14. *Mel'nikov A.K.* Metodika rascheta raspredeleniy veroyatnostey znacheniy statistik, blizkikh k ikh tochnym raspredeleniyam [Calculation methodology of approximate-to-exact distribution of statistics probabilities], *Obozrenie prikladnoy i promyshlennoy matematiki* [Review of applied and industrial mathematics], 2017, Vol. 24, Issue 5. Available at: http://tvp.ru/conferen/vsppmXVIII/kisso075.pdf (accessed 13 July 2018).
15. *Mel'nikov A.K.* Metodika rascheta raspredeleniya veroyatnostey znacheniy simmetrichnykh additivno razdelyaemykh statistik, priblizhennykh k ikh tochnomu raspredeleniyu [Processing complexity for exact probability distributions of symmetrical additively partitioned statistics and application area of limit distributions], *Nauchnyy vestnik NGTU* [Science bulletin of the Novosibirsk state technical university], 2018, No. 1 (70), pp. 153-166. ISBN 1814-1196. Doi: 10.17212/1814-1196-2018-1-153-166.
16. *Pearson K.* On the criterion that a given system of deviations from the probable in the case of a correlated system of variables in such that it can be reasonably supposed to have arisen from random sampling, *Philos. Mag. Ser. 5*, 1900, Vol. 50, No. 302, pp. 157-170.
17. *Neyman F., Pearson E.S.* On the use and interpretation of certain test criteria for purposes of statistical inference, *Biometrika*, 1928, Vol. 20-A, pp. 175-240, 264-299.
18. *Smith P.F., Rae D.S., Manderscheid R.W., Silbergeld S.* Exact and approximate distributions of the chi-squared statistic for equiprobability, *Commun. Statist*., 1979, B. 8 (2), No. 1, pp. 131-149.
19. *Matusita K.* Decision rules, based on the distanse, for problems of fit tu o samples, and estimation, *Ann. Math. Stat*., 1955, Vol. 26, pp. 631-640.
20. *Ronzhin A.F.* Asimptoticheskaya lokal'naya otnositel'naya effektivnost' (ALOE) kriteriev soglasiya [Asymptotic local relative efficiency (ALRE) of fitting criteria], *Tezisy dokladov Vsesoyuznoy konferentsii «Veroyatnostnye metody v diskretnoy matematike»* [Reports of All-USSR conference “Probabilistic methods in discrete mathematics”]. Petrozavodsk, 1983, pp. 70-71.

Статью рекомендовала к опубликованию д.т.н. А.В. Никитина.

Мельников Андрей Кимович – НТЦ ЗАО «ИнформИнвестГрупп»; e-mail: ak@iigroup.ru; 117587, Москва, Варшавское шоссе, д. 125, стр. 17; тел.: 84952870035; к. т. н.; доцент ВАК; г.н.с.

Melnikov Andrey Kimovitch – STC CLSC «InformInvestGroup»; e-mail: ak@iigroup.ru; 125, Varshavskoye road, building 17, Moscow, 117587, Russia; phone: +74952870035; cand. of eng. sc.; associate professor of SAC; chief research officer.

УДК 004.932 DOI 10.23683/2311-3103-2018-8-135-145

А.М. Абасова, Л.К. Бабенко

ЗАЩИТА АВТОРСКИХ ПРАВ НА ИЗОБРАЖЕНИЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МОРФОЛОГИЧЕСКОЙ ОБРАБОТКИ*

В настоящей статье рассматривается вопрос о внедрении цифровых водяных знаков в области изображения, которые наименее вероятно подвергнутся модификации и, следовательно, подходят для обеспечения эффективной защиты авторских прав, с учетом типа деструктивных воздействий, характерных при их нарушении. В качестве контейнера выступает цветное изображение, а в качестве цифрового водяного знака – текст, содержащий знак охраны авторских прав. Для внедрения выбираются блоки переднего плана, так как согласно проведенному исследованию именно они представляют ценность изображения, что особенно характерно для коммерческих фотографий. Поиск данных блоков для внедрения осуществляется с помощью маркирования с использованием методов математической морфологии. Также в статье на примере показана способность структурного элемента выполнять роль ключевой информации. Предложено использовать геометрический центр каждого найденного блока переднего плана для внедрения цифрового водяного

* Работа выполнена при поддержке гранта РФФИ № 18-07-01347.

знака как точку отсчета при его заполнении. Представлены результаты оценки способности корректного извлечения внедренного цифрового водяного знака согласно предложенного решения с использованием разработанной программы, результаты анализа эффективности разработанной программы, реализация и сравнение с существующими программными продуктами, используемыми для защиты авторских прав.

Стеганография; стегоконтейнер; цифровой водяной знак; морфологическая обработка изображений.

A.M. Abasova, L.K. Babenko

PROTECTION OF COPYRIGHT TO THE IMAGE WITH THE USE OF METHODS OF MORPHOLOGICAL PROCESSING

This article raises the issue of the introduction of digital watermarks in the image area, which are less likely modified and, therefore, are suitable for ensuring effective protection of copyright, taking into account the type of destructive effects that are characteristic of their violation. The container is a color image, as a digital watermark - a text containing a copyright protection symbol. For the implementation, foreground blocks are chosen, because according to the survey they represent the value of the image, which is especially characteristic for commercial photographs. The search for data blocks for implementation is carried out using marking using methods of mathematical morphology. Also in the article, the ability of a structural element to fulfill the role of key information has been demonstrated. It is proposed to use the geometric center of each found block of the foreground for the introduction of the digital watermark as a reference point when it is filled. The results of the evaluation of the ability to correctly extract an embedded digital watermark according to the proposed solution using the developed program, the results of the analysis of the effectiveness of the developed program and a comparison with existing software products used for copyright protection are presented

Steganography; stegocontainer; digital watermarkind; morphological image processing.

Введение. На сегодняшний день активно растет количество средств массовой информации, в том числе представленных в сети Интернет, а соответственно растет и количество наполняемого их контента. Цифровые изображения считаются достаточно уязвимыми объектами авторских прав, так как их легко скопировать и незаконно использовать, что влечет за собой финансовые потери для автора, откуда следует, что исследования в области обеспечения защиты авторских прав на цифровые изображения являются актуальными [1].

Предлагается для обеспечения защиты авторских прав на изображения использовать цифровые водяные знаки (далее – ЦВЗ) так как они обладают сравнительно невысокой стоимостью, в отличие от других технических методов, невидимы для злоумышленника и подходят при регистрации цифровых изображений, в отличие от организационных методов [2]. Анализ деструктивных воздействий на системы ЦВЗ, характерных при нарушении авторских прав показал, что, как правило, такие воздействия направлены на удаление или модификацию ЦВЗ (сжатие изображения, изменение яркости/контрастности и др.) или на блокирование корректной работы стегодетектора, в результате чего теряется возможность приема ЦВЗ (усечение изображения, перестановка пикселов и др.). Существующие методы внедрения ЦВЗ не всегда обеспечивают высокую устойчивость ЦВЗ к указанным деструктивным воздействиям с учетом обеспечения незаметности ЦВЗ и слепого извлечения ЦВЗ, поэтому целью работы является обеспечение эффективной защиты цифрового изображения, как объекта интеллектуальной собственности от угроз хищения. Принимая во внимание требования к системам ЦВЗ, и самим ЦВЗ [3] был сделан вывод, что одним из важных направлений для обеспечения целостности ЦВЗ является выбор такой области для его внедрения, которая наименее вероятно подвергнется модификации.

1. Существующие решения по определению областей для встраивания ЦВЗ. Один из подходов к решению данного вопроса предложен в работе [4] и заключается в разделении изображения на блоки фиксированного размера и встраивание в частотные области каждого блока по небольшой части ЦВЗ. Также в данном подходе предлагается использовать в качестве организационного метода защиты базу данных для устойчивости к таким деструктивным воздействиям, как повороты и масштабирование изображений. В базе данных помимо информационных сведений об изображении содержатся образцы ЦВЗ и ключи, с помощью которых осуществлялась защитная маркировка. Оценка стойкости встроенной информации показала, что ЦВЗ будет выявляться при удалении части изображения справа/снизу, автоуровню/автоконтрасту/автоцвету, частично детектироваться при клонировании фрагментов. В качестве недостатка можно выделить тот факт, что в общем случае частотные алгоритмы внедрения ЦВЗ являются вычислительно сложными, так как исходное изображение необходимо декомпозировать для встраивания в определенные спектральные области [5,6]. Более простым решением является предложенный в работе [7] частотный алгоритм, согласно которому ЦВЗ встраивается в центральную часть изображения, однако автором указано, что допустимо удаление только 25 % изображения для обеспечения обнаружения ЦВЗ. Следует отметить, что если брать во внимание художественную (в том числе профессиональную сьемку) то, как правило, автор старается придерживаться правила золотого сечения, которое не предусматривает располагать объект в центре [8].

В рамках анализа источников, описывающих цели использования изображения злоумышленником и методов обхода наличия ЦВЗ, был выявлен факт того, что злоумышленник оставляет нетронутыми объекты (или часть из объектов), которые находятся на переднем плане, так как именно они и представляют ценность изображения (особенно актуально для рекламных постеров, корреспондентских фото). Исходя из вышеизложенного, предлагается для внедрения ЦВЗ использовать пиксели изображения-контейнера, принадлежащие объектам переднего плана. К переднему плану относятся объекты, расположенные ближе к камере, чем объекты локального фона [9], то есть это множество ключевых объектов, расположенных в разных частях одного изображения (каждый объект – в конкретном выделенном фрагменте изображения).

Для распознавания объектов переднего плана на изображении используют сегментацию. В работе [10] описаны алгоритмы выделения объектов переднего плана (алгоритм случайного блуждания, Байесовский подход, алгоритм GrabCut и др.), но по причине высокой ресурсоемкости вычислительных операций алгоритмов, необходимости внесения со стороны пользователя понятийной информации в некоторых случаях (рисуя примерные границы объектов в виде линий, кривых и мазков на изображении), а также по причине обнаружения четких контуров объектов (для разных алгоритмов границы объектов могут отличаться) при выполнении сегментации (что позволит злоумышленнику легко обнаружить объект для внедрения ЦВЗ, зная алгоритм) предлагается использовать другой метод.

2. Предлагаемое решение для обеспечения защиты авторских прав на изображения. Для определения блоков переднего плана предлагается проводить автоматическое маркирование. Для маркировки блоков переднего плана используются морфологические операции, такие как замыкание (выполнение операций морфологической дилатации изображения с последующей морфологической эрозией изображения), размыкание (выполнение операций морфологической эрозии изображения с последующей морфологической дилатацией изображения) [11]. С помощью данных операций проводится анализ внутренней области объектов изображения, а также убираются из рассмотрения несущественные детали (темные/небольшие) на изображении. Морфологические операции больше подходят

для анализа форм объектов, чем стандартные линейные фильтры, поскольку последние иногда искажают основные геометрические формы изображения. Алгоритм работы и математическая схема были представлены автором в работе [12], а результаты проведенных испытаний на изображениях приведены в работе [13].

Необходимо отметить, что некоторые скрытые или закрытые объекты на изображении–контейнере не будут промаркированы. Данное свойство отражается на обработке подобных объектов изображения–контейнера с позиции сегментации, однако данные неявные объекты могут быть изъяты из рассмотрения, так как они не являются ключевыми элементами изображения–контейнера.

При реализации упомянутых выше морфологических функций используется структурный элемент (примитив). Структурный элемент представляет собой определенного размера матрицу, состоящую из нулей и единиц, где совокупность нулей определяет форму структурного элемента. В разработанном методе предлагается структурный элемент особой сложной формы использовать как стегоключ. Кроме того, в качестве ключевой информации можно использовать дополнительные критерии выбора объектов переднего плана, описанных автором в работе [14].

Так как в большинстве стегосистем заполнение бит изображения–контейнера осуществляется на основе линейных функций, либо последовательно, что влияет на возможность легкого стегоанализа со стороны злоумышленника и неустойчивость к деструктивным воздействиям, было предложено дополнительно использовать геометрический центр объекта (центроид) переднего плана как точку отсчета при внедрении ЦВЗ.

Геометрический центр объекта – это центр масс фигуры такой же формы как объект. Центр масс представляет собой точку, в которой можно зафиксировать всю массу объекта без преобразования его первого момента относительно какой-либо оси [15]. В нашем случае в двумерном пространстве изображения–контейнера первый момент относительно оси x вычисляется по формуле [16]:

$$\bar{x} \iint b(x, y)\, dx\, dy = \iint x b(x, y)\, dx\, dy, \quad (1)$$

а относительно оси y:

$$\bar{y} \iint b(x, y)\, dx\, dy = \iint y b(x, y)\, dx\, dy, \quad (2)$$

где $(\bar{x}, \bar{y})$ – координаты геометрического центра, $b(x, y)$ – плотность яркости изображения.

Интеграл в левой части приведенных соотношений – является площадью маркированного объекта переднего плана.

В табл. 1, 2 указаны координаты центроидов, рассчитанных в соответствии с приведенными соотношениями (1, 2) для маркированных объектов переднего плана (МБПП – маркированный блок переднего плана) для изображения, представленного на рис. 1, вычисленных по соответствующему примитиву.

Рис. 1. Исходное изображение-контейнер

Представленные данные подтверждают способность примитива быть стегоключом. Координаты пикселей, в которые будет производиться внедрение ЦВЗ, также будут зависеть от самого метода встраивания, так как есть методы, в которых для встраивания ЦВЗ недопустимо использование рядом находящихся пикселей.

Так, например, в методе Куттера-Джордана-Боссена встраивание бита s в синюю компоненту пикселя $p = (x, y)$ выполняется в результате изменения яркости. Встраивание выполняется согласно формуле [17]:

$$B'(p) = \begin{cases} B(p) + qI(p), & \text{если } s = 0 \\ B(p) - qI(p), & \text{если } s = 1 \end{cases} \quad (3)$$

где $B'(p)$ – модифицированное синее значение пикселя, q – энергия встраиваемого сигнала, причем чем больше его значение, тем сильнее заметность встраиваемых данных [18].

Таблица 1

Координаты центроидов для МБПП по структурным элементам диск 20 и 19 пикселей, ромб 20 и 19 пикселей

Коорд. Центроида	№ строки	№ столбца	№ строки	№ столбца	№ строки	№ столбца	№ строки	№ столбца
Примитив	«Диск 20»		«Диск 19»		«Ромб 20»		«Ромб 19»	
МБПП 1	375	35	375	34	375	34	375	34
МБПП 2	218	55	218	56	217	57	217	57
МБПП 3	129	123	128	123	123	129	123	129
МБПП 4	366	159	366	159	372	167	372	167
МБПП 5	191	255	106	222	104	223	104	222
МБПП 6	145	451	190	255	189	254	189	254
МБПП 7	270	460	145	450	100	368	98	365
МБПП 8			270	461	145	450	147	443
МБПП 9					269	463	269	463

Таблица 2

Координаты центроидов для МБПП по структурным элементам диск 10 пикселей и ромб 10 пикселей

Координаты центроидов	№ строки	№ столбца	№ строки	№ столбца
Примитив	«Диск 10»		«Ромб 10»	
Количество МБПП	15		17	
МБПП 1	378	24	335	5
МБПП 2	278	49	378	24
МБПП 3	215	59	278	49
МБПП 4	231	129	214	59
МБПП 5	124	140	231	128
МБПП 6	260	157	127	139
МБПП 7	372	170	259	157
МБПП 8	311	285	372	170
МБПП 9	99	217	311	284
МБПП 10	184	254	99	217

Окончание табл. 2

Координаты центроидов	№ строки	№ столбца	№ строки	№ столбца
Примитив	«Диск 10»		«Ромб 10»	
Количество МБПП	15		17	
МБПП 11	117	283	182	255
МБПП 12	177	370	117	283
МБПП 13	93	365	372	331
МБПП 14	141	445	177	370
МБПП 15	269	461	92	367
МБПП 16			141	446
МБПП 17			268	461

Так как на принимающей стороне нет оригинала изображения-контейнера, то нет возможности узнать однозначно, как изменилась яркость синего цвета. Поэтому для извлечения ЦВЗ предполагается возможное значение яркости синего цвета на основе значений яркости пикселей – соседей [19]:

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

где $\sigma = 1 \ldots 3$. Данный метод проиллюстрирован на рис. 2, при $\sigma = 3$.

Темный пиксель в центре с координатами (x, y) – это пиксель, яркость синего цвета которого необходимо предположить, опираясь на пиксели, которые обозначены более светлым цветом.

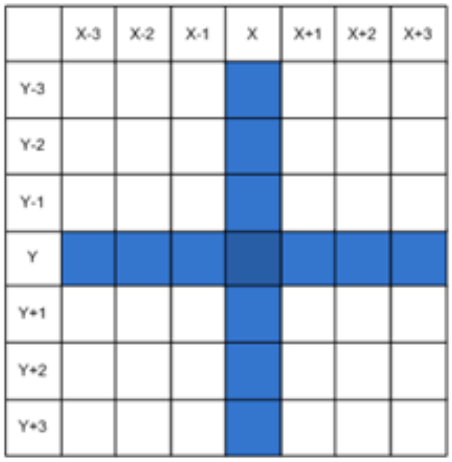

Рис. 2. Пример прогнозируемого извлечения ЦВЗ

Встраивание ЦВЗ будет осуществляться не во все синие компоненты пикселей изображения, сохраненного в цветовой модели RGB, а только в окружающие центроиды маркированных блоков переднего плана, способом, представленным на рис. 3, где $(10{,}10)$ – координаты центроида.

Основной идеей построения такой схемы встраивания информации является то, что процесс извлечения носит вероятностный характер, следовательно, нельзя производить изменения в пикселях которые будут использованы для прогнозирования яркости измененного пикселя в момент извлечения ЦВЗ.

Для извлечения встроенного ЦВЗ используется формула:

$$s_i = \begin{cases} 1, & \text{при } B^*_{x,y} > \overline{B_{x,y}}; \\ 0, & \text{при } B^*_{x,y} < \overline{B_{x,y}}. \end{cases} \quad (5)$$

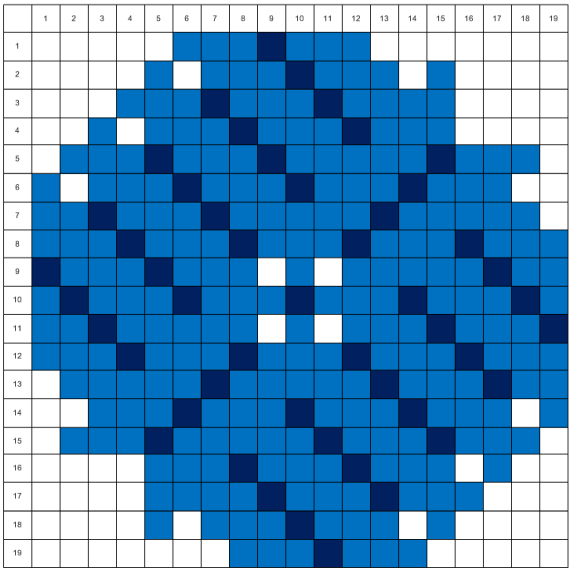

Рис. 3. Схема встраивания ЦВЗ

3. Оценка. Для оценки способности корректного извлечения внедренного ЦВЗ согласно предложенного решения, а также разработанных алгоритмов с применением корректирующего кода [2], который позволяет также осуществлять параллельную обработку данных [20], была разработана программа AStego, которая позволяет встраивать ЦВЗ, представленный в виде текста или набора символов в блоки переднего плана изображения – контейнера с применением метода Куттера-Джордана-Боссена. Были проведены эксперименты с использованием 100 различных цифровых изображений: текстурные, нетекстурные, монотонные, многоцветные; пейзажи, рекламные постеры, натюрморты, корреспондентские фото и др. Данный разброс типов изображения был обусловлен необходимостью проверить и оценить способность определения маркированных блоков переднего плана необходимого размера и количества, вероятность правильного извлечения при деструктивных воздействиях. В рамках данной статьи под эффективностью защиты цифрового изображения, как объекта интеллектуальной собственности будем понимать способность ЦВЗ противостоять деструктивным воздействиям.

Для анализа эффективности ΔQ были вычислены показатели эффективности Q двух существующих популярных решений по защите авторских прав Suresign и DropWaterMark по частным показателям, представленным табл. 3, и показатели разработанной программы, после чего была вычислена разница между их максимальными значениями.

$$Q = \frac{1}{n}\sum_{i=1}^{n} q_i, \quad (6)$$

где Q – эффективность метода, q_i – частная эффективность противодействия $i-$ому деструктивному воздействию.

Таблица 3

Результаты экспериментальных исследований

Программа / Деструктивное воздействие		Suresign		DropWaterMark		AStego	
		Частн.	Групп.	Частн.	Групп.	Частн.	Групп.
Изменение контрастности	+10%	1	1	1	1	1	1
	+50%	1		1		1	
	-10%	1		1		1	
	-50%	1		1		1	
Изменение яркости	+10%	1	1	1	1	1	0,99
	+50%	1		1		0,97	
	-10%	1		1		1	
	-20%	1		1		1	
Смена формата изображения на JPEG	качество 8	1	1	1	1	1	1
	качество 10	1		1		1	
	качество 12	1		1		1	
	качество 14	1		1		1	
Смена формата изображения	BMP	1	0,84	1	0,86	1	0,85
	TIFF	1		1		1	
	PNG	1		1		1	
	GIF	0,37		0,42		0,4	
Вычеркивание	5 строк шириной 5 пикс	0	0	0	0	1	1
	10 строк шириной 1 пикс	0		0		1	
	5 столбцов шириной 5 пикс	0		0		1	
	10 столбцов шириной 1 пикс	0		0		1	
Поворот изображения	на 1°	1	0,67	1	0,67	1	0,67
	на 50°	1		1		1	
	на 50,5°	0		0		0	
Сдвиг на 10%	по горизонтали	0	0	0	0	0,96	0,96
	по вертикали	0		0		0,96	
Перемещение части изображения	5%	0	0	0	0	0,98	0,97
	10%	0		0		0,95	
Замена изображения	10%	0	0	0	0	0,95	0,78
	50%	0		0		0,6	
Удаление	10 крайних пикселей	0	0	0	0	1	0,89
	50 крайних пикселей	0		0		1	
	10% изображения	0		0		0,95	
	50% изображения	0		0		0,6	

$Q_{Suresign} = 0{,}53;$

$Q_{DropWaterMark} = 0{,}53;$

$Q_{AStego} = 0{,}92;$

$Q_{\text{сущ}} = \max(Q_{Suresign}; Q_{DropWaterMark}) = 0{,}53$

$Q_{\text{разраб}} = Q_{AStego} = 0{,}92$

$\Delta Q = Q_{\text{разраб}} - Q_{\text{сущ}} = 0{,}39.$

Таким образом, эффективность разработанного метода заключалась в росте корректного извлечения ЦВЗ на 39% относительно существующих решений.

Вывод. Предложенное решение по внедрению ЦВЗ в значимые области цифрового изображения, отличающееся от известных, позволяет повысить его целостность при различных деструктивных воздействиях, с учетом обеспечения незаметности ЦВЗ и слепого извлечения ЦВЗ, а также преодолеть недостатки последовательного внедрения ЦВЗ в изображение.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Невская М.А., Тарасова Е.Н., Сухарев Е.Е.* Авторское право в издательском бизнесе и СМИ. – М.: Дашков и К, 2008. – 300 с.
2. *Абасова А.М., Бабенко Л.К.* Разработка алгоритма внедрения цифрового водяного знака на базе морфологической обработки изображения и модулярной арифметики для противодействия угрозам хищения объектов интеллектуальной собственности // Международный журнал прикладных и фундаментальных исследований. – 2018. – № 6. – С. 9-14.
3. *Грибунин В.Г., Костюков В.Е., Мартынов А.П., Николаев Д.Б., Фомченко В.Н.* Стеганографические системы. Атаки, пропускная способность каналов и оценка стойкости: учебно-методическое пособие / ред. В.Г. Грибунин. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2015. – 217 с.
4. *Белобокова Ю.А.* Модели и алгоритмы защитной маркировки для обеспечения аутентичности и целостности растровых изображений: автореф. дис. … канд. технич. наук (05.13.17). – М., 2014. – 19 с.
5. *Конахович, Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
6. *Cox I.J., Miller M., Bloom J., Fridrich J.* Digital watermarking and steganography. – San Francisco: Morgan Kaufmann Publishing, 2008. – 624 p.
7. *Terzija N.* Robust digital image watermarking algorithms for copyright protection: genehmigte dissertation. – Belgrad, 2006. – 161 p.
8. *Карпин А.* Фотография для начинающих. – Самиздат, 2012. – 239 с.
9. *Gupta S., Girshick R., Arbel´aez P., Malik J.* Learning rich features from RGB-D images for object detection and segmentation // European Conference on Computer Vision. – Springer, 2014. – P. 345-360.
10. *Кухаренко Б.Г.* Алгоритмы выделения объектов переднего плана из фона и интерактивного редактирования изображений // Приложение к журналу информационные технологии. – № 4. – М., 2012. – 32 с.
11. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. – М.: Техносфера, 2005. – 1072 с.
12. *Абасова А.М.* Алгоритм повышения устойчивости к деструктивным воздействиям цифровых водяных знаков, встраиваемых в цветное изображение // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 75-81.
13. *Абасова А.М.* Использование методов морфологической обработки изображений для внедрения цифровых водяных знаков // Материалы VI Международной научно-технической конференции «Инфокоммуникационные технологии в науке, производстве и образовании (Инфоком-6)». ФГАОУ ВПО Северо-Кавказский федеральный университет, 2014. – С. 199-203.
14. *Абасова А.М.* Защита информационного содержания цифровых изображений путем применения дополнительных критериев выбора объектов для внедрения цифровых водяных знаков // Вестник современных исследований. – 2018. – № 10-1. – С. 249-252.
15. *Mills R.L.* Novel method and system for pattern recognition and processing using data encoded as Fourier series in Fourier space // Engineering Applications of Artificial Intelligence. – March 2006. – Vol. 19, Issue 2. – P. 219-234.
16. *Хорн Б.К.П.* Зрение роботов: пер. с англ. – М.: Мир, 1989. – 487 с.

17. *Kutter M., Jordan F., Bossen F.* Digital signature of color images using amplitude modulation // Journal of Electronics Imaging, – 1998. – Vol. 7. – P. 326-332.
18. *Kutter M., Jordan F., Bossen F.* Digital signature of color images using amplitude modulation // Proc. of the SPIE Storage and Retrieval for Image and Video Databases. – 1997. – P.518-526
19. *Грибунин В.Г., Оков И.Н., Туринцев В.И.* Цифровая стеганография. – М.: СОЛОН-Пресс, 2017. – 262 с.
20. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.

REFERENCES

1. *Nevskaya M.A., Tarasova E.N., Sukharev E.E.* Avtorskoye pravo v izdatel'skom biznese i SMI [Copyright in the publishing business and media]. Moscow: Dashkov i K, 2008, 300 p.
2. *Abasova A.M., Babenko L.K.* Razrabotka algoritma vnedreniya tsifrovogo vodyanogo znaka na baze morfologicheskoy obrabotki izobrazheniya i modulyarnoy arifmetiki dlya protivodeystviya ugrozam khishcheniya ob''ektov intellektual'noy sobstvennosti [Development of an algorithm for the introduction of a digital watermark based on morphological image processing and modular arithmetic to counter threats of theft of intellectual property], *Mezhdunarodnyy zhurnal prikladnykh i fundamental'nykh issledovaniy* [International journal of applied and fundamental research], 2018, No. 6, pp. 9-14.
3. *Gribunin V.G., Kostyukov V.E, Martynov A.P., Nikolayev D.B., Fomchenko V.N.* Steganograficheskiye sistemy. Ataki, propusknaya sposobnost kanalov i otsenka stoykosti: uchebno-metodicheskoye posobiye [Steganographic systems. Attack, channel capacity and durability assessment: textbook], ed. by V.G. Gribunin. Sarov: FGUP «RFYATS-VNIIEF», 2015, 217 p.
4. *Belobokova Y.A.* Modeli i algoritmy zashchitnoy markirovki dlya obespecheniya autentichnosti i tselostnosti rastrovykh izobrazheniy: avtoref. dis. na soisk. uchen. step. kand. tekhnich. nauk [Models and algorithms of protective marking to ensure the authenticity and integrity of bitmaps: the author's abstract cand. of eng. sc. diss.] (05.13.17). Moscow, 2014, 19 p.
5. *Konakhovich, G.F., Puzyrenko A.Y.* Komp'yuternaya steganografiya. Teoriya i praktika [Computer steganography. Theory and practice]. Kiev: MK-Press, 2006, 288 p.
6. *Cox I.J., Miller M., Bloom J., Fridrich J.* Digital watermarking and steganography. San Francisco: Morgan Kaufmann Publishing, 2008, 624 p.
7. *Terzija N.* Robust digital image watermarking algorithms for copyright protection: genehmigte dissertation. Belgrad, 2006, 161 p.
8. *Karpin A.* Fotografiya dlya nachinayushchikh [Photography for beginners]. Samizdat, 2012, 239 p.
9. *Gupta S., Girshick R., Arbel´aez P., Malik J.* Learning rich features from RGB-D images for object detection and segmentation, *European Conference on Computer Vision*, Springer, 2014, pp. 345-360.
10. *Kukharenko B.G.* Algoritmy vydeleniya ob"yektov perednego plana iz fona i interaktivnogo redaktirovaniya izobrazheniy [Algorithms for selecting foreground objects from the background and interactive image editing], *Prilozheniye k zhurnalu informatsionnye tekhnologii* [Appendix to the journal information technology], No. 4. Moscow, 2012, 32 p.
11. *Gonsales R., Vuds R.* Tsifrovaya obrabotka izobrazheniy [Digital image processing]. Moscow: Tekhnosfera, 2005, 1072 p.
12. *Abasova A.M.* Algoritm povysheniya ustoychivosti k destruktivnym vozdeystviyam tsifrovykh vodyanykh znakov, vstraivayemykh v tsvetnoye izobrazheniye [Algorithm for increasing resistance to destructive effects of digital watermarks embedded in a color image], *Izvestiya YuFU. Tekhnicheskiye nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 75-81.
13. *Abasova A.M.* Ispolzovaniye metodov morfologicheskoy obrabotki izobrazheniy dlya vnedreniya tsifrovykh vodyanykh znakov [The use of morphological image processing methods for the introduction of digital watermarks], *Materialy VI Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «Infokommunikatsionnyye tekhnologii v nauke, proizvodstve i obrazovanii (Infokom-6)». FGAOU VPO Severo-Kavkazskiy federalnyy universitet, 2014* [Proceedings of the VI International scientific and technical conference " infocommunication technologies in science, production and education (InfoCom-6)". North Caucasus Federal University, 2014], pp. 199-203.

14. *Abasova A.M.* Zashchita informatsionnogo soderzhaniya tsifrovykh izobrazheniy putem primeneniya dopolnitel'nykh kriteriyev vybora ob"yektov dlya vnedreniya tsifrovykh vodyanykh znakov [Protection of information content of digital images by applying additional criteria for the selection of objects for the introduction of digital watermarks], *Vestnik sovremennykh issledovaniy* [Bulletin of modern research], 2018, No. 10-1, pp. 249-252.
15. *Mills R.L.* Novel method and system for pattern recognition and processing using data encoded as Fourier series in Fourier space, *Engineering Applications of Artificial Intelligence,* March 2006, Vol. 19, Issue 2, pp. 219-234.
16. *Khorn B. K. P.* Zreniye robotov [Vision robots]: transl. from Engl. Moscow: Mir, 1989б 487 p.
17. *Kutter M., Jordan F., Bossen F.* Digital signature of color images using amplitude modulation, *Journal of Electronics Imaging*, 1998, Vol. 7, pp. 326-332.
18. *Kutter M., Jordan F., Bossen F.* Digital signature of color images using amplitude modulation, *Proc. of the SPIE Storage and Retrieval for Image and Video Databases,* 1997, pp. 518-526.
19. *Gribunin V.G., Okov I.N., Turintsev V.I.* Tsifrovaya steganografiya [Digital steganography]. Moscow: SOLON-Press, 2017, 262 p.
20. *Akushskiy I.Ya., Yuditskiy D.I.* Mashinnaya arifmetika v ostatochnykh klassakh [Machine arithmetic in residual classes]. Moscow: Sovetskoye radio, 1968, 440 p.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Абасова Анастасия Михайловна – Южный федеральный университет; e-mail: moonriel@yandex.ru; 347928, г. Таганрог, ул. Чехова, 22; тел.:+79615006290; кафедра безопасности информационных технологий; аспирантка.

Бабенко Людмила Климентьевна – e-mail: lkbabenko@sfedu.ru; тел.: +78634361518; кафедра безопасности информационных технологий; профессор.

Abasova Anastasiya Mikhailovna – Southern Federal University; e-mail: moonriel@yandex.ru; 22, Chehov street, Taganrog, 347928, Russia; phone: +79615006290; the department of security of information technologies; postgraduate student.

Babenko Liudmila Klimentevna – e-mail: lkbabenko@sfedu.ru; phone: +78634361518; the department of security of information technologies; professor.

УДК 621.315.592, 004.272.3 DOI 10.23683/2311-3103-2018-8-145-153

П.Л. Новиков, К.В. Павский, А.В. Двуреченский

ИССЛЕДОВАНИЕ ПОВЕРХНОСТНОЙ АТОМНОЙ ДИФФУЗИИ НА СТРУКТУРИРОВАННЫХ ПОДЛОЖКАХ КРЕМНИЯ МЕТОДОМ МОЛЕКУЛЯРНОЙ ДИНАМИКИ − МОДЕЛИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ВЫСОКОЭФФЕКТИВНЫХ АЛГОРИТМОВ*

В мире наблюдается интерес к созданию пространственно-упорядоченных массивов квантовых точек (КТ). Эти структуры являются перспективными для создания термически стабильных лазеров на КТ, МОП-структур на подвижных носителях, матриц фоточувствительных сенсоров и др. Для создания таких структур многообещающей является концепция гетероэпитаксии на структурированной подложке. Структурированными мы называем подложки, на поверхности которых с помощью методов литографии создается регулярный рисунок с канавками или ямками. В ходе гетероэпитаксии на структурированной подложке можно добиться того, чтобы нановостровки зарождались в ямках/канавках и, таким образом, формировали пространственно упорядоченный массив КТ. С точки зрения фундаментальных вопросов малоизученным является механизм атомной диффузии по

*Работа выполнена при финансовой поддержке Президиума РАН (ГЗ 0306-2018-0012), РФФИ и Правительства Новосибирской области в рамках научного проекта № 18-41-540005_р_а..