может использоваться для устранения проблемы с ложным срабатыванием.

$$A = USV^T, \qquad (10)$$

$$A = \begin{bmatrix} U_{1,1}\ U_{1,2} \dots U_{1,n} \\ U_{2,1}\ U_{2,2} \dots U_{2,n} \\ \dots \\ U_{n,1}\ U_{n,2} \dots U_{n,n} \end{bmatrix} \begin{bmatrix} \sigma_{1,1}\ 0\ 0\ 0 \\ 0\ \sigma_{2,2}\ 0\ 0 \\ \dots \\ 0\ 0\ 0\ \sigma_{n,n} \end{bmatrix} \begin{bmatrix} V_{1,1}\ V_{1,2} \dots V_{1,n} \\ V_{2,1}\ V_{2,2} \dots V_{2,n} \\ \dots \\ V_{n,1}\ V_{n,2} \dots V_{n,n} \end{bmatrix}, \qquad (11)$$

где U и V - ортонормированные матрицы, S - диагональная матрица, состоящая из квадратов собственных значений матрицы A в порядке убывания.

Заключение

Концепция цифровых водяных знаков дает пользователям свободу делится своим контентом в Интернете с другими пользователями, сохраняя при этом его подлинность. Цифровые водяные знаки обеспечивают защиту авторских прав различного типа контента, такого как аудио, видео или изображения. Водяные

знаки могут выполняться в пространственно-частотной области. В пространственной области бит водяного знака непосредственно внедряется в пиксели изображения-контейнера. Наименьший значащий бит (LSB), метод на основе корреляции — это некоторые из методов, используемых при нанесении водяных знаков в пространственной области. Простота вычисления являются главным преимуществом таких методов. Но эти методы небезопасны, а также сильно ухудшают качество изображения обложки, поэтому чаще используют частотное разложение. В частотной области биты водяных знаков разбросаны по всему изображению, поэтому злоумышленнику трудно обнаружить изображение водяного знака. ДКП, ДВП, ДПФ и SVD – методы, которые используются при частотном разложении. В этой статье содержится описание методов разложения изображения. Некоторые обеспечивают только незаметность, а другие - и то, и другое - и незаметность, и надежность. В настоящее время в области водяных знаков используется ряд методов машинного обучения и глубокого обучения, чтобы улучшить баланс между надежностью и незаметностью и сделать алгоритм эффективным по времени.

В будущем работа может быть расширена для других типов данных, используемых для встраивания водяных знаков, таких как аудио или видео.

Литература

1. Nasr A., Ahmed S., Roslizah A.,Wan A., Wan A., Rahman. A state-of-the-art in techniques of text digital watermarking: challenges and limitations // J. Comput. Sci. 2016. P. 62–80.
2. Zear A., Singh A., Pardeep Kumar. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimedia Tools Application. 2016.
3. Agarwal N., Singh A., Singh P. Survey of robust and imperceptible watermarking // Multimedia Tools Application Springer. 2019. P. 1–31.
4. Ingemar M.L.M., Cox J., Bloom J.A., Fridrich J., Kalker T. Digital watermarking and steganography // Morgan Kaufmann Publishers. 2008.

5. Mohammad L.A., Zeki A., Chebil J., Gunawan T. Properties of digital image watermarking // Proceedings - 2013 IEEE 9th International Colloquium on Signal Processing and its Applications. 2013. P. 235–240.
6. Qingtang Su. Color Image watermarking Algorithms and Technologies // Berlin; Boston: De Gruyter; [Beijing]: Tsinghua University Press. 2017.
7. Nematollahi, Ali M., Vorakulpipat, Chalee, Rosales, Gamboa H. Digital watermarking techniques and trend // Springer Singapore. 2017.
8. Matsui K., Tanaka K. Video-steganography: How To secret Embed A Signature In A Picture // IMA intellectual properly project proceeding. 1994. P. 187-205.
9. Pradhan C., Saxena V., Bisoi A. Non blind digital watermarking technique using DCT and cross chaos map // International conference on Communications, Devices and Intelligent Systems (CODIS) IEEE. 2012. P. 274–277
10. Parah S., Sheikh J., Loan N., Bhat G. Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing // Digital signal Process Elsevier. 2016. P. 1–25.
11. Xu H., Kang X., Wang Y., Wang Y. Exploring robust and blind watermarking approach of colour images in DWT-DCT-SVD domain for copyright protection // Inderscience Int. J Electronic Security and Digital Forensics. 2018. P. 79–96.
12. Moosazadeh M., Gholamhossein Ekbatanifard. An improved robust image watermarking method using DCT and YCoCg-R Color Space // International Journal for Light and Electron Optics. 2017. P. 1–32.
13. Kansal M., Singh G., Kranthi B. DWT, DCT and SVD based Digital Image Watermarking // IEEE International Conference on Computing Sciences. 2012. P. 77–81.
14. Hong W., Hang M. Robust Digital Watermarking Scheme for Copy Right // Protection IEEE Trans. Signal Process l2. 2006. P. 1–8.