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.

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 information security data integrity problem relevant for electronic archive management. In high-tech industry large electronic photo archives arise as a part of quality management. Photofixation applied for responsible operations control, documenting 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. These illegal actions can be both the result of an operator's mistake and motivated by intentional 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 allows talking about integrity of the whole photo documents set. One of the most important method characteristic is image format invariability and making additional metadata files unnecessary which allows user to apply standard software for a further work with photo document.

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

Introduction. Currently, photographic recording is a mandatory tool for product quality control in many high-tech industries [1; 2]. It allows documenting the progress of particularly critical operations, recording the state of components at the input and output control, registering non-conformities. As a rule enterprises use the procedure for photographic documentation which has been fixed by industry or internal standards; determines technical requirements for the result of photographic documentation (image file format, resolution, quality, etc.), as well as for the accounting methods, storage and photographic documents handling. To ensure the possibility of photofixation materials' unhindered use by different parties in legal relations (customer and contractor, policyholder and risk insurer), photofixation systems are often organized on the basis of generally accepted technologies and formats. Thus, for example, an archive of photofixation files in practice is often organized on the basis of a file server in the form of a directory structure with identification mechanisms based on the names, attributes and metadata of the image files.

At the stage of placing images in such storages certain threats to the integrity of information arise (property of resistance to unauthorized change [3]): substitution of an image in the storage, reuse of photographic documents [4]. A potential intruder can deliver on these threats both by accident, making mistakes when working with a large number of similar images in a complex storage directory structure, and deliberately while perusing the goal of hiding technological defects by replacing images or saving time for preparing and taking photographs using previously performed images of similar operations.

Frequently the control of such violations is carried out organizationally, while the technical mechanisms at the level of work with the archive management are commonly missing. The authors propose a method for organizing electronic archives of photographic documents and the structure of the information system that provides it (hereinafter - IS), based on the use of steganographic digital watermarks (hereinafter – DWM). DWM are metadata of the image (the survey author, the operation number, the production process marker, etc.), invisibly embedded in the image using an asymmetric key and steganographic transformations (Fig. 1). A DWM consists of a tuple of image metadata and a DWM hash of the previous image, thus a chain of images is formed.

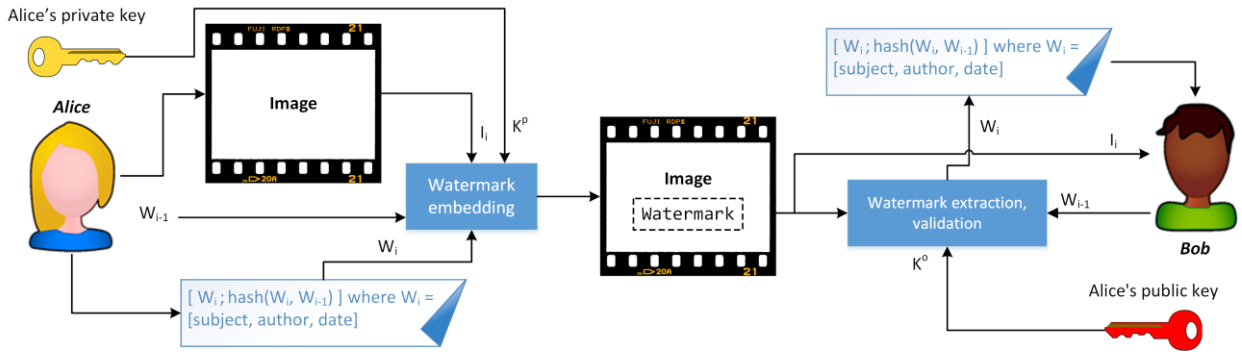

Рис. 1. Процесс встраивания, извлечения и проверки ЦВЗ

Fig. 1. Embedding, extraction and checking processes

Marking of images applying digital watermarking (DWM). Methods for marking DWM images have been actively developing by scientists in recent years; approaches to the classification of methods are proposed in [4–6]. The most promising methods for marking images resistance-wise to noise and invariance to linear transformations (geometric attacks) are moment methods (based on Zernike, Chebyshev, Legendre moments, etc.) [7–11]. The paper [12] proposes a method for marking images of any size with a digital watermark at special points of an image based on Zernike moments.

The proposed method for marking the image of a digital watermark assumes sequential multiple introduction of a digital watermark copy in the surrounding area of each s-th selected singular point in the image. The general scheme of the process of introducing digital watermarks into the image is shown in Fig. 2.

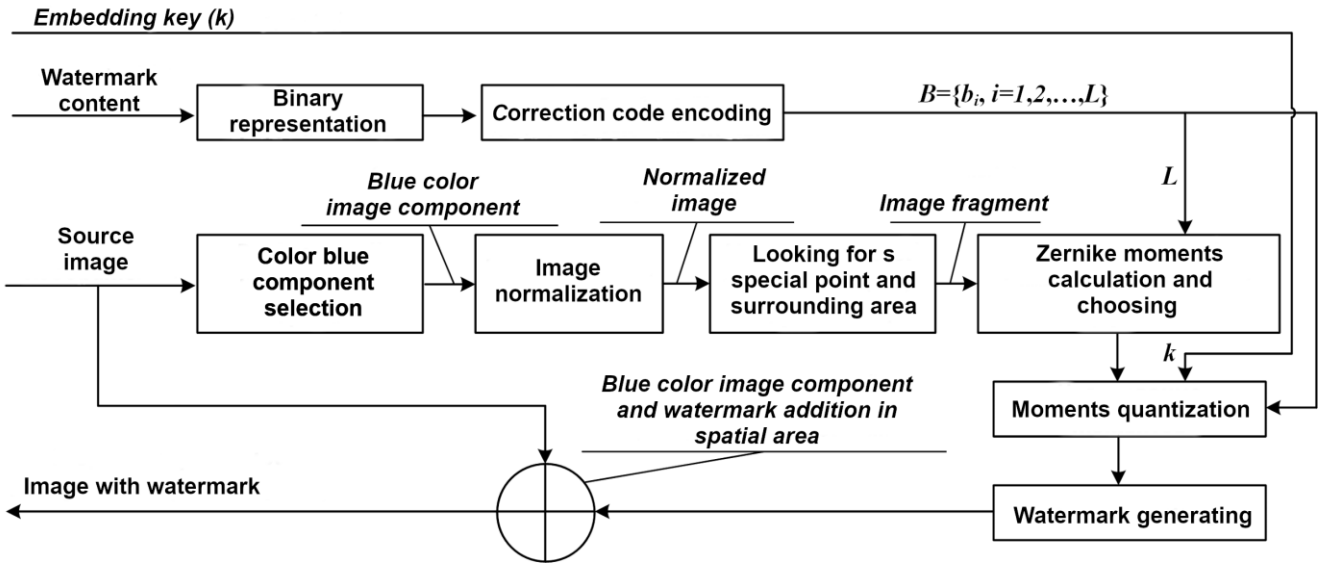

Рис. 2. Общая структурная схема внедрения копии ЦВЗ в изображение

Fig. 2. A watermark copy embedding diagram

The digital watermarking process includes the following stages:

1. Representation of digital watermarks in the form of a binary array B of length L, encoded using corrective coding algorithms (for example, Hamming code)

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

2. Selection of the blue color channel (B-channel) of the RGB model, its normalization to a set of values by $\{0,\ldots,255\}$ function $g(x,y) = \frac{f(x,y) - f_{\min}}{f_{\max} - f_{\min}} \cdot 255$, where $f(x,y)$ – the function of the values of the B-channel at (x,y) image, $f_{\min}$, $f_{\max}$ – are the minimum and maximum values of *f*, respectively.

3. Finding special points of the image by the Shi - Tomasi method [13], calculating coordinates of the surrounding area of special points sized 256x256 pixels.

4. Calculation of the orthogonal moments and the radial Zernike polynomial applying the Kintner method; the choice of suitable moments taking into account the conditions [14–17], formation of the moments' vector $Z_{nm} = \{z_{n_1 m_1}, z_{n_2 m_2}, ..., z_{n_L m_L}\}$.

5. Vector quantization Z_{nm} by a sequence of bits *B*, where each bit of the digital watermark $b_i \in B$ is embedded into the corresponding element $z_{n_i m_i} \in Z_{nm}$ using the modulation function, which performs a pseudo-random change in Zernike moments, adding the following «noise»: $\left|\tilde{z}_{n_i m_i}\right| = \left\lceil \frac{\left|z_{n_i m_i}\right| - d(b_i)}{\Delta} \right\rceil \cdot \Delta + d(b_i)$, where Δ – quantization interval, $d(b_i)$ – dithering function. Quantization interval is a configurable parameter of the system, the value of the dither function depends on the following embedded bit: $d_i(0) \leftarrow random(k) : d_i(0) \in \left[0, \frac{\Delta}{2}\right]$, $d_i(1) = d_i(0) + \frac{\Delta}{2}$. When forming the values, a pseudo-random number generator (PRNG) is involved which is initialized with the key k.

6. Formation of a digital watermarking applying the image reconstruction function

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

where $\varepsilon_{n_i m_i} = \left(\tilde{z}_{n_i m_i} - z_{n_i m_i}\right)$, $\varepsilon_{n_i(-m_i)} = \left(\tilde{z}_{n_i(-m_i)} - z_{n_i(-m_i)}\right)$, $i = 1,2,...,L$, $V_{n_i m_i}$ – the value of the radial Zernike polynomial.

7. Formation of the final image with the DWM by adding a fragment of the original image in the surrounding area of the special s-th point and DWM in the spatial domain $f_s(x,y) = f_s(x,y) + w(x,y)$, где $f_s(x,y)$ – image function in the surrounding of the singular s-th point.

Extraction of the digital watermark from the image is carried out almost similarly to the embedding process and involves a sequential extraction of a digital watermark copy from the surrounding area of each s-th selected singular point in the image. The general block diagram of the process of extracting a digital watermark copy from an image is shown in Fig. 3. After extraction of all digital watermark copies, their correctness is checked with a predetermined threshold and a decision is made whether or not the digital watermark is identified in the image.

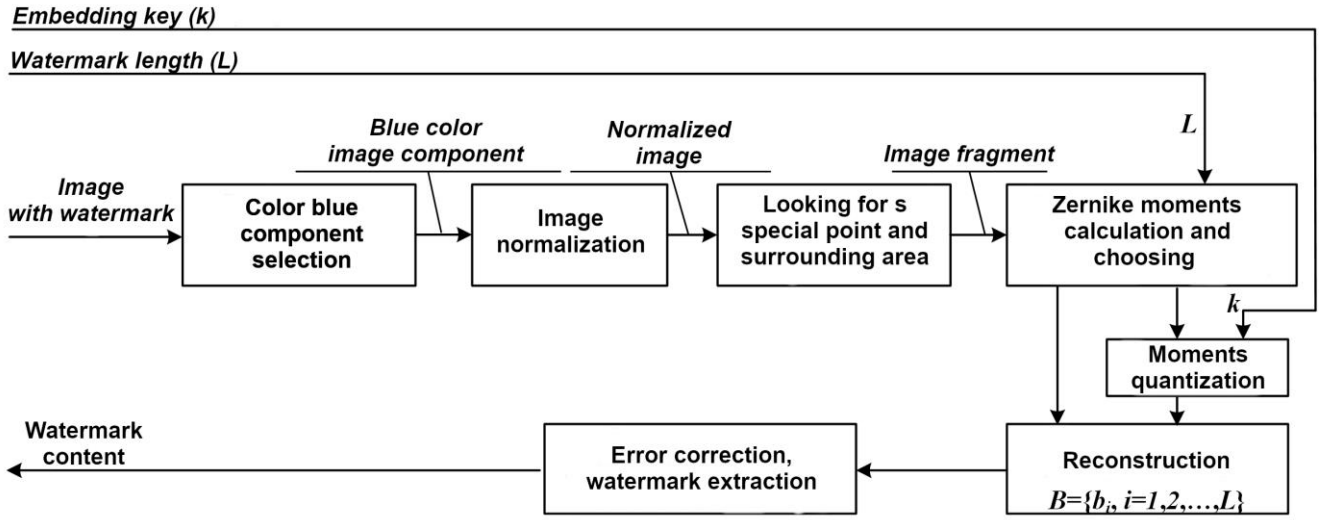

Рис. 3. Общая структурная схема извлечения копии ЦВЗ из изображения

Fig. 2. A watermark-copy extraction diagram

The initial parameters for extracting the digital watermark are the extraction key – k, quantization interval – Δ, the length of the digital watermark sequence – L. The calculation of the special points of the image, their surroundings and the calculation of Zernike moments for them is carried out similarly to the process of embedding the digital watermark. The momentum vector Z_{nm} is quantized twice, first with a sequence of zero and then unit bits. To recover the digital watermark bits $B' = \{b_i' \in \{0,1\}, i = 1,2,\ldots,L\}$ the minimum difference between the calculated moment and the quantized Zernike moment is used, i.e. the detection of the digital watermark bits is carried out by the peaks in the moments' difference:

$$b_i' = \begin{cases} 1, & \text{если } \left(\left|\tilde{z}_{n_i m_i}\right|_1 - \left|z_{n_i m_i}\right|\right)^2 < \left(\left|\tilde{z}_{n_i m_i}\right|_0 - \left|z_{n_i m_i}\right|\right)^2 \\ 0, & \text{в противном случае} \end{cases}, \text{ where } i = 1,2,\ldots,L.$$

After recovering all bits of the digital watermark, they are proofread $B \leftarrow h(B')$ by decoding the correcting code.

The proposed method has a number of advantages in comparison with analogues:

1. High indicators of robustness - invariability of the digital watermark in the majority of noise and geometric attacks on the image (turns, compression, reflections, etc.) [7].
2. Acceptable computational complexity for images of any size is provided by calculating Zernike moments not for the entire image, but only for the surroundings of its characteristic points.

It should be noted that the method is applicable for marking digital watermarks of images with various formats and characteristics, including the most popular one - JPEG.

Diagram of electronic archive organization. The client-server architecture of IS is shown in Fig. 4. Briefly, the algorithm of IS operation can be presented as follows.

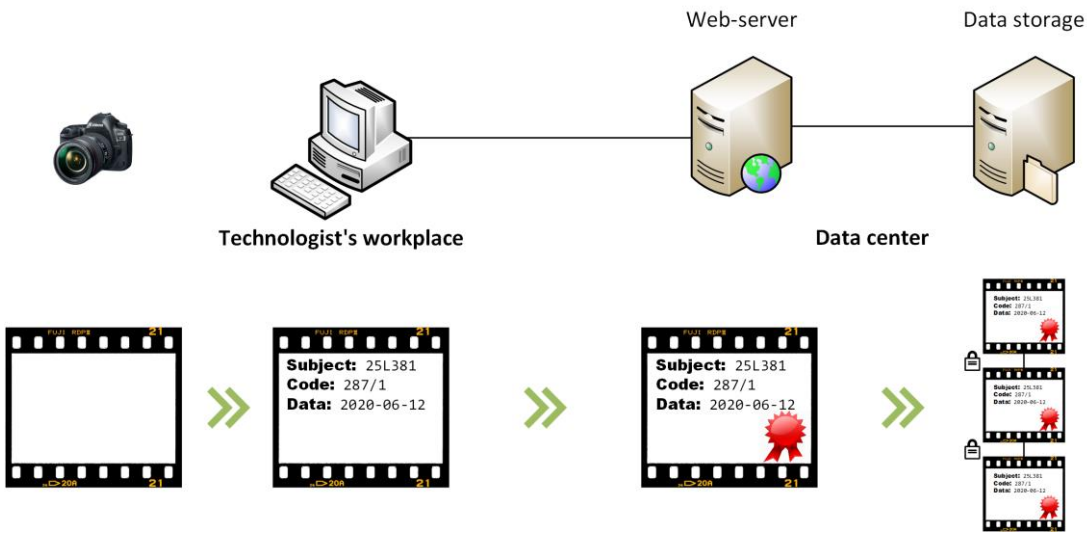

Рис. 4. Функциональная схема ИС учёта фотодокументов

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

Step 1. The assigned person uploads the images to the server via a special software interface, supplying them with the necessary metadata.

Step 2. The server checks the presence of a digital watermark in the image and generates a corresponding digital watermark if the validation is successful.

Step 3. The images are placed in storage, where they are in a linked chain - the continuity of the chain is based on the strength of asymmetric cryptography algorithms.

An attempt to substitute (insert) images inside the storage is excluded, since the digital watermark is a linked chain (see Figure 5). When validating the DWM, the digital watermark metadata of the current image and the hash of the digital watermark of the previous image are fed to the input of the validation subsystem, so that when an attempt to substitute (insert) an image is made, the chain will be broken - either illegal image or legal one following after will not pass the test.

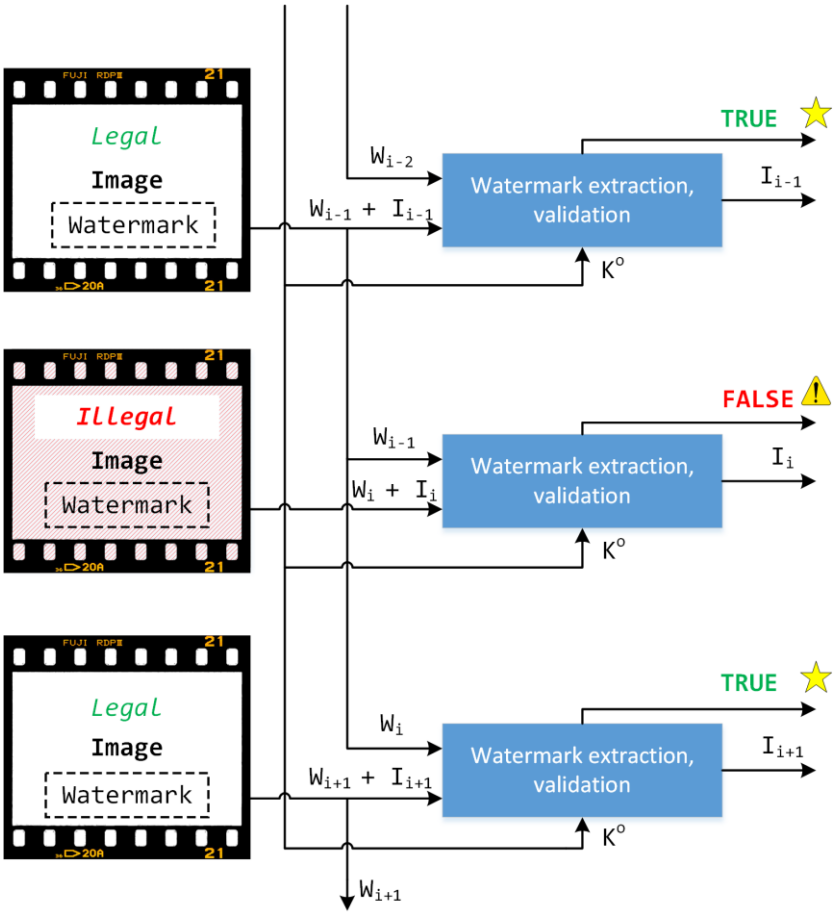

Рис. 5. Попытка нелегального добавления изображения в цепочку

Fig. 5. An illegal image insertion attempt

An attempt to reuse images will be prevented at the stage of uploading an image to the server, since the IS checks the presence of another DWM in the image before generating a new DWM. It is also possible to detect forgery of an image bypassing the operator's software console, since the reused image will have more than one digital watermark.

Conclusion. The proposed method of digital watermarking to organize electronic archives of photographic documents makes it possible to manage photograpfixation materials and ensure reliable protection of the latter from threats of insertion and reuse. When applying the digital watermarking, neither the presentation format of a photo document changes, nor side structures are created in the form of metadata or system files - the file of the photo document remains unchanged both externally for a person and technically, which allows a further work with it in standard software applications.

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 staganography]. 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 kosmonavtiki*. 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 rt 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 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 Mikhaylovich – 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 Sergeyevich – software engineer of the information security sector; JSC Academician M. F. Reshetnev "Information Satellite Systems". E-mail: sosnovskiyms@iss-reshetnev.ru.