УДК 004.056.55:004.932.2

ЗАЩИТА ГРАФИЧЕСКОЙ ИНФОРМАЦИИ ОТ НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ МАРКИРОВАНИЕМ В ПРОСТРАНСТВЕННОЙ ОБЛАСТИ

[1]Земцов А.Н., [2]Чан Зунг Хань

[1]ФГБОУ ВО «Волгоградский государственный технический университет», Волгоград, e-mail: ecmsys@yandex.ru;

[2]Национальный экономический университет, Ханой, Вьетнам, e-mail: ecmsys@yandex.ru

Рассматриваются вопросы защиты от неправомерного использования графической информации с помощью внедрения данных лица с правом собственности в неподвижные изображения и видеопоследовательности. Представление изображений и видео в цифровом виде способствует эффективному и широкому распространению информации, но подобный способ доступа к данным также создает возможность для неправомерного заимствования результата интеллектуальной деятельности без согласования и компенсирующих выплат авторам. После внедрения в неподвижные изображения или кадры видеопоследовательности данных лица с правом собственности на результат интеллектуальной деятельности представляется возможным отслеживание распространения копий художественного произведения. Встраивание данных лица с правом собственности на результат интеллектуальной деятельности предлагается производить в компоненты цветности сигнала в области, которые имеют низкий показатель насыщенности, так как на подобные области алгоритмы обработки изображений не оказывают существенного влияния, что повышает робастность алгоритма. Обнаружение подобных областей на изображении выполняется путем обработки и анализа яркостной составляющей, для чего осуществляется преобразование из исходного цветового пространства в YCbCr. На основе мер оценки эффективности работы алгоритма внедрения данных на эталонных изображениях проведен анализ результатов экспериментов. Приводится обоснование эффективности предлагаемой методики защиты графической информации от неправомерного использования.

Ключевые слова: авторское право, результат интеллектуальной деятельности, стеганография, скрытие данных, цифровой водяной знак, защита информации

SECURING OF IMAGES FROM UNAUTHORIZED USE BASED ON EMBEDDING IN THE SPATIAL DOMAIN

[1]Zemtsov A.N., [2]Chan K.Z.

[1]Volgograd State Technical University, Volgograd, e-mail: ecmsys@yandex.ru;

[2]National Economics University, Hanoi, Vietnam, e-mail: ecmsys@yandex.ru

The issues of unauthorized use of graphic information by embedding data of the owner in still images and video sequences are considered. Representing images and videos in digital form facilitates effective and widespread dissemination of information, but this way of accessing data also creates the opportunity for illegal borrowing of the result of intellectual activity without approval and compensatory payments to authors. After embedding in still images or frames of a video sequence the data of the person with the right of ownership of the result of intellectual activity, it becomes possible to track the distribution of copies of a work of art. It is proposed to embed the data of the person with the right of ownership of the result of intellectual activity into the chrominance components of the signal in areas that have a low saturation index because image processing algorithms do not have a significant effect on such areas, which increases the robustness of the algorithm. The detection of such areas in the image can be performed by processing and analyzing the brightness component, for which a conversion from the original color space to YCbCr is performed. On the basis of measures for evaluating the efficiency of the algorithm for introducing data on reference images, an analysis of the results of experiments was carried out. The rationale for the effectiveness of the proposed methodology for securing graphical information from unauthorized use is given.

Keywords: copyright, result of intellectual activity, steganography, data hiding, digital watermark, information security

Стеганография – это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи [1]. Под стегосистемой в данной работе понимается объединение методов и средств, используемых для создания скрытого канала для передачи информации. Данные лица с правом собственности на результат интеллектуальной деятельности внедряются в пустой контейнер, не содержащий секретного сообщения, например элемент картографической информации, кадр видеопоследовательности или медицинские данные, хранимые в облачной платформе в форме физиологических сигналов [2], таких как ЭЭГ, ЭКГ, ЭОГ, ЭМГ, КТ, МРТ, ПЭТ, и т.д. Стегоконтейнером называется контейнер, содержащий секретное сообщение. Для дополнительной защиты данных лица с правом собственности на результат интеллектуальной деятельности может использоваться ключ, который необходим для внедрения данных в заданные области стегоконтейнера [3]. Ключи в стегосистемах бывают двух типов: секретные и открытые. Если стегосистема использует секретный ключ, то он должен быть

или создан до начала обмена сообщениями, или передан по защищенному каналу. Стегосистема, использующая открытый ключ, должна быть устроена таким образом, чтобы было невозможно получить закрытый ключ, а открытый ключ передается по незащищенному каналу. Одним из наиболее эффективных методов защиты графической информации от неправомерного использования является использование стеганографических методов [1].

Задача защиты графической информации от неправомерного использования заключается в том, чтобы произвести внедрение информации с минимальным искажением исходного изображения. Представляется целесообразным задействовать для этого наименее значимую относительно восприятия изображения информацию.

Изображения или видеопоследовательности обладают большой избыточностью благодаря несовершенству человеческого зрения, а также особенностям их представления в цифровом формате.

С другой стороны, форматы файлов, содержащих графическую информацию, спроектированы таким образом, чтобы минимизировать размер хранимых данных изображений с целью отказаться от малозначительной для восприятия системой человеческого зрения информации [4].

Защита графической информации от неправомерного использования маркированием в пространственной области основана на внедрении в неподвижные изображения или кадры видеопоследовательности данных лица с правом собственности на результат интеллектуальной деятельности, которые также известны как цифровые водяные знаки. Неподвижные изображения или кадры видеопоследовательности, которые подвергаются процедуре превентивной защиты на основе внедрения данных лица с правом собственности на результат интеллектуальной деятельности, обычно называют оригиналом или произведением.

Основная проблема, с которой сталкиваются подобные методы, заключается в том, что данные лица с правом собственности на результат интеллектуальной деятельности должны быть устойчивыми к обработке изображения. К причинам, вызывающим данную проблему, относятся различные виды шума в канале связи, особенно выраженные в повсеместно используемых беспроводных сетях связи [5], выполнение процедур фильтрации широким спектром алгоритмов обработки изображений, передискретизация, кадрирование [6], компрессия графической информации с потерями [7–9], цифро-аналоговые и аналого-цифровые преобразования и т.д. Перечисленные операции являются типовыми при стандартном процессе обработки графической информации. В то же время эти макрооперации могут осуществляться преднамеренно, с целью удалить данные лица с правом собственности на результат интеллектуальной деятельности.

Другая проблема систем превентивной защиты графической информации состоит в том, что добавление данных лица с правом собственности на результат интеллектуальной деятельности изменяет изображение, что может вызывать раздражение потребителя результата интеллектуальной деятельности, но также позволяет лицу, осуществляющему неправомерную деятельность, получить представление о существовании данных отслеживания.

Методы встраивания данных лица с правом собственности на результат интеллектуальной деятельности можно классифицировать по различным признакам. К одному из таких классификационных признаков исследователи относят область встраивания, в которую производится внедрение данных лица с правом собственности на результат интеллектуальной деятельности. Например, данные лица с правом собственности на результат интеллектуальной деятельности могут быть встроены в пространственную область стегоконтейнера [10]. Альтернативная возможность предусматривает встраивание этих данных в частотной области, что позволяет достичь устойчивости к внешним по отношению к стегоконтейнеру воздействиям [11, 12].

При извлечении внедренных данных анализируются младшие n бит контейнера. В случае, если значение, образованное этими битами, меньше 2^{n-2}, то считается что в контейнер встроена нулевая посылка, в противном случае в контейнер встраивалась единичная посылка.

Предлагается также использовать модификацию метода наименьшего значащего бита, позволяющую внедрять данные в старшие биты путем замены значения на ближайшее по кодовому расстоянию. Таким образом, выбирая нужную битовую плоскость или элементы разных плоскостей, можно манипулировать отношением робастности к степени скрытности сообщения. Дополнительно рассматриваются следующие модификации метода: при записи битов водяного знака используется канал синего цвета, как наименее воспринимаемого системой человеческого зрения, а также при записи битов водяного знака используется канал яркости, производный от каналов исходного цветового простран-

ства. Цель исследования заключается в разработке технических решений по преодолению описанных ограничений.

Предлагаемая методика защиты графической информации

Для достижения поставленной цели подавляющее большинство методов превентивной защиты графической информации используют исходное цветовое пространство. Данные лица с правом собственности на результат интеллектуальной деятельности встраиваются в процессе кодирования в определенные области изображения или кадра видеопоследовательности одной из основных цветовых компонент.

На рис. 1 представлена известная схема внедрения данных в изображения или кадр видеопоследовательности, где $I = RGB$ – исходное изображение, W – цифровой водяной знак, $W = \{\omega_{ij} \mid \omega_{ij} \in \{0,1\}\}$, I_W – маркированное изображение.

Функция встраивания данных лица с правом собственности на результат интеллектуальной деятельности E_{mb} осуществляет внедрение в изображение I цифрового водяного знака W с опциональным использованием ключа K, использование которого позволяет в целом повысить защищенность встраиваемых данных. Встраивание осуществляется в компоненту синего цвета $B = \{b_{ij} \mid b_{ij} \in [0,255]\}$ исходного цветового пространства в соответствии с выражением $b'_{ij} = b_{ij} \otimes \left[256 - (1 - \omega_{ij})2^{n-1}\right]$. Предварительно изображение разбивается на множество непересекающихся блоков размером, например, 8×8 пикселей. В результате выполнения функции E_{mb} генерируется модифицированное изображение I_W.

Извлечение из компоненты синего цвета $B = \{b_{ij} \mid b_{ij} \in [0,255]\}$ исходного цветового пространства осуществляется в соответствии с выражением

$$\omega_{ij} = \begin{cases} 0, b_{ij} \bmod 2^{n-1} < 2^{n-2} \\ 1, b_{ij} \bmod 2^{n-1} \geq 2^{n-2} \end{cases}.$$

На практике стегоконтейнер, содержащий водяной знак, может быть намеренно или случайно искажен. В обоих случаях стегосистема должна обеспечивать возможность обнаружения и извлечения цифрового водяного знака после атаки.

Встраивание данных лица с правом собственности на результат интеллектуальной деятельности предлагается производить в компоненты цветности сигнала в области, которые имеют цвет, близкий к черному, так как на подобные области алгоритмы обработки изображений не оказывают существенного влияния, что повышает робастность алгоритмов превентивной защиты. Обнаружение подобных областей на изображении выполняется путем обработки и анализа яркостной составляющей, для чего осуществляется преобразование из исходного цветового пространства, которое используется в современных сканерах, принтерах и системах отображения графической информации, в *YCbCr* [13].

На рис. 2 представлена схема внедрения данных в компоненту яркости изображения.

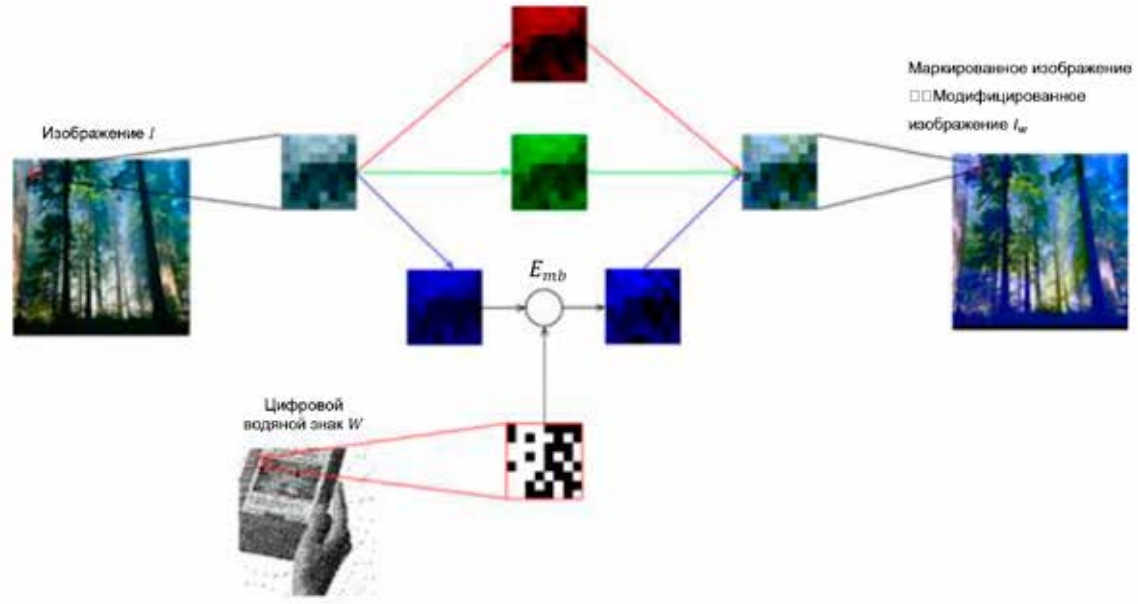

Рис. 1. Схема внедрения данных в методе наименьшего значащего бита

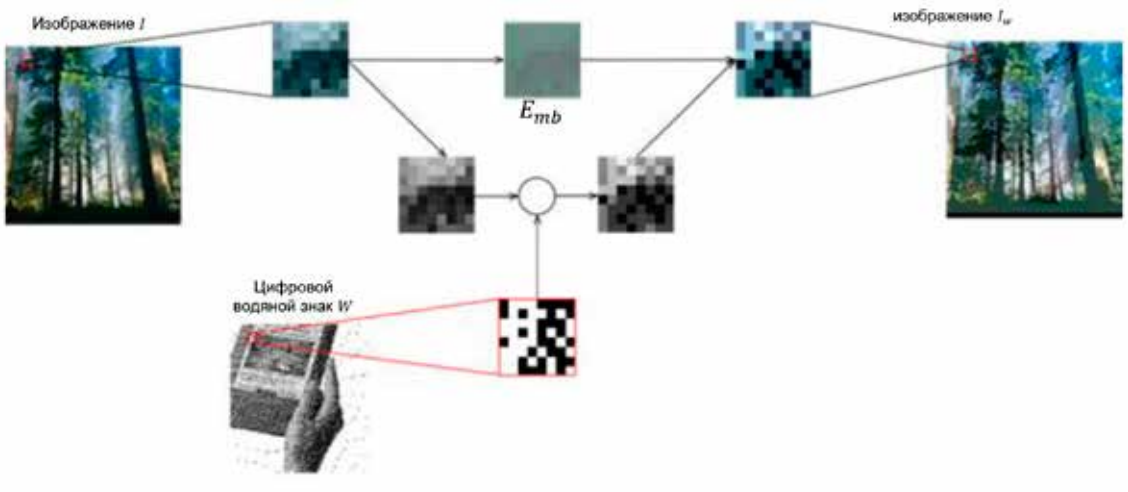

Рис. 2. Схема внедрения данных в компоненту яркости изображения

В соответствии с рекомендацией МСЭ-R BT.601-7 для систем цифрового телевидения и цифровых изображений преобразование из исходного цветового пространства в *YCbCr* определяется как

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.29900000 & 0.58700000 & 0.11400000 \\ -0.16873600 & -0.33126400 & 0.50000000 \\ 0.50000000 & -0.4186680 & -0.08131200 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix},$$

где *Y* представляет собой компоненту яркости, *Cb* и *Cr* являются соответственно синей и красной цветоразностными компонентами. Необходимо отметить, что результирующий битовый поток совместим со стандартизованными декодерами.

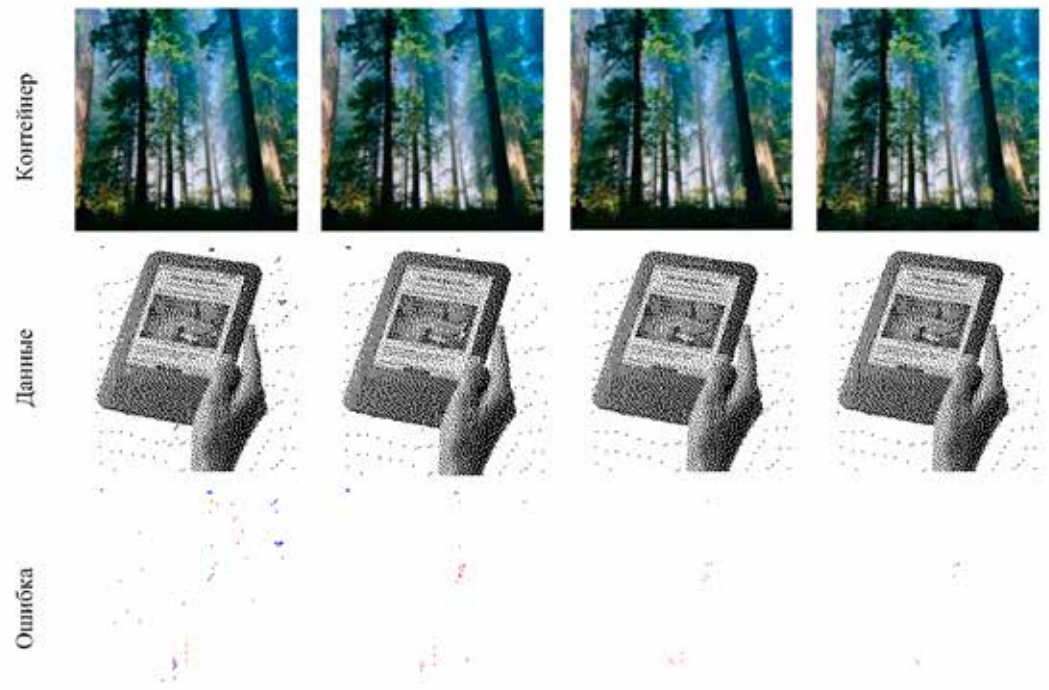

Рис. 3. Результаты встраивания и извлечения данных

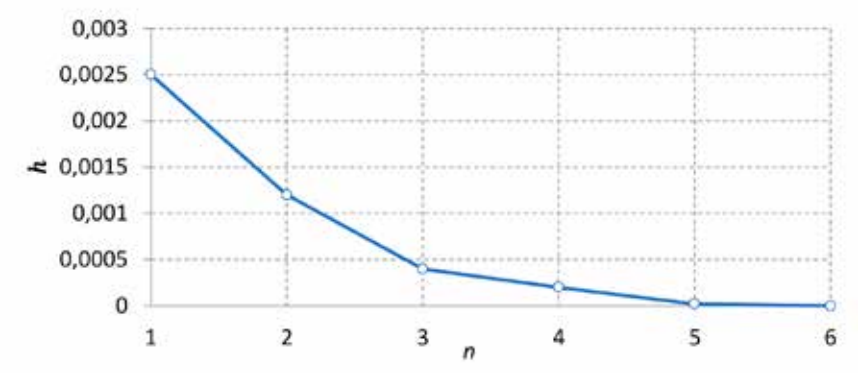

Рис. 4. Зависимость h от n

Результаты экспериментов

Встраивание данных лица с правом собственности на результат интеллектуальной деятельности в контейнер неизбежно приводит к искажению исходного изображения. С целью анализа степени вносимых в контейнер искажений проводится исследование влияния алгоритма и входных параметров на контейнер. При извлечении данных лица с правом собственности на результат интеллектуальной деятельности осуществляется его сравнение с исходным изображением с целью расчета меры вносимых искажений.

Примеры результатов встраивания и извлечения данных лица с правом собственности на результат интеллектуальной деятельности показаны на рис. 3.

В качестве меры искажений, вносимых алгоритмом встраивания данных лица с правом собственности на результат интеллектуальной деятельности, используются различные метрики, такие как среднеквадратическое отклонение

$$MSE = \frac{\sum_{x,y}\left(I_{x,y} - I_{Wx,y}\right)^2}{N_1 N_2},$$

пиковое отношение уровня сигнала к уровню шума

$$PSNR = 10\log_{10}\left(N_1 N_2 \frac{\max\limits_{x,y} I_{x,y}^2}{\sum_{x,y}\left(I_{x,y} - I_{Wx,y}\right)^2}\right),$$

коэффициент битовых ошибок h, и другие, широко принятые в теории связи [14]. Здесь N_1, N_2 – размеры изображения в пикселях, $I_{x,y}$ – яркость пикселя x, y в исходном контейнере, $I_{Wx,y}$ – яркость пикселя в модифицированном контейнере.

На рис. 4 показана зависимость коэффициента битовых ошибок h от n.

Заключение

В настоящей работе предложена методика защиты графической информации от неправомерного использования с помощью стеганографических методов, встраивающих и скрывающих данные лица с правом собственности на результат интеллектуальной деятельности в пространственной области. С точки зрения вносимых алгоритмом в изображение искажений хорошие показатели имеет группа алгоритмов с использованием младшего значащего бита, имеющего множество модификаций, в том числе устойчивых к атакам. Следует отметить, что группа стегоалгоритмов на основе дискретного косинусного преобразования при эквивалентных начальных условиях имеет худшие с точки зрения вносимых стегоалгоритмом в изображение искажений показатели, так как основаны на более сильном по среднему значению искажении сообщения по сравнению с стегоалгоритмами на основе младшего значащего бита, а также связано с перегруженностью контейнера в алгоритмах с использованием дискретного косинусного преобразования, что может нивелироваться уменьшением доступной для внедрения емкости контейнера. При сохранении контейнера в формате JPEG хорошие результаты при n = 8 или q = 100 показывают стегоалгоритмы на основе младшего значащего бита. Операция масштабирования незначительно влияет на результативность алгоритма превентивной защиты на основе младших значащих бит при сохранении как в формате PNG, так и в других форматах. Сохранение в формате JPEG полностью уничтожает содержимое контейнера при значениях h, близких к 0,5. Также было установлено, что слабо адаптируются к операции масштабирования контейнера алгоритмы на основе дискретного косинус-

ного преобразования в результате нарушения границ блоков 8×8 пикселей, которое приводит к значительному искажению матриц коэффициентов.

Список литературы

1. Shih F.Y. Digital Watermarking and Steganography: Fundamentals and Techniques, Second Edition, CRC Press, 2017. 270 p.

2. Бабенко Л.К., Шумилин А.С., Алексеев Д.М. Алгоритм обеспечения безопасности конфиденциальных данных медицинской информационной системы хранения и обработки результатов обследований // Известия ЮФУ. Технические науки. 2020. № 5 (215). С. 6–16.

3. Kanwal S. A Robust Data Hiding Reversible Technique for Improving the Security in e-Health Care System. Computer Modeling in Engineering and Sciences. 2023. № 134 (1). P. 201–219.

4. Jeong S. An overhead-free region-based JPEG framework for task-driven image compression. Pattern Recognition Letters. 2023. № 165. P. 1–8.

5. Devi G.N.S., Mittal V.K. Enhancing Signal in Noisy Environment: A Review. Smart Innovation, Systems and Technologies. 2022. № 248. P. 183–194.

6. Шемякина Ю.А., Жуковский А.Е., Коноваленко И.А., Николаев Д.П. Алгоритм автоматического кадрирования цифровых изображений при проективном преобразовании // Труды Института системного анализа Российской академии наук. 2018. Т. 68. № S1. С. 142–149.

7. Земцов А.Н. Сравнительный анализ эффективности методов сжатия изображений на основе дискретного косинусного преобразования и фрактального кодирования // Прикладная информатика. 2011. Ч. 1. № 4 (34). С. 90–104.

8. Земцов А.Н. Сравнительный анализ эффективности методов сжатия изображений на основе дискретного косинусного преобразования и фрактального кодирования // Прикладная информатика. 2011. Ч. 2. № 5 (35). С. 77–84.

9. Zemtsov A. Medical Image Coding Using Le Gall Transform. Proceedings of the IV International Research Conference Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2017). 2017. № 72. P. 148–151.

10. Wang H., Su Q. A color image watermarking method combined QR decomposition and spatial domain. Multimedia Tools and Applications. 2022. № 81 (26). P. 37895–37916.

11. Земцов А.Н., Цыбанов В.Ю. Защита от неправомерного использования графической информации в социальных сетях // Современные наукоемкие технологии. 2020. № 7. С. 51–56.

12. Gupta S., Saluja K., Solanki V., Kaur K., Singla P., Shahid M. Efficient methods for digital image watermarking and information embedding. Measurement: Sensors. 2022. № 24. P. 100520.

13. He J., Xu X., Wang D., Guo T. Image Highlight Elimination Method Based on the Combination of YCbCr Spatial Conversion and Pixel Filling. Advances in Intelligent Systems and Computing. 2021. № 1303. P. 1303-1309.

14. Panwar P., Dhall S., Gupta S. A multilevel secure information communication model for healthcare systems. Multimedia Tools and Applications. 2021. № 80 (5). P. 8039-8062.