

УДК 004.056

Doi: 10.31772/2712-8970-2021-22-1-61-69

Для цитирования: Шипулин П. М., Лебедев Р. В., Сосновский М. С. Применение цифровых водяных знаков на основе моментов Цернике в задаче управления электронным архивом фотодокументов // Сибирский аэрокосмический журнал. 2021. Т. 22, № 1. С. 61–69. Doi: 10.31772/2712-8970-2021-22-1-61-69.

For citation: Shipulin P. M., Lebedev R. V., Sosnovskiy M. S. An application of Zernike moments based digital watermarks for photo document electronic archive management // Siberian Aerospace Journal. 2021, Vol. 22, No. 1, P. 61–69. Doi: 10.31772/2712-8970-2021-22-1-61-69.

Применение цифровых водяных знаков на основе моментов Цернике в задаче управления электронным архивом фотодокументов

П. М. Шипулин, Р. В. Лебедев, М. С. Сосновский

АО «Информационные спутниковые системы» имени академика М. Ф. Решетнева
Российская Федерация, 662972, г. Железногорск Красноярского края, ул. Ленина, 52
E-mail: pshipulin@gmail.com

В статье рассмотрен подход к решению проблемы обеспечения целостности наборов данных, характерной для задач управления электронными архивами. Данная проблема актуальна для высокотехнологичных производств, где посредством фотофиксации осуществляется обязательный контроль выполнения особо ответственных операций. Фотофиксация позволяет документировать ход выполнения технологического процесса, фиксировать состояние комплектующих на входном и выходном контроле, регистрировать несоответствия. Контроль целостности фотоматериалов необходим для исключения возможной подмены изображения или его повторного использования как в результате непреднамеренных ошибок исполнителя, так и в целях сокрытия дефектов производства. Предложен способ организации электронного архива фотодокументов, который использует метод внедрения стеганографических цифровых водяных знаков (ЦВЗ), основанный на моментах Цернике, вычисляемых для особых точек маркируемых изображений. Данный метод позволяет сохранять ЦВЗ на изображении даже после его геометрических преобразований (повороты, сжатие, отражения и т. д.). В ЦВЗ предложено включать данные идентификации фиксируемого фотодокументом процесса, а также сведения о других фотодокументах, что позволяет контролировать целостность всего набора материалов фотофиксации. При нанесении ЦВЗ данным методом не меняется формат представления фотодокумента и не создается побочных структур в виде метаданных или служебных файлов, файл фотодокумента остается неизменным как внешне для человека, так и технически, что обеспечивает дальнейшую работу с ним в стандартных программных приложениях.

Ключевые слова: управление доступом, стеганография, цифровые водяные знаки, маркирование изображений, моменты изображений, моменты Цернике.

An application of Zernike moments based digital watermarks for photo document electronic archive management

P. M. Shipulin, R. V. Lebedev, M. S. Sosnovskiy

JSC Academician M. F. Reshetnev “Information Satellite Systems”
52, Lenin St., Zheleznogorsk, Krasnoyarsk region, 662972, Russian Federation
E-mail: pshipulin@gmail.com

In this article authors are considering about information security data integrity problem relevant for electronic archive management. In high-tech industry large electronic photo archives arises as a part of quality management. Photofixation applied for responsible operations control, documenting the technological process, fixing the components state on input and output control, incongruities registration. An image substitution or reuse possibility makes necessary electronic archive proto document integrity control. This illegal actions can be both the result of operator mistake and motivated by intentional a defect concealment. As a solution authors suggest an electronic archive organizing method for storing photo documents. The method based on a digital watermark labeling of full-color images with orthogonal Zernike moments calculated for certain image points (and their neighborhoods). Suggested method can prevent watermark destruction by geometric image transformation (rotation, compressing, reflection etc.). Digital watermark contains both information about technological process on current image and information about other images – this fact lets talk about integrity of whole photo documents set. One of the most important method characteristic is image format invariability and additional metadata files unnecessary what allows user to use standard software for a further work with photo document.

Keywords: access management, steganography, digital watermarking, image labeling, image moments, Zernike moments.

Введение. В настоящее время фотофиксация является обязательным инструментом контроля качества продукции во многих высокотехнологических производствах [1; 2]. Она позволяет документировать ход выполнения особо ответственных операций, фиксировать состояние комплектов на входном и выходном контроле, регистрировать несоответствия. Как правило, на предприятиях порядок фотодокументирования закрепляется отраслевыми или внутренними стандартами и определяет технические требования к результату фотодокументирования (формат файлов изображения, разрешение, качество и пр.), а также к способам учета, хранения и обращения с фотодокументами. Для обеспечения возможности беспрепятственного использования материалов фотофиксации разными сторонами правоотношений (заказчик и исполнитель работ, страхователь и страховщик рисков) системы фотофиксации часто организуют на основе общепринятых технологий и форматов. Так, например, архив файлов фотофиксации на практике часто организуют на базе файлового сервера в виде структуры каталогов с механизмами идентификации на основе имен, атрибутов и метаданных файлов изображений.

На этапе помещения изображений в подобные хранилища возникают определенные угрозы целостности информации (свойство устойчивости к несанкционированному изменению [3]): подмена изображения в хранилище, повторное использование фотодокументов [4]. Потенциальный нарушитель может реализовать данные угрозы как случайно, совершая ошибки при работе с большим количеством схожих изображений в сложной структуре каталогов хранилища, так и намеренно, преследуя цели сокрытия технологического дефекта путём подмены изображений или экономии времени на подготовку и проведение фотосъемки, используя ранее выполненные изображения в аналогичной операции.

Часто контроль таких нарушений осуществляется организационно, технические же механизмы на уровне управления работой с архивом, как правило, отсутствуют. Авторами предлагается способ организации электронного архива фотодокументов и структура обеспечивающей его информационной системы (далее – ИС), основанные на использовании стеганографических цифровых водяных знаков (далее – ЦВЗ). ЦВЗ – метаданные изображения (автор съемки, номер операции, маркер производственного процесса и т. д.), невидимо встраиваемые в изображение при помощи асимметричного ключа и стеганографических преобразований (рис. 1). ЦВЗ состоит из кортежа метаданных изображения и хеша ЦВЗ предыдущего изображения, таким образом образуется цепочка изображений.

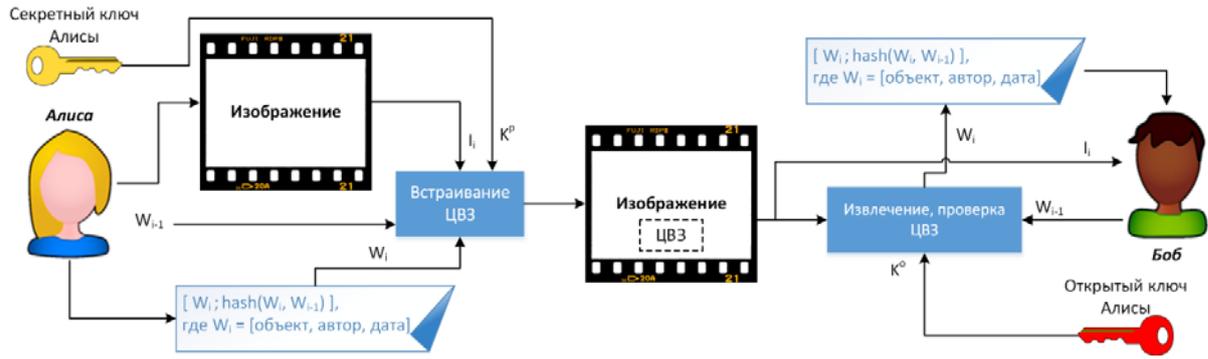


Рис. 1. Процесс встраивания, извлечения и проверки ЦВЗ

Fig. 1. Embedding, extraction and checking processes

Маркирование изображений с помощью ЦВЗ. Методы маркирования изображений ЦВЗ активно разрабатываются учёными в последние годы, подходы к классификации методов предложены в [4–6]. Наиболее перспективными методами маркирования изображений с точки зрения устойчивости к шуму и инвариантности к линейным преобразованиям (геометрическим атакам) являются моментные методы (на основе моментов Цернике, Чебышева, Лежандре и др.) [7–11]. В работе [12] предлагается метод маркирования изображений любых размеров цифровым водяным знаком в особых точках изображения на основе моментов изображений Цернике.

Предложенный метод маркирования изображения ЦВЗ предполагает последовательное многократное внедрение копии ЦВЗ в окрестность каждой s -ой выбранной особой точки на изображении. Общая схема процесса внедрения ЦВЗ в изображение представлена на рис. 2.

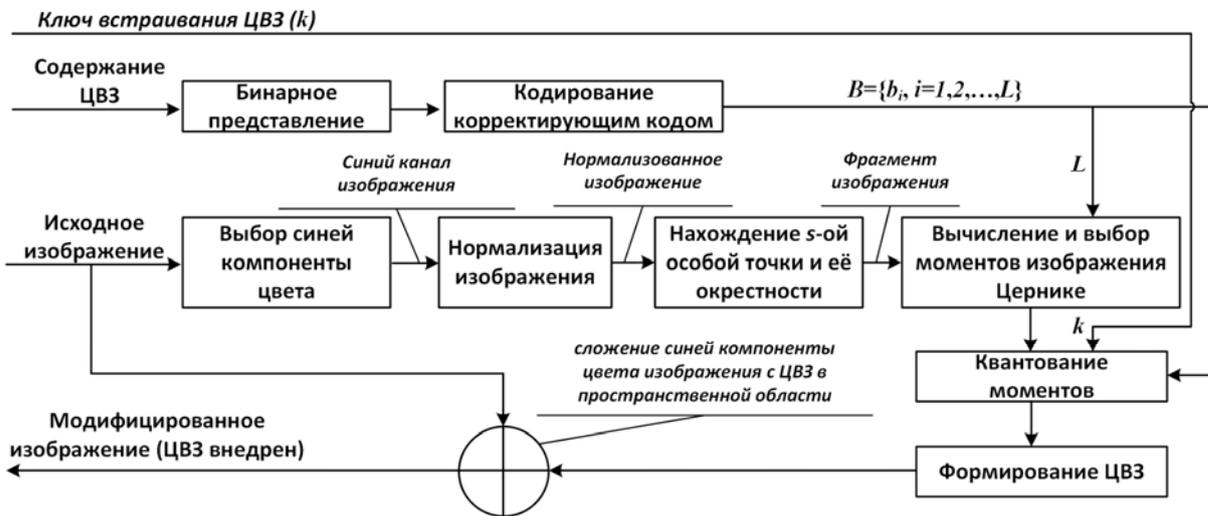


Рис. 2. Общая структурная схема внедрения копии ЦВЗ в изображение

Fig. 2. A watermark-copy embedding diagram

Процесс внедрения ЦВЗ включает следующие этапы:

1. Представление ЦВЗ в виде бинарного массива B длины L , закодированного с использованием алгоритмов корректирующего кодирования (например, кода Хемминга)

$$B = \{b_i \in \{0,1\}, i = 1,2,\dots,L\}.$$

2. Выделение синего цветового канала (В-канала) модели RGB, его нормализация на множество значений $\{0, \dots, 255\}$ функцией $g(x, y) = \frac{f(x, y) - f_{\min}}{f_{\max} - f_{\min}} \cdot 255$, где $f(x, y)$ – функция значений В-канала в точке (x, y) изображения, f_{\min} , f_{\max} – минимальное и максимальное значения f , соответственно.

3. Нахождение особых точек изображения методом Ши – Томаси [13], вычисление координат окрестности особых точек размера 256×256 пикселей.

4. Вычисление ортогональных моментов и радиального полинома Цернике с применением метода Кинтера, выбор подходящих моментов с учетом условий [14–17], формирование вектора моментов $Z_{nm} = \{z_{n_1 m_1}, z_{n_2 m_2}, \dots, z_{n_L m_L}\}$.

5. Квантование вектора Z_{nm} последовательностью битов B , при котором каждый бит ЦВЗ $b_i \in B$ встраивается в соответствующий элемент $z_{n_i m_i} \in Z_{nm}$ при помощи функции модуляции, которая осуществляет псевдослучайное изменение моментов Цернике, добавляя следующий

«шум»: $\left| \tilde{z}_{n_i m_i} \right| = \left| \frac{|z_{n_i m_i}| - d(b_i)}{\Delta} \right| \cdot \Delta + d(b_i)$, где Δ – шаг квантования, $d(b_i)$ – функция дизеринга.

Шаг квантования – настраиваемый параметр системы, значение функции дизеринга зависит от очередного внедряемого бита: $d_i(0) \leftarrow \text{random}(k) : d_i(0) \in \left[0, \frac{\Delta}{2} \right]$, $d_i(1) = d_i(0) + \frac{\Delta}{2}$. При формировании значений участвует генератор псевдослучайных чисел (ГПСЧ), который инициализирован ключом k .

6. Формирование ЦВЗ с использованием функции реконструкции изображения

$$w(x, y) = \sum_{i=1}^L \left(\varepsilon_{n_i m_i} \cdot V_{n_i m_i} + \varepsilon_{n_i(-m_i)} \cdot V_{n_i(-m_i)} \right),$$

где $\varepsilon_{n_i m_i} = (\tilde{z}_{n_i m_i} - z_{n_i m_i})$, $\varepsilon_{n_i(-m_i)} = (\tilde{z}_{n_i(-m_i)} - z_{n_i(-m_i)})$, $i = 1, 2, \dots, L$, $V_{n_i m_i}$ – значение радиального полинома Цернике.

7. Формирование итогового изображения с ЦВЗ путем сложения фрагмента исходного изображения в окрестности особой s -й точки и ЦВЗ в пространственной области

$$\tilde{f}_s(x, y) = f_s(x, y) + w(x, y),$$

где $f_s(x, y)$ – функция изображения в окрестности особой s -й точки.

Извлечение ЦВЗ из изображения осуществляется практически аналогично процессу встраивания и предполагает последовательное извлечение копии ЦВЗ из окрестности каждой s -й выбранной особой точки на изображении. Общая структурная схема процесса извлечения копии ЦВЗ из изображения представлена на рис. 3. После извлечения всех копий ЦВЗ осуществляется проверка их корректности с заранее заданным порогом и принимается решение об идентификации или не идентификации ЦВЗ в изображении.

Исходными параметрами для извлечения ЦВЗ являются ключ извлечения – k , шаг квантования – Δ , длина бинарной последовательности ЦВЗ – L . Вычисление особых точек изображения, их окрестностей и вычисление моментов Цернике для них осуществляется по аналогии с процессом встраивания ЦВЗ. Квантование вектора моментов Z_{nm} выполняется дважды, сперва последовательностью из нулевых, а затем единичных битов. Для восстановления битов ЦВЗ

$B' = \{b'_i \in \{0,1\}, i = 1, 2, \dots, L\}$ используется минимальная разница между вычисленным моментом и квантованным моментом Цернике, т. е. обнаружение бит ЦВЗ осуществляется по пикам в разнице моментов:

$$b'_i = \begin{cases} 1, & \text{если } \left(|z_{n_i m_i}|_1 - |z_{n_i m_i}| \right)^2 < \left(|z_{n_i m_i}|_0 - |z_{n_i m_i}| \right)^2, \text{ где } i = 1, 2, \dots, L. \\ 0, & \text{в противном случае} \end{cases}$$

После восстановления всех бит ЦВЗ производится их корректировка $B \leftarrow h(B')$ путём декодирования корректирующего кода.



Рис. 3. Общая структурная схема извлечения копии ЦВЗ из изображения

Fig. 2. A watermark-copy extraction diagram

Предложенный метод имеет ряд преимуществ в сравнении с аналогами:

1. Высокие показатели робастности – неизменность ЦВЗ при большинстве шумовых и геометрических атак на изображение (повороты, сжатие, отражения и т. д.) [7].
2. Приемлемая вычислительная сложность для изображений любых размеров – обеспечивается за счёт вычисления моментов Цернике не для всего изображения, а лишь для окрестностей его характерных точек.

Необходимо отметить, что метод является применимым для маркирования ЦВЗ изображений различных форматов и характеристик, в том числе к наиболее популярному – JPEG.

Схема организации электронного архива. Клиент-серверная архитектура ИС представлена на рис. 4. Кратко алгоритм работы ИС можно представить следующим образом.

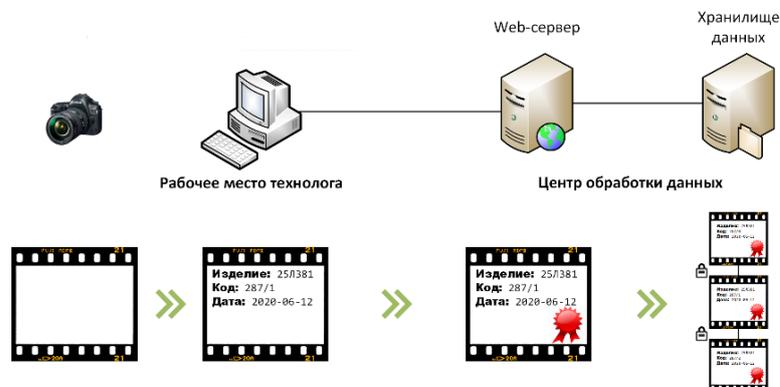


Рис. 4. Функциональная схема ИС учёта фотодокументов

Fig. 4. A functional scheme of photo document archiving information system

Шаг 1. Ответственный исполнитель загружает изображения на сервер через специальный программный интерфейс, снабжая их необходимыми метаданными.

Шаг 2. На сервере происходит проверка наличия ЦВЗ на изображении и вырабатывается соответствующий ЦВЗ в случае успеха проверки.

Шаг 3. Изображения помещаются в хранилище, где находятся в связанной цепочке – неразрывность цепочки основывается на стойкости алгоритмов асимметричной криптографии.

Попытка подмены (вставки) изображений внутри хранилища исключена, так как ЦВЗ представляют собой связанную цепочку (рис. 5). При проверке ЦВЗ на вход проверяющей подсистемы подаётся ЦВЗ, метаданные текущего изображения и хеш ЦВЗ предыдущего изображения – при попытке подмены (вставки) изображения цепочка будет нарушена: проверку не пройдёт либо нелегальное изображение, либо следующее после него легальное.

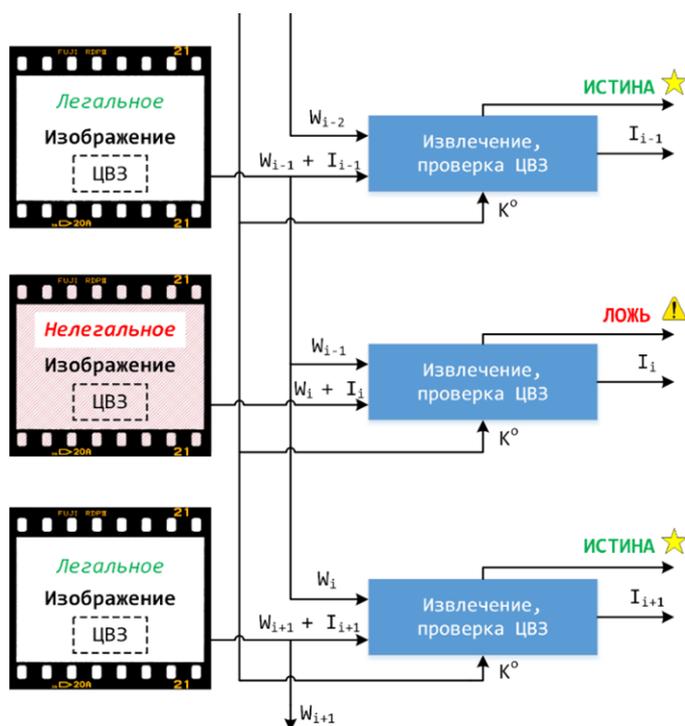


Рис. 5. Попытка нелегального добавления изображения в цепочку

Fig. 5. An illegal image insertion attempt

Попытка повторного использования изображений будет пресечена на этапе загрузки изображения на сервер, так как ИС перед генерацией нового ЦВЗ проверяет наличие другого ЦВЗ на изображении. Подлог изображения в обход программной консоли оператора так же возможно выявить, так как повторно использованное изображение будет иметь более одного ЦВЗ.

Заключение. Предложенный способ применения ЦВЗ при организации электронного архива фотодокументов позволяет осуществлять управление материалами фотофиксации и обеспечить надежную защиту последних от угроз подмены и повторного использования. При нанесении ЦВЗ не меняется формат представления фотодокумента и не создается побочных структур в виде метаданных или служебных файлов – файл фотодокумента остается неизменным как внешне для человека, так и технически, что обеспечивает возможность дальнейшей работы с ним в стандартных программных приложениях.

Библиографические ссылки

1. Бояринова Л. В., Покидышева А. А. Процесс фотофиксации как инструмент для улучшения системы менеджмента качества // Метрология, стандартизация и управление качеством : материалы III Всеросс. науч.-техн. конф. Омск : ОГТУ, 2018. С. 26–29.
2. Гнедых А. Ю. Способы и средства документирования // Документационное обеспечение организационной и производственной деятельности : сб. материалов региональной науч.-практ. конф. Курск : ООО «Инвестсфера», 2015. С. 17–19.
3. Балановская А. В. Анализ угроз информационной безопасности деятельности промышленных предприятий // Вестник самарского муниципального института управления. 2013. № 2 (25). С. 7–17.
4. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М. : Солон-Пресс, 2002. 272 с.
5. Sharma C., Prashar D. Visible and invisible watermarking methods for quality loss of data // International Journal of Advanced Research in Computer Science and Electronics Engineering. 2012. Vol. 1, No. 3. P. 57–63.
6. Орешкина Е. И., Фаворская М. Н. Классификация методов нанесения цифровых водяных знаков // Актуальные проблемы авиации и космонавтики. Красноярск : СибГАУ, 2015. Т. 14, №. 1. С. 414–415.
7. Борисова С. Н. Использование алгоритма вейвлет-преобразования для встраивания цифровых водяных знаков в файлы изображений // XXI век: итоги прошлого и проблемы настоящего плюс. 2015. № 3 (25). С. 110–115.
8. Chen Q., Yang X., Zhao J. Robust image watermarking with Zernike moments // IEEE Canadian Conference on Electrical and Computer Engineering. 2005. P. 1340–1343.
9. Wang Xiang-yang et al. A new robust digital watermarking using local polar harmonic Transform // Computers and Electrical Engineering. 2015. No. 46. P. 403–418.
10. Karthik P., Sathiyapriya E. Robust and High-Secured Watermarking System Using Zernike Moments // International Journal of Innovative Research in Computer and Communication Engineering. 2014. Vol. 2. P. 7074–7079.
11. Hui Zhang, HuazhongShu, GouenouCoatrieux, Jie Zhu, Jonathan Wu. Affine Legendre moment invariants for image watermarking robust to geometric distortions // IEEE Transactions on Image Processing, Institute of Electrical and Electronics Engineers. 2011. No. 20 (8). P. 2189–99.
12. Шниперов А. Н., Сосновский М. С., Шипулин П. М. Робастный метод маркирования изображений цифровым водяным знаком, основанный на ортогональных моментах Цернике // Информационные технологии. 2019. Т. 25, № 7. С. 405–413.
13. Shi J., Tomasi C. Good Features to Track // IEEE Conference on Computer Vision and Pattern Recognition. 1994. P. 593–600.
14. Chandan Singh, Sukhjeet K. Ranade. An Effective Image Watermarking System for High Embedding Capacity // IJCA Proceedings on International Conference on Recent Advances and Future Trends in Information Technology. 2012. P. 22–28.
15. Ismail A. Ismail, Mohamed A. Shouman, Khalid M. Hosny and Hayam M. Abdel Salam. Invariant Image Watermarking Using Accurate Zernike Moments // Journal of Computer Science. 2010. No. 6 (1). P. 52–59.
16. ChandanSingha, EktaWaliab. Fast and numerically stable methods for the computation of Zernike moments // Pattern Recognition. 2010. Vol. 43, P. 2497–2506.

17. Chen Q., Yang X., Zhao J. Robust image watermarking with Zernike moments // IEEE Canadian Conference on Electrical and Computer Engineering. 2005. P. 1340–1343.

References

1. Boyarinova L. V. *Process fotofiksacii kak instrument dlya uluchsheniya sistemy menedzhmenta kachestva* [Photofixation as the quality management system improving tool]. *Metrologiya, standartizatsiya i upravleniye kachestvom: Materialy III Vserossiyskoy nauchno-tekhnicheskoy konferentsii*. Omsk, 2018, P. 26–29. (In Russ.)
2. Gnedykh A. Yu. [Methods and means of documenting]. *Dokumentatsionnoye obespecheniye organizatsionnoy i proizvodstvennoy deyatel'nosti: Sbornik materialov regional'noy nauchno-prakticheskoy konferentsii*. Kursk, 2015. P. 17–19. (In Russ.)
3. Balanovskaya A. V. [Information security threat analysis of an industrial enterprise]. *Vestnik samarskogo munitsipalnogo instituta upravleniya*. 2013, No. 2 (25), P. 7–17. (In Russ.)
4. Gribunin V. G., Okov I. N., Turincev I. V. *Cifrovaya steganographia* [Digital steganography]. Moscow, Solon-Press Publ., 2002, 272 p.
5. Sharma C., Prashar D. Visible and invisible watermarking methods for quality loss of data. *International Journal of Advanced Research in Computer Science and Electronics Engineering*. 2012, Vol. 1, No. 3, P. 57–63.
6. Oreshkina E. I., Favorskaya M. N. [Classification of digital watermarking methods]. *Aktualniye problemy aviatsii i kosmonavтики*. 2015, No. 14 (1), P. 414–415. (In Russ.)
7. Borisova S. N. [Using the wavelet transform algorithm for embedding digital watermarks into image files]. *XXI vek: itogi proshlogo i problemy nastoyashchego plyus*. 2015, No. 2 (25), P. 110–115. (In Russ.)
8. Wang Xiang-yang et al. A new robust digital watermarking using local polar harmonic Transform. *Computers and Electrical Engineering*. 2015, No. 46, P. 403–418.
9. Chen Q., Yang X., Zhao J. Robust image watermarking with Zernike moments. *IEEE Canadian Conference on Electrical and Computer Engineering*. 2005, P. 1340–1343.
10. Karthik P., Sathiyapriya E. Robust and High-Secured Watermarking System Using Zernike Moments. *International Journal of Innovative Research in Computer and Communication Engineering*. 2014, Vol. 2, P. 7074–7079.
11. Hui Zhang, HuazhongShu, GouenouCoatrieux, Jie Zhu, Jonathan Wu. Affine Legendre moment invariants for image watermarking robust to geometric distortions. *IEEE Transactions on Image Processing, Institute of Electrical and Electronics Engineers*. 2011, No. 20 (8), P. 2189–99.
12. Shniperov A. N., Sosnovskiy M. S., Shipulin P. M. [The Robust Image Digital Watermark Labeling Method Based on Orthogonal Zernike Moments]. *Information technologies*. 2019, Vol. 25, No. 7, P. 405–413. (In Russ.)
13. Shi J., Tomasi C. Good Features to Track. *IEEE Conference on Computer Vision and Pattern Recognition*. 1994, P. 593–600.
14. Chandan Singh, Sukhjeet K. Ranade. An Effective Image Watermarking System for High Embedding Capacity. *IJCA Proceedings on International Conference on Recent Advances and Future Trends in Information Technology*. 2012, P. 22–28.
15. Ismail A. Ismail, Mohamed A. Shouman, Khalid M. Hosny and Hayam M. Abdel Salam. Invariant Image Watermarking Using Accurate Zernike Moments. *Journal of Computer Science*. 2010, No. 6 (1), P. 52–59.

16. Chandan Singha, Ekta Waliab. Fast and numerically stable methods for the computation of Zernike moments. *Pattern Recognition*. 2010, Vol. 43, P. 2497–2506.

17. Chen Q., Yang X., Zhao J. Robust image watermarking with Zernike moments. *IEEE Canadian Conference on Electrical and Computer Engineering*. 2005, P. 1340–1343.

© Шипулин П. М., Лебедев Р. В., Сосновский М. С., 2021

Шипулин Павел Михайлович – инженер-программист 2 категории сектора защиты информации; АО «Информационные спутниковые системы» имени академика М. Ф. Решетнева». E-mail: pshipulin@gmail.com.

Лебедев Роман Владимирович – начальник сектора защиты информации; АО «Информационные спутниковые системы» имени академика М.Ф. Решетнёва». E-mail: lebedevrv@iss-reshetnev.ru.

Сосновский Максим Сергеевич – инженер-программист 3 категории сектора защиты информации; АО «Информационные спутниковые системы» имени академика М.Ф. Решетнева». E-mail: sosnovskiyms@iss-reshetnev.ru.

Shipulin Pavel Mikhailovich – software engineer of the information security sector; JSC Academician M. F. Reshetnev “Information Satellite Systems”. E-mail: pshipulin@gmail.com.

Lebedev Roman Vladimirovich – head of the information security sector; JSC Academician M. F. Reshetnev “Information Satellite Systems”. E-mail: lebedevrv@iss-reshetnev.ru.

Sosnovskiy Maksim Sergeevich – software engineer of the information security sector; JSC Academician M. F. Reshetnev “Information Satellite Systems”. E-mail: sosnovskiyms@iss-reshetnev.ru.
