Алексей Н. Шниперов[1], Валерий А. Мельников[2]
ФГАОУ ВО «Сибирский федеральный университет»,
пр–кт Свободный, 79, Красноярск, 660041, Россия
[1]e-mail: ashniperov@sfu-kras.ru, https://orcid.org/0000-0003-4231-9805
[2]e-mail: MelnikoffVA@yandex.ru, https://orcid.org/0000-0001-9671-2755

ИСПОЛЬЗОВАНИЕ ПОЛЯРНЫХ ГАРМОНИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ПРИ РАЗРАБОТКЕ МЕТОДОВ МАРКИРОВАНИЯ ИЗОБРАЖЕНИЙ РОБАСТНЫМ ЦИФРОВЫМ ВОДЯНЫМ ЗНАКОМ

DOI: http://dx.doi.org/10.26583/bit.2021.4.07

Аннотация. Необходимость разработки методов маркирования изображений стойким невидимым цифровым водяным знаком остается актуальной до сих пор. Это обуславливается тем, что существующие методы маркирования зачастую либо не обладают достаточной стойкостью к атакам, либо требуют значительных вычислительных затрат, либо подвержены накоплению погрешности при вычислении – так называемой вычислительной неустойчивости. В данной работе предлагается использование полярных гармонических преобразований в качестве базиса разработки стеганографического метода маркирования полноцветных изображений невидимым цифровым водяным знаком (ЦВЗ), устойчивым к различным воздействиям на изображение. В статье предлагается сравнительная оценка устойчивости цифрового водяного знака, внедренного в частотную область изображения различными методами. Предлагается метод маркирования изображения водяным знаком, включая алгоритмы встраивания и извлечения водяного знака, а также предлагаются варианты многократного маркирования: многократное встраивание и извлечение по правилу большинства, многократное встраивание и извлечение по правилу бóльшего подобия, встраивание и извлечение фрагментов ЦВЗ. Кроме того, в работе приводятся экспериментальные результаты с оценкой характеристик метода, а именно: устойчивости к атакам, скорости работы для фиксированного размера области, максимального объема встраиваемой информации, проводилась посредством применения атак, использующихся в программе StirMark Benchmark 4. Предлагаемый в работе метод маркирования изображений оказывается устойчивым ко многим геометрическим атакам, JPEG-сжатию и иным атакам, обладает приемлемой скоростью встраивания водяного знака и не обладает вычислительной неустойчивостью. Разработанный метод может использоваться для маркирования растровых изображений формата JPEG с целью защиты авторских прав.

Ключевые слова: стеганография, цифровой водяной знак, полярные гармонические преобразования, защита авторских прав, маркирование изображений.
Для цитирования: ШНИПЕРОВ, Алексей Н.; МЕЛЬНИКОВ, Валерий А. ИСПОЛЬЗОВАНИЕ ПОЛЯРНЫХ ГАРМОНИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ПРИ РАЗРАБОТКЕ МЕТОДОВ МАРКИРОВАНИЯ ИЗОБРАЖЕНИЙ РОБАСТНЫМ ЦИФРОВЫМ ВОДЯНЫМ ЗНАКОМ. Безопасность информационных технологий, [S.l.], т. 28, № 4, с. 90–103, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1379. DOI: http://dx.doi.org/10.26583/bit.2021.4.07.

Alexey N. Shniperov[1], Valeriy A. Melnikov[2]
Siberian federal university,
79 Svobodny prospekt, Krasnoyarsk, 660041, Russia
[1]e-mail: ashniperov@sfu-kras.ru, https://orcid.org/0000-0003-4231-9805
[2]e-mail: MelnikoffVA@yandex.ru, https://orcid.org/0000-0001-9671-2755

The use of polar harmonic transformations in the development of methods for robust image watermarking

DOI: http://dx.doi.org/10.26583/bit.2021.4.07

Abstract. The need for developing a robust image watermarking method remains relevant. This is caused by the fact that existing watermarking methods are either not robust enough to various types of attacks on

images, or computationally complex, or they are subject to the so-called numerical instability, i.e., accumulation of errors. This paper proposes the use of polar harmonic transformations as the basis of the method for image watermarking, including algorithms for embedding and extracting a watermark, and methods for multiple marking are proposed: multiple embedding and extracting by majority rule, multiple embedding and extracting according to the rule of greater similarity, embedding and extracting fragments of a watermark. The performance characteristics, such as robustness to various attacks, embedding and extraction time for a fixed area size, and maximum size of watermark, are measured using attacks implemented in StirMark BenchMark 4. The proposed method has been proven to be robust to many types of geometric attacks, JPEG-compression and other attacks, to have a high embedding and extraction rate, and to be numerically stable. The proposed method can be used to watermark JPEG images for copyright protection.
Keywords: steganography, digital watermark, polar harmonic transformations, intellectual property protection, image watermarking.
For citation: SHNIPEROV, Alexey N.; MELNIKOV, Valeriy A. The use of polar harmonic transformations in the development of methods for robust image watermarking. IT Security (Russia), [S.l.], v. 28, n. 4, p. 90–103, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1379. DOI:http://dx.doi.org/10.26583/bit.2021.4.07.

Введение

С развитием информационных технологий все большую актуальность приобретает задача защиты авторского права. Это обуславливается тем, что объекты авторского права в цифровой форме легко распространяются среди пользователей посредством копирования, кроме того, сравнительно легко могут быть модифицированы. При этом достаточно часто возникает ситуация, в которой автору или правообладателю того или иного цифрового ресурса необходимо подтвердить (заявить) свои права на него, что бывает сделать весьма проблематично.

Для частичного решения проблемы сохранения авторских прав в отношении цифровых изображений традиционно применяют видимые цифровые водяные знаки, которые наносятся поверх изображения. Такой подход традиционно применяется в различных фотобанках, при этом сам видимый водяной знак снимается в момент покупки изображения. Однако дальнейшая судьба этого цифрового изображения остаётся уже не известной для автора (правообладателя). При этом использоваться изображение может в нарушение лицензионных ограничений.

Таким образом продолжает иметь место быть научно-техническая задача по организации маркирования изображения цифровым водяным знаком (ЦВЗ), который сохранялся бы в изображении на всём его жизненном цикле. При этом по данным, хранящимся в ЦВЗ, можно было бы идентифицировать автора или правообладателя на случай спорного использования цифрового ресурса, а сам ЦВЗ было бы проблематично удалить из изображения без его значительных визуальных искажений.

В данной работе предлагается стеганографический метод маркирования полноцветных растровых изображений формата JPEG робастным цифровым водяным знаком, устойчивым к преднамеренным или случайным внешним воздействиям на промаркированное им изображение. Предлагаемый в работе метод отличается от своих аналогов тем, что имеет приемлемую вычислительную сложность, является устойчивым к геометрическим атакам, а также общим атакам цифровой обработки изображений. При этом предлагаемый метод маркирования является вычислительно устойчивым.

1. Подходы к маркированию изображений цифровым водяным знаком

Цифровые водяные знаки представляют из себя встраиваемые в защищаемый объект специальные визуально не различимые метки, сравнительно небольшой

информационной ёмкости. В зависимости от области встраивания ЦВЗ методы маркирования принято разделять на:

– пространственные, которые непосредственно оперируют значениями интенсивности цветов изображения, а также прозрачностью пикселей и не требуют сложных вычислений для встраивания ЦВЗ;

– частотные, которые основываются на преобразованиях в частотной области изображения;

– основанные на моментах изображения.

Ввиду низкой стойкости пространственных методов маркирования [1], а рамках данной работы они не будут рассматриваться.

Частотные методы маркирования основываются на преобразованиях в частотной области изображения (дискретное косинусное и вейвлет-преобразование – далее ДКП и ДВП, дискретное преобразование Фурье – ДПФ, преобразование Адамара). Наиболее часто используемыми в стеганографических целях, в том числе для внедрения в изображение ЦВЗ, являются ДВП И ДКП. К данной группе методов относятся методы Кокса [2] и Барни [3] на основе ДКП, Полицака [4] на основе ДПФ, Прамилы [5] на основе ДВП и метод Фальковски [6] на основе преобразования Адамара.

Другая группа методов позволяет встраивать ЦВЗ в моменты изображения. Такие алгоритмы основываются на преобразованиях, известных как моменты Чебышева, Лежандра, Цернике, а также на ортогональных моментах Фурье-Меллина, дескрипторах Фурье-Меллина, радиальных гармонических моментах Фурье и др. [7]. Среди недостатков таких методов выделяют проблему вычислительной устойчивости (numerical stability), а также проблему скорости вычисления радиального полинома (вычислительная сложность). И если, как в случае моментов Цернике, вторая проблема решается с помощью алгоритмов быстрого вычисления моментов [8], то проблемы вычислительной устойчивости решены лишь частично [9, 10].

Момент – скалярная величина, характеризующая особенности некоторой функции (в случае цифровой обработки сигналов – функции изображения) [11].

Момент является ортогональным, если формирующий его базис является ортогональным базисом. Среди достоинств ортогональных моментов выделяется простота восстановления исходного изображения по моментам:

$$f(x,y)=\sum_{p,q} M_{pq}\cdot V_{pq}(x,y),$$

где $V_{pq}(x,y)$ – базис момента, M_{pq} – момент изображения порядка p с числом повторений q.

В первую очередь, методы встраивания ЦВЗ на основе моментов призваны решить проблему устойчивости к геометрическим атакам. Решение заключается в выделении областей, инвариантных к определенным геометрическим преобразованиям, с дальнейшей маркировкой изображения на основе значений моментов в этих областях [12]. Из данной группы нами ранее предлагался метод на основе моментов Цернике [13], а также был рассмотрен метод на основе радиальных моментов Фурье (далее – РМФ) [7].

Существует еще одна группа методов, которые основаны на полярных гармонических преобразованиях (ПГП) [14] – это ортогональный момент изображения, значения которого инвариантны к повороту и масштабированию изображения [15]. По сравнению с моментами Цернике методы на основе ПГП не требуют сложных вычислений, а также показывают лучшие результаты в тестах вычислительной устойчивости [16].

Свойство ортогональности ПГП делает возможным восстановление исходного изображения по формуле:

$$\hat{f}(r,\theta)=\sum_{-n_{\max}}^{n_{\max}}\sum_{-m_{\max}}^{m_{\max}}A_{nm}V_{nm}(r,\theta).$$

Из данной группы методов нами были рассмотрены методы Ли [15], Хосни [17], и метод Яна [18]. Необходимо отметить, что, как и в случае с моментами, существуют быстрые алгоритмы вычисления ПГП [19].

Проанализировав экспериментальные результаты, полученные авторами работ, мы составили сравнительную таблицу показателей стойкости ЦВЗ, внедренного различными методами, к различным атакам (табл. 1). Можно отметить, что лучшую устойчивость имеют группы методов на основе полярных гармонических преобразований (полярных комплексных экспоненциальных преобразований, полярных косинусных преобразований и полярных синусных преобразований), а также методы на основе моментов (Цернике и радиальных моментов Фурье).

Таблица 1. Сравнительная оценка устойчивости ЦВЗ, внедренного различными методами («+» – устойчив, «–» – не устойчив, «?» – частичная устойчивость/нет оценки устойчивости)

Метод	Устойчивость к атаке							
	Поворот	Масштабирование	Смещение	Обрезка	Шум	Сжатие	Фильтрация	Вычислительная устойчивость
Метод Кокса (ДКП)	?	+	?	+	+	+	–	?
Метод Барни (ДКП)	?	+	?	+	+	+	+	?
Метод Полицака (ДПФ)	+	+	–	+	+	+	?	?
Метод Прамилы (ДВП)	+	+	+	?	?	+	?	?
Метод Фальковски (преобразование Адамара)	+	+	?	+	+	+	?	?
Метод на основе моментов Цернике	+	+	?	+	+	+	?	–
Метод Вана (РМФ)	+	+	?	?	+	+	+	+
Метод Ли (ПГП)	+	+	?	–	+	+	+	+
Метод Хосни (ПГП)	+	+	?	?	+	+	+	+
Метод Яна (ПГП)	+	+	?	–	+	+	+	+

Необходимо отметить, что ключевыми конкурентными преимуществами использования полярных гармонических преобразований в качестве базиса метода маркирования являются сравнительно низкая вычислительная сложность, вычислительная устойчивость и резистивность к различным атакам фильтрации.

В данной работе предлагается ***метод маркирования изображений цифровым водяным знаком на основе полярных гармонических преобразований***, включающий в себя различные подходы к внедрению ЦВЗ в изображение с оценкой их эффективности.

2. Описание метода маркирования изображений цифровым водяным знаком

Цифровой водяной знак представляет собой некоторое бинарное изображение $B_{img}=\left\{B_{img}(i,j)\in\{0,1\},0\le i<P,0\le j<Q\right\}$, размером $P\times Q$, встраивание происходит в

синий канал полноцветного изображения H размера $N \times N$. Предварительно, водяной знак B с помощью преобразования Арнольда отображается в одномерную последовательность бит $B(l) = \left\{ B_{img}\left(i, j\right) \in \{0,1\}, 0 \le i < P, 0 \le j < Q, l = i \times Q + j \right\}$.

Далее происходит вычисление ПГП и выбор, подлежащих модификации, моментов изображения $M = \left\{ M_{p_1 q_1}, M_{p_2 q_2}, ..., M_{p_l q_l} \right\}$ из множества $S = \left\{ M_{pq}, p \le p_{\max}, q \le q_{\max}, q > 0 \right\}$, где p_i, q_i – порядок и число повторений момента, представляющие собой параметры функции момента, $p_{\max}$ – максимальный порядок вычисляемых моментов, $q_{\max}$ – максимальное число повторений момента.

В общем виде вычисления моментов осуществляется следующим образом:

$$M_{pq} = \lambda \sum_r \sum_\theta \hat{f}\left(r, \theta\right) V_{pq}\left(r, \theta\right), \tag{2.1}$$

где $\hat{f}\left(r, \theta\right)$ – функция изображения в полярных координатах, $V_{pq}\left(r, \theta\right) = R_{pq}\left(r\right) e^{jq\theta}$ – базисная функция момента, $R_{pq}\left(r\right)$ – радиальная функция, p, q – порядок и число повторений момента, λ – коэффициент, используемый при вычислении момента изображения (зависит от вида преобразования).

Принципиальное отличие при использовании того или иного ПГП заключается в виде радиальной функции. Так, в табл. 2 приведены выражения для вычисления радиальной составляющей различных моментов ПГП.

Таблица 2. Радиальные функции вычисления моментов

Момент	Радиальная функция момента $R_{pq}\left(r\right)$	Значение λ
полярные комплексные экспоненциальные преобразования	$e^{j2\pi pr^2}$	$\frac{1}{\pi}$
полярные косинусные преобразования	$\cos\left(\pi p r^2\right)$	$\begin{cases} \frac{1}{\pi}, p = 0 \\ \frac{2}{\pi}, p \ne 0 \end{cases}$
полярные синусные преобразования	$\sin\left(\pi p r^2\right)$	$\begin{cases} \frac{1}{\pi}, p = 0 \\ \frac{2}{\pi}, p \ne 0 \end{cases}$
радиальные гармонические моменты Фурье	$\begin{cases} \frac{1}{\sqrt{r}}, p = 0 \\ \sqrt{\frac{2}{r}} \cos\left(\pi p r\right), p - \textit{четное} \\ \sqrt{\frac{2}{r}} \sin\left(\pi\left(p+1\right) r\right), p - \textit{нечетное} \end{cases}$	$\frac{p+1}{\pi}$

Правило квантования моментов $M_{p_i q_i}$ для внедрения бита b_i описывается следующими выражениями [21]:

$$\left|M'_{p_i q_i}\right| = \left\lfloor \frac{\left|M_{p_i q_i}\right| - d_i\left(b_i\right)}{\Delta} \right\rfloor \Delta + d_i\left(b_i\right), \tag{2.2}$$

$$M'_{p_i q_i} = \frac{\left|M'_{p_i q_i}\right|}{\left|M_{p_i q_i}\right|} M_{p_i q_i}, \tag{2.3}$$

где $\lfloor ... \rfloor$ – оператор округления, Δ – шаг квантования, от которого зависит соотношение видимости и устойчивости ЦВЗ, $d = \left\{d_1\left(b\right), ..., d_n\left(b\right)\right\}$ – функция дизеринга.

Внедрение значений моментов в исходное изображение происходит достаточно распространённым способом, аналогичным использованным в работах [7, 13, 14, 17]:

$$f_{rem}\left(r,\theta\right) = \sum_p \sum_q \left(M'_{p,q} - M_{p,q}\right) \cdot V_{p,q}\left(r,\theta\right), \tag{2.4}$$

$$f'\left(r,\theta\right) = f\left(r,\theta\right) + f_{rem}\left(r,\theta\right). \tag{2.5}$$

где $f_{rem}\left(r,\theta\right)$ – псевдо-изображение ЦВЗ, восстановленное из разницы моментов, $f'\left(r,\theta\right)$ – изображение, представляющее собой область встраивания в полярных координатах, заменяет соответствующую область в исходном изображении, $M_{p,q}, M'_{p,q}$ – соответственно изначальные и модифицированные моменты.

Алгоритм извлечения состоит из вычисления на основании моментов области пары значений:

$$M^1_{p_i,q_i} = \left\lfloor \frac{\left|M_{p_i q_i}\right| - d_i\left(1\right)}{\Delta} \right\rfloor \Delta + d_i\left(1\right), \tag{2.6}$$

$$M^0_{p_i,q_i} = \left\lfloor \frac{\left|M_{p_i q_i}\right| - d_i\left(0\right)}{\Delta} \right\rfloor \Delta + d_i\left(0\right) \tag{2.7}$$

и определении последовательности ЦВЗ следующим образом:

$$B' = \left\{ b_i \middle| \min\left(\left(M^0_{p,q} - M_{p,q}\right)^2, \left(M^1_{p,q} - M_{p,q}\right)^2\right) = \left(M^i_{p,q} - M_{p,q}\right)^2 \right\}. \tag{2.8}$$

2.1. Алгоритм внедрения ЦВЗ в изображение

Метод маркирования изображения ЦВЗ предполагает внедрение его псевдо-изображения в исходное изображение определенным способом. Общая структурная схема процесса внедрения ЦВЗ в изображение представлена на рис. 1.

Алгоритм внедрения ЦВЗ в изображение включает в себя следующие шаги.

Шаг 1. Цифровой водяной знак представляется в виде бинарной последовательности $\overline{B} = \left\{b_i\right\}$.

Шаг 2 (выбор области встраивания). Для внедрения ЦВЗ в пространственную область изображения необходимо определить область внедрения. Это может быть

окрестность особой точки, выбранной посредством того или иного детектора, например, детектора Ши-Томаси. Однако эксперименты показали, что в некоторых случаях выбор произвольной области встраивания, осуществляемый псевдослучайным образом, приводит к сохранению большей доли бит ЦВЗ при извлечении, чем при выборе особой точки посредством детектора.

Шаг 3 (вычисление моментов и их выбор). Выполняется вычисление моментов изображения по выражению (2.1). В качестве радиальной функции выбирается одна из возможных (табл. 2). Необходимо отметить, что максимальный порядок вычисляемых моментов $p_{\max}$ не влияет значительно на качество извлекаемого ЦВЗ, однако влияет на то, какова максимальная длина водяного знака. Поскольку один бит информации встраивается в один момент, значение $p_{\max}$ должно быть достаточным, чтобы уместить в области встраивания весь ЦВЗ.

Шаг 4 (квантование моментов). Выполняется квантование моментов изображения по формулам (2.2) и (2.3). Необходимо отметить, что данном шаге выбирается множество значений функции дизеринга $d = \{d_1(b),...,d_n(b)\}$. Конкретное значение функции дизеринга позволяет внедрить в исходное изображение тот или иной бит ЦВЗ. Так, дизеринг при внедрении единичного бита зависит от дизеринга при внедрении нулевого бита следующим образом:

$$d_i(1) = d_i(0) + \Delta / 2,$$

где Δ – шаг квантования, определяющий соотношение надежности и видимости. В качестве нулевого значения функции дизеринга использовалось значение $d_i(0) = \Delta / 32$.

Шаг квантования Δ определяет соотношение надежности и видимости. Использованное значение по умолчанию $\Delta = 2$, однако, в случае моментов, которые при таком значении демонстрируют отрицательные результаты, данное значение может выбираться адаптивно.

Шаг 5 (формирование псевдо-изображения ЦВЗ). Выполняется формирование псевдо-изображения, восстановленного из разницы моментов согласно выражению (2.4).

Шаг 6 (внедрение ЦВЗ). Выполняется **с**ложение в пространственной области полученного псевдо-изображения и оригинального изображения согласно выражению (2.5).

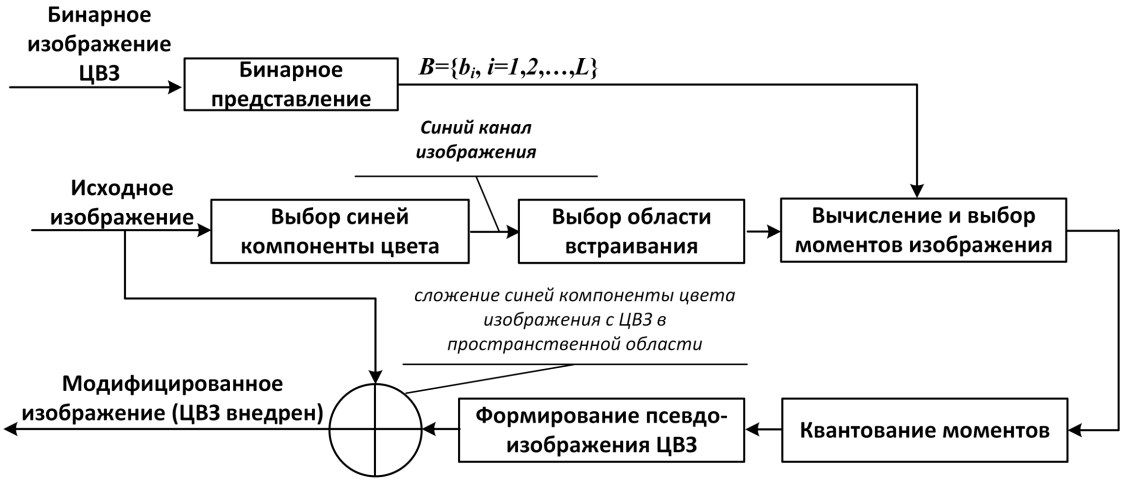

Рис. 1. Общая структурная схема внедрения ЦВЗ в изображение
Fig. 1. General structural diagram of the image watermarking

2.2. Алгоритм извлечения ЦВЗ из изображения

Общая структурная схема процесса внедрения ЦВЗ в изображение представлена на рис. 2.

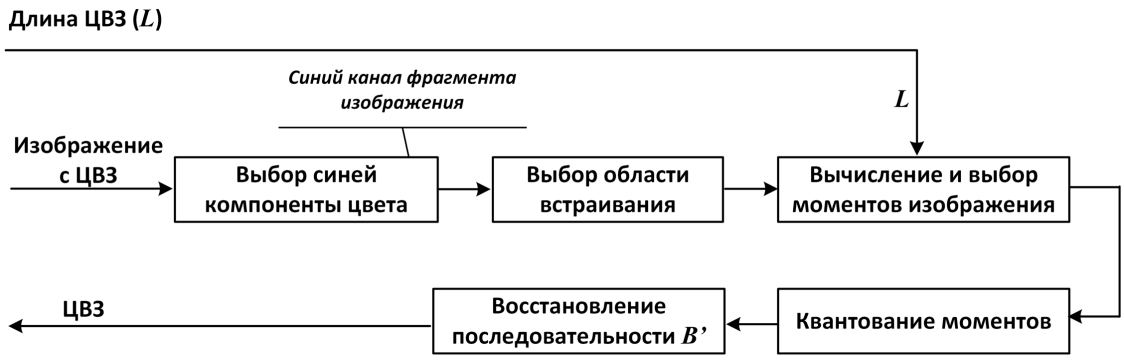

Рис. 2. Общая структурная схема извлечения ЦВЗ из изображения
Fig. 2. General structural diagram of extracting a digital watermark from an image

Алгоритм извлечения ЦВЗ из изображения включает в себя следующие шаги.

Шаг 1 (выбор области встраивания). Для извлечения ЦВЗ из изображения необходимо определить область внедрения. Способ определения области извлечения должен быть аналогичным тому, который использовался на этапе внедрения ЦВЗ.

Шаг 2 (вычисление моментов и их выбор). Выполняется вычисление моментов изображения по выражению (2.1). Для извлечения ЦВЗ необязательно наличие на принимающей стороне эталонного ЦВЗ, однако необходимо знание длины L встроенного ЦВЗ, т.к. необходимо знать максимальный порядок момента $p_{\max}$.

Шаг 3 (квантование моментов). Выполняется квантование моментов изображения по выражениям (2.6) и (2.7).

Шаг 4 (восстановление бит ЦВЗ). В соответствии с (2.8) выполняется восстановление бит ЦВЗ, используя значения моментов, вычисленные на предыдущим шаге. Следует отметить, что, хотя и предполагается равенство области встраивания и области извлечения, в общем случае это равенство необязательно будет выполняться. Например, при высоких значениях шага квантования, когда на изображении появляются видимые артефакты, встроенный ЦВЗ не удается извлечь в том числе и потому, что функция определения особых точек уже не рассматривает прежнюю особую точку как таковую. Именно поэтому следует тщательно выбирать порядок значения и само значение шага квантования Δ.

3. Оценка робастности внедренного цифрового водяного знака

Для получения оценочных характеристик предлагаемого метода маркирования была выполнена его программная реализация на языке программирования Python с использованием библиотек OpenCV, numpy.

Оценка стойкости предлагаемого метода маркирования изображения производилось с помощью программы StirMark Benchmark 4, автоматизирующей процесс внесения различных атак из базы имеющихся:

- внесение Гауссова шума с варьируемым уровнем шума (NOISE);
- JPEG-сжатие с варьируемой степенью сжатия (JPEG);
- медианная фильтрация с различными размерами фильтров (MEDIAN);
- атака замены подобными блоками пикселей (SS);

– удаление строк и столбцов пикселей (RML);
– обрезка изображения (CROP);
– масштабирование (RESC);
– поворот (ROT);
– поворот и обрезка (ROTCROP);
– поворот и масштабирование (ROTSCALE);
– аффинные преобразования с варьируемыми параметрами a,b,c,d,e (AFFINE), определяемые формулой:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} d \\ e \end{pmatrix};$$

– две версии атаки случайных искажений (RNDIST и LATESTRNDIST);
– атака увеличения яркости изображения (PSNR);
– сверточный фильтр (CONV).

Работа с StirMark Benchmark 4 производилась следующим образом: сначала происходило внедрение ЦВЗ в исходное изображение, после чего это изображение подавалось на вход программе StirMark для его модификации (искажение тем или иным способом). Все искаженные изображения подавались на вход модуля извлечения ЦВЗ, разработанного программного прототипа, реализующего предлагаемый метод маркирования. Далее извлеченные ЦВЗ сравнивались с исходным эталоном, на основании чего подсчитывалось количество ошибок.

Результаты тестов устойчивости к атакам разработанных вариантов метода приведены в табл. 3. Устойчивость определялась посредством вычисления отношения числа корректно извлекаемых ЦВЗ, полученных при разных значениях параметра атаки, к общему числу попыток извлечения.

Таблица 3. Устойчивость метода к атакам в зависимости от используемого момента изображения

Момент, используемый в методе	AFFINE, %	CONV, %	CROP, %	JPEG, %	LATESTRNDIST, %	MEDIAN, %	NOISE, %	PSNR, %	RESC, %	RML, %	RNDIST, %	ROT, %	ROTCROP, %	ROTSCALE, %	SS, %
ПСП	75	0	0	69	100	0	0	100	0	98	100	100	100	95	100
ПКП	84	0	0	77	100	0	0	100	17	98	13	99	100	100	100
РМФ	59	0	0	48	94	0	0	100	17	95	75	97	100	90	100
ПКЭП	81	0	0	77	0	0	0	100	17	98	100	99	100	100	100

Таким образом, можно сделать вывод, что применение полярного синусного преобразования даёт наибольшую стойкость среди полярных гармонических преобразований.

4. Подходы к маркированию изображения цифровым водяным знаком

С целью увеличения стойкости разработанного метода оценивались различные подходы внедрения ЦВЗ в изображение, а именно проверялись следующие варианты многократного маркирования:

– многократное встраивание и извлечение по правилу большинства;
– многократное встраивание и извлечение по правилу наибóльшего подобия;
– встраивание и извлечение фрагментов ЦВЗ.

Многократное встраивание и извлечение по правилу большинства основывается на подсчете значений бит для всех позиций в извлеченных из нескольких областей водяных знаках, после чего на данную позицию в итоговом ЦВЗ устанавливается то значение, которое в извлеченных знаках встречается в данной позиции чаще всего. Результаты показателя *BER* (*Bit error rate*), который показал метод маркирования при использовании такого способа извлечения, приведены в табл. 4.

Таблица 4. Среднее значение BER для маркирования по правилу большинства

Корректирующий код	$\overline{BER}$, при $L=8$	$\overline{BER}$ при $L=15$	$\overline{BER}$ при $L=21$
–	0.048	0.121	0.179
Сверточный код	0.173	0.187	0.238

Извлечение по правилу наибольшего подобия основывается на сравнении восстановленных из изображения водяных знаков с эталонным значением ЦВЗ. На основании сравнения выбирается тот водяной знак, который обладает минимальным расстоянием Хемминга. Результаты, которые показал метод маркирования при использовании такого способа извлечения, приведены в табл. 5.

Таблица 5. Среднее значение BER для маркирования по правилу наибольшего подобия

Корректирующий код	$\overline{BER}$ при $L=8$	$\overline{BER}$ при $L=15$	$\overline{BER}$ при $L=21$
–	0	0.005	0.032
Сверточный код	0	0.041	0.09

Многократное маркирование фрагментами ЦВЗ основывается на том, что ЦВЗ разделяется на несколько частей, после чего каждый фрагмент встраивается в свою область. Максимальное число фрагментов – 5. Результаты оценки применимости данного подхода приведены в табл. 6.

Таблица 6. Среднее значение BER для маркирования фрагментами ЦВЗ

Корректирующий код	$\overline{BER}$ при $L=8$	$\overline{BER}$ при $L=15$	$\overline{BER}$ при $L=21$
–	0.125	0.11	0.13
Сверточный код	0.106	0.11	0.14

Кроме того, проверялась возможность применения корректирующих кодов, однако приемлемые результаты продемонстрировали лишь сверточные коды. Применялся сверточный код с порождающими полиномами $G_1(X)=1+X^2$ и $G_2(X)=1+X+X^2$. Также были оценены традиционный код Хемминга (7,4) и код Рида-Соломона с параметрами $N-K=8$, исправляющий 4 ошибки в блоке.

5. Оценка характеристик разработанного метода маркирования изображений

5.1. Оценка стойкости оптимизированного метода к атакам

Оценка стойкости ЦВЗ, внедренным различными подходами к маркированию изображения, представлена в табл. 7. Длина ЦВЗ была выбрана средняя из тех, с которыми ранее оценивалась работоспособность метода, а именно – 15 байт. В данной таблице приведены средние по трем изображениям показатели устойчивости к атакам. Показатель устойчивости здесь – это среднее для трех изображения значение отношения количества корректно восстановленных бит к общему числу бит ЦВЗ для разных параметров атак в процентном представлении. Лучшие показатели наблюдаются при использовании многократного маркированию по принципу наибольшего подобия.

Таблица 7. Показатель стойкости вариантов оптимизации метода

Атака	Многократное маркирование по правилу большинства	Многократное маркирование по правилу наибольшего подобия	Маркирование фрагментами	Маркирование фрагментами с использованием сверточного кода	Маркирование без использования корректирующих кодов	Маркирование с использованием сверточного кода
AFFINE	44.2	78.6	21.1	21.6	30	31.9
CONV	0	0	0	1.1	0	0
CROP	19.5	16.3	0.9	1.5	2.2	2.2
JPEG	55.9	63.7	36.7	34.3	44.6	45.9
LATEST RNDIST	9.4	26.1	6.7	2.8	3.9	5.6
MEDIAN	6.1	23.3	3.3	3.9	15.6	16.7
NOISE	17	18.1	17	16.7	14.4	14.4
PSNR	100	100	93.3	96.6	84.6	86.7
RESC	18.5	7	0.7	1.9	3.7	1.5
RML	77.3	78	43.8	52.7	23.3	24.4
RNDIST	30.6	41.7	5.6	11.1	51.1	19.4
ROT	58.1	93.7	24.2	24.8	37.8	40
ROT CROP	51.8	92.2	16	16.4	30.2	28.7
ROT SCALE	48.7	85.1	15.6	19.8	13.1	12.4
SS	31.1	51.9	28.9	30.4	24.4	25.9
$\Sigma/15$	36.7	51.7	20.9	22.4	25.3	23.7

5.2. Оценка максимальной длины цифрового водяного знака

Для оценки максимальной длины ЦВЗ, при которой ещё возможно его корректное извлечение, было использовано 10 тестовых изображений. В данном случае атаки не применялись.

Результаты оценки приведены в табл. 8. В четных столбцах приведено общее количество некорректно восстановленных бит для всех 10 тестовых изображений. В результате можно заметить, что значительное увеличение количества ошибок начинается примерно с длины ЦВЗ L=21.Таким образом, рекомендуется использовать ЦВЗ длины $L \le 20$.

Таблица 8. Количество ошибочно восстанавливаемых бит в зависимости от длины ЦВЗ

Длина L	Количество ошибочно восстановленных бит	Длина L	Количество ошибочно восстановленных бит
5	2	18	3
6	2	19	4
7	1	20	1
8	3	21	5
9	4	22	6
10	5	23	8
11	1	24	7
12	4	25	7
13	5	26	11
14	3	27	6
15	4	28	8
16	2	29	11
17	4	30	10

Заключение

В данной работе предлагается метод маркирования полноцветных изображений невидимым цифровым водяным знаком на основе полярных гармонических преобразований, а также сопутствующие алгоритмы. Данный метод и алгоритмы были реализованы в виде программного прототипа, посредством которого были получены следующие оценочные характеристики метода, а именно:

– применение полярных синусных преобразований в качестве базиса метода маркирования даёт его наибольшую эффективность, в сравнении с иными полярными гармоническими преобразованиями;

– использование многократного маркирования ЦВЗ по принципу наибольшего подобия, повышает устойчивость метода к атакам. Однако такой подход требует наличия эталонного ЦВЗ на принимающей стороне. Несколько худшие результаты демонстрирует маркирование фрагментами ЦВЗ. Многократное маркирование по принципу большинства имеет худшие показатели, что объясняется тем, что из всего множества используемых областей встраивания оказывается больше областей, из которых ЦВЗ извлекается некорректно, в результате восстановление оригинального ЦВЗ зачастую невозможно;

– метод оказывается устойчив к атакам поворота, аффинным преобразованиям, JPEG-сжатию с сохранением качества до 40–50%, разновидностям атаки замены подобными блоками, атаки удаления строк и столбцов пикселей. В некоторых случаях метод демонстрирует устойчивость к атакам случайных искажений;

– среднее время внедрения и извлечения равно 4 с при однократном маркировании и 6 с при многократном маркировании (типовой персональный компьютер со средними техническими характеристиками);

– рекомендуемая максимальная длина ЦВЗ L_{max}=20, однако в случае некоторых изображений можно использовать и бóльшие ЦВЗ. Бóльшая часть ошибок, наблюдаемых в данной серии экспериментов, приходилась на одни и те же 1–2 изображения из общей базы 26 изображений. Это объясняется тем, что в случае этих изображений детектором выбирались непригодные области встраивания.

СПИСОК ЛИТЕРАТУРЫ:

1. Батура В.А. Методы цифрового маркирования неподвижных изображений // Электронный научно-технический журнал «Инженерный вестник», 77-48211/612552, № 08 август 2013. Москва, ФГБОУ ВПО «Московский государственный технический университет им. Н.Э. Баумана». С. 583–590. URL: http://www.ainjournal.ru/doc/612552.html (дата обращения: 26.10.2021).
2. Cox I., Kilian J., Leighton T., Shamoon T. Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing. Vol. 6, no. 12. 1997. P. 1673–1687. DOI: https://10.1109/83.650120.
3. Barni M., Bartolini F., Cappellini V., Piva A. A DCT-domain system for robust image watermarking. Signal Processing 66. 1998. P. 357–372. DOI: https://doi.org/10.1016/S0165-1684(98)00015-2.
4. Poljicak A., Mandic L., Agic D. Discrete Fourier transform-based watermarking method with an optimal implementation radius. Journal of Electronic Imaging 20(3). 2011. P. 1–8. DOI: http://dx.doi.org/10.1117/1.3609010.
5. Pramila A., Keskinarkaus A., Seppanen T. Multiple Domain Watermarking for Print-Scan and JPEG Resilient Data Hiding. IWDW' 07 Proceedings of the 6th International Workshop on Digital Watermarking. 2008. P. 279–293. DOI: http://dx.doi.org/10.1007/978-3-540-92238-4_22.
6. Falkowski B., Lim L. Image Watermarking Using the Complex Hadamard Transform. ISCAS 2000, IEEE International Symposium on Circuits and Systems. 2000. P. 573–576. DOI: https://doi.org/10.1109/ISCAS.2000.858816.
7. Wang C., Wang X., Xia Z. Geometrically invariant image watermarking based on fast Radical Harmonic Fourier Moments. Signal Processing: Image Communication 45. 2016. P. 10–23. DOI: https://doi.org/10.1109/ACCESS.2019.2935174.
8. Singh C., Ranade S.K. An Effective Image Watermarking System for High Embedding Capacity. International Conference on Recent Advances and Future Trends in Information Techonology (iRAFIT2012), Proceedings published in International Journal of Computer Applications (IJCA) 2012. P. 22–28. URL:https://www.academia.edu/31980739/An_Effective_Image_Watermarking_System_for_High_Embedding_Capacity (дата обращения: 26.10.2021).
9. Papakostas G.A., Boutalis Y.S., Papaodysseus C.N., Fragoulis D.K. Numerical stability of fast computation algorithms of Zernike moments. Applied Mathematics and Computation 195. 2008. P. 326–345. DOI: http://dx.doi.org/10.1016/j.amc.2007.04.110.
10. Singh C., Walia E. Algorithms for fast computation of Zernike moments and their numerical stability. Image and Vision Computing 29. 2011. P. 251–259. DOI: http://dx.doi.org/10.1016/j.imavis.2010.10.003.
11. Flusser J., Suk T., Zitova B. Moments and Moment Invariants in Pattern Recognition. John Wiley & Sons, Ltd. 2009. DOI: http://dx.doi.org/10.1002/9780470684757.
12. Никитина О.Ю. О методе цифровых водяных знаков на основе особенностей изображения и моментов Цернике // «Искусственный интеллект» 3'2008. С. 339–347. URL: http://dspace.nbuv.gov.ua /bitstream/handle/123456789/6977/13-Nikitina.pdf?sequence=1 (дата обращения: 26.10.2021).
13. Шниперов А.Н., Сосновский М.С., Шипулин П.М. Робастный метод маркирования изображений цифровым водяным знаком, основанный на ортогональных моментах Цернике // «Информационные технологии», М.: Новые технологии, 2019. Т. 25, № 7. С. 405–413. DOI: http://dx.doi.org/10.17587/it.25.405-413.
14. Yap P., Jiang X., Kot A. Two-Dimensional Polar Harmonic Transforms for Invariant Image Representation. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 32, no. 7. 2010. P. 1259–1270. DOI: http://dx.doi.org/10.1109/TPAMI.2009.119.
15. Li L., Li S., Abraham A., Pan J. Geometrically invariant image watermarking using Polar Harmonic Transforms. Information Sciences 199. 2012. P. 1–19. DOI: http://dx.doi.org/10.1016/j.ins.2012.02.062.
16. Tsougenis E.D., Papakostas G.A. Should We Consider Adaptivity in Moment-based Image Watermarking? Science Gate Publishing. 2014. P. 253–274. DOI: http://dx.doi.org/10.15579/gcsr.vol1.ch11.
17. Hosny K., Darwish M. Invariant image watermarking using accurate Polar Harmonic Transforms. Computers and Electrical Engineering. 2017. P. 1–19. DOI: http://dx.doi.org/10.1016/j.compeleceng.2017.05.015.
18. C. Wang, X. Wang, X. Chen, C. Zhang Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping. Multimedia Tools and Applications 76(24). 2017. DOI: https://link.springer.com/article/10.1007/s11042-016-4130-7.
19. Singh C., Kaur A. Fast computation of polar harmonic transforms. J Real-Time Image Proc. 2012. DOI: http://dx.doi.org/10.1007/s11554-012-0252-y.
20. Singh C., Pooja S., Upneja R. On Image Reconstruction, Numerical Stability, and Invariance of Orthogonal Radial Moments and Radial Harmonic Transforms. ISSN 1054-6618, Pattern Recognition and Image Analysis. Vol. 21, no. 4. 2011. P. 663–676. DOI: http://dx.doi.org/10.1134/S1054661811040158.
21. Singh C., Walia E. Algorithms for fast computation of Zernike moments and their numerical stability. Image and Vision Computing 29. 2011. P. 251–259. DOI: http://dx.doi.org/10.1016/j.imavis.2010.10.003.

REFERENCES:

[1] Batura V.A. Methods of digital marking of still images. Electronic Publishing «Engineering Bulletin», 77-48211/612552, № 08 August 2013. Moscow, Bauman Moscow State Technical University. P. 583–590. URL: http://www.ainjournal.ru/doc/612552.html (accessed: 26.10.2021) (in Russian).

[2] Cox I., Kilian J., Leighton T., Shamoon T. Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing. Vol. 6, no. 12. 1997. P. 1673–1687. DOI: https://10.1109/83.650120.

[3] Barni M., Bartolini F., Cappellini V., Piva A. A DCT-domain system for robust image watermarking. Signal Processing 66. 1998. P. 357–372. DOI: https://doi.org/10.1016/S0165-1684(98)00015-2.

[4] Poljicak A., Mandic L., Agic D. Discrete Fourier transform-based watermarking method with an optimal implementation radius. Journal of Electronic Imaging 20(3). 2011. P. 1–8. DOI: http://dx.doi.org/10.1117/1.3609010.

[5] Pramila A., Keskinarkaus A., Seppanen T. Multiple Domain Watermarking for Print-Scan and JPEG Resilient Data Hiding. IWDW' 07 Proceedings of the 6th International Workshop on Digital Watermarking. 2008. P. 279–293. DOI: http://dx.doi.org/10.1007/978-3-540-92238-4_22.

[6] Falkowski B., Lim L. Image Watermarking Using the Complex Hadamard Transform. ISCAS 2000, IEEE International Symposium on Circuits and Systems. 2000. P. 573–576. DOI: https://doi.org/10.1109/ISCAS.2000.858816.

[7] Wang C., Wang X., Xia Z. Geometrically invariant image watermarking based on fast Radical Harmonic Fourier Moments. Signal Processing: Image Communication 45. 2016. P. 10–23. DOI: https://doi.org/10.1109/ACCESS.2019.2935174.

[8] Singh C., Ranade S.K. An Effective Image Watermarking System for High Embedding Capacity. International Conference on Recent Advances and Future Trends in Information Techonology (iRAFIT2012), Proceedings published in International Journal of Computer Applications (IJCA) 2012. P. 22–28. URL:https://www.academia.edu/31980739/An_Effective_Image_Watermarking_System_for_High_Embedding_Capacity (accessed: 26.10.2021).

[9] Papakostas G.A., Boutalis Y.S., Papaodysseus C.N., Fragoulis D.K. Numerical stability of fast computation algorithms of Zernike moments. Applied Mathematics and Computation 195. 2008. P. 326–345. DOI: http://dx.doi.org/10.1016/j.amc.2007.04.110.

[10] Singh C., Walia E. Algorithms for fast computation of Zernike moments and their numerical stability. Image and Vision Computing 29. 2011. P. 251–259. DOI: http://dx.doi.org/10.1016/j.imavis.2010.10.003.

[11] Flusser J., Suk T., Zitova B. Moments and Moment Invariants in Pattern Recognition. John Wiley & Sons, Ltd. 2009. DOI: http://dx.doi.org/10.1002/9780470684757.

[12] Nikitina O.Yu. O metode cifrovyh vodyanyh znakov na osnove osobennostej izobrazheniya i momentov Cernike. «Artificial Intelligence Problems» 3'2008. P. 339–347. URL: http://dspace.nbuv.gov.ua /bitstream/handle/123456789/6977/13-Nikitina.pdf?sequence=1 (дата обращения: 26.10.2021) (in Russian).

[13] Shniperov A.N., Sosnovsky M.S., Shipulin P.M. A robust method for marking images with a digital watermark based on Zernike orthogonal moments. Information Technologies, Moscow: New Technologies, 2019. Vol. 25, no. 7. P. 405–413. DOI: http://dx.doi.org/10.17587/it.25.405-413 (in Russian).

[14] Yap P., Jiang X., Kot A. Two-Dimensional Polar Harmonic Transforms for Invariant Image Representation. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 32, no. 7. 2010. P. 1259–1270. DOI: http://dx.doi.org/10.1109/TPAMI.2009.119.

[15] Li L., Li S., Abraham A., Pan J. Geometrically invariant image watermarking using Polar Harmonic Transforms. Information Sciences 199. 2012. P. 1–19. DOI: http://dx.doi.org/10.1016/j.ins.2012.02.062.

[16] Tsougenis E.D., Papakostas G.A. Should We Consider Adaptivity in Moment-based Image Watermarking? Science Gate Publishing. 2014. P. 253–274. DOI: http://dx.doi.org/10.15579/gcsr.vol1.ch11.

[17] Hosny K., Darwish M. Invariant image watermarking using accurate Polar Harmonic Transforms. Computers and Electrical Engineering. 2017. P. 1–19. DOI: http://dx.doi.org/10.1016/j.compeleceng.2017.05.015.

[18] C. Wang, X. Wang, X. Chen, C. Zhang Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping. Multimedia Tools and Applications 76(24). 2017. DOI: https://link.springer.com/article/10.1007/s11042-016-4130-7.

[19] Singh C., Kaur A. Fast computation of polar harmonic transforms. J Real-Time Image Proc. 2012. DOI: http://dx.doi.org/10.1007/s11554-012-0252-y.

[20] Singh C., Pooja S., Upneja R. On Image Reconstruction, Numerical Stability, and Invariance of Orthogonal Radial Moments and Radial Harmonic Transforms. ISSN 1054-6618, Pattern Recognition and Image Analysis. Vol. 21, no. 4. 2011. P. 663–676. DOI: http://dx.doi.org/10.1134/S1054661811040158.

[21] Singh C., Walia E. Algorithms for fast computation of Zernike moments and their numerical stability. Image and Vision Computing 29. 2011. P. 251–259. DOI: http://dx.doi.org/10.1016/j.imavis.2010.10.003.

Поступила в редакцию – 21 июля 2021 г. Окончательный вариант – 26 ноября 2021 г.
Received – July 21, 2021. The final version – November 26, 2021.