УДК 004.056.55:004.932.2
DOI 10.17513/snt.39725

ЗАЩИТА ГРАФИЧЕСКОЙ ИНФОРМАЦИИ ОТ НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ МАРКИРОВАНИЕМ НА ОСНОВЕ МОДУЛЯЦИИ ИНДЕКСА КВАНТОВАНИЯ

[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

Кодирование графической информации с целью обеспечения правомерного использования при визуализации, обработке изображений и многомодальном взаимодействии в социокиберфизических системах очень важно. Методы, основанные на квантовании информации, сегодня широко используются в существующих системах компьютерной графики в составе подсистемы обеспечения информационной безопасности из-за низкой вычислительной сложности и возможности работы в слепом режиме. Выделение требуемых для выполнения встраивания цифрового водяного знака областей на изображении может осуществляться путем анализа и обработки массива яркостной компоненты, для чего в предлагаемом алгоритме структуры графической информации в исходном цветовом пространстве преобразуются в пространство YCbCr. Устойчивость к геометрическим атакам остается одной из самых сложных и актуальных задач в исследованиях защиты графической информации. С целью повышения робастности предлагается использовать преимущества встраивания в частотную область вместе с квантованием индекса модуляции. Результаты экспериментов были проанализированы с использованием типовых показателей оценки эффективности работы алгоритма встраивания стегосообщения на наборе эталонных изображений. На основе проведенного анализа результатов экспериментов обоснована эффективность предлагаемого алгоритма защиты от неправомерного использования структур данных графической информации на основе модуляции индекса квантования.

Ключевые слова: авторское право, дискретное косинусное преобразование, DCT, QIM, модуляция индекса квантования, результат интеллектуальной деятельности, стеганография, скрытие данных, цифровой водяной знак, защита информации

SECURING OF IMAGES FROM UNAUTHORIZED USE BASED ON QUANTIZATION INDEX MODULATION

[1]Zemtsov A.N., [2]Tran Dung Khanh

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

The coding of graphical information to ensure legitimate use in visualization, image processing and multi-modal interaction in socio-cyber-physical systems plays an important role. Methods based on information quantization are widely used today in existing computer graphics systems as part of the information security subsystem due to low computational complexity and the ability to work in blind mode. The selection of areas required for embedding a digital watermark on an image can be carried out by analyzing and processing an array of brightness components, for which, in the proposed algorithm, the structures of graphic information in the original color space are converted to the YCbCr space. Resistance to geometric attacks remains one of the most complex and urgent problems in the study of the protection of graphic information. In order to improve robustness, it is proposed to take advantage of frequency domain embedding along with modulation index quantization. The results of the experiments were analyzed using typical indicators for evaluating the effectiveness of the stego message embedding algorithm on a set of reference images. Based on the analysis of the experimental results, the effectiveness of the proposed algorithm for protecting against misuse of data structures of graphic information based on the modulation of the quantization index is substantiated.

Keywords: copyright, discrete cosine transform, DCT, quantization index modulation, QIM, result of intellectual activity, steganography, data hiding, digital watermark, information security

В связи с быстро меняющейся политической и экономической обстановкой в мире вопросы обеспечения достоверности данных в системах обработки и визуализации графической информации, при многомодальном взаимодействии в социокиберфизических системах, в многомодальных биометрических системах, в том числе с использованием стеганографических методов защиты [1, с. 8; 2, с. 9], построения доверенной вычислительной среды [3, с. 6] становятся особенно актуальными. Типичными приложениями многомодального взаимодействия в социокиберфизических системах являются защита конфиденциальных голосовых данных при передаче [4], защита персональных данных, шифрование изображений, например, в составе медицинской информационной системы хранения и обработки результатов обследований [5], защита прав интеллектуальной собственности при распространении цифровых обучающих материалов [6]

и т.п. Под цифровой стегосистемой в данной работе понимается совокупность методов и средств, используемых для организации скрытого канала передачи цифровых данных в стегоконтейнере [2, с. 10].

Стеганографические методы могут использовать пространственную область стегоконтейнера для защиты от неправомерного использования графической информации [7, 8].

Подобные методы сталкиваются с тем, что биты стегосообщения привязаны к определенному месту в изображении, и существует множество причин, приводящих к потере синхронизации между системой защиты и детектором стегосообщений. Геометрические атаки нарушают синхронизацию, что приводит к некорректному извлечению встроенного стегосообщения. Робастные стегосистемы защиты графической информации должны гарантировать устойчивость и к геометрическим атакам, что обуславливает необходимость встраивания данных в частотной области [9].

По сравнению с пространственными схемами встраивания цифровых водяных знаков, методы на основе встраивания в частотную область более надежны, поскольку водяной знак встраивается путем коррекции коэффициентов спектрального преобразования. Как следствие, для защиты графической информации от неправомерного использования был предложен ряд надежных методов встраивания цифровых водяных знаков, работающих в домене преобразования. Наиболее широко используемыми преобразованиями являются дискретное косинусное преобразование [10], дискретное вейвлет-преобразование [11], дискретное преобразование Фурье [12].

В связи с этим устойчивость к геометрическим атакам остается одной из самых сложных и актуальных задач в исследованиях защиты графической информации. Цель исследования заключается в разработке алгоритма кодирования изображений, позволяющего обеспечить требуемую робастность при низких значениях среднеквадратичной ошибки.

Предлагаемый алгоритм защиты графической информации

Многие методы обработки и визуализации графической информации, в том числе при многомодальном взаимодействии в социокиберфизических системах, традиционно устойчивы к различным типовым операциям, производящимся в промежуточных устройствах и конечных социокиберфизических системах, таким как сжатие с потерей информации, выполнение процедур фильтрации различными алгоритмами обработки изображений, цифро-аналоговые и аналого-цифровые преобразования, кадрирование [13], но менее устойчивы к определенным типам вредоносных атак.

Формат сжатия цифровых изображений JPEG на сегодняшний день является наиболее распространенным форматом кодирования цифровых изображений и представлен на рынке колоссальным количеством как программных, так и аппаратных реализаций. В основе формата сжатия цифровых изображений JPEG лежит одноименный алгоритм, приведенный на рис. 1, который работает как с цифровыми изображениями в режиме оттенков серого, так и с цветными цифровыми изображениями.

Основным в алгоритме JPEG является этап вычисления значений спектральных коэффициентов дискретного косинусного преобразования, которое является разновидностью преобразования Фурье [14]. Дискретное косинусное преобразование относится к спектральным ортогональным декоррелирующим преобразованиям. В результате вычисления такого преобразования получается разложение исходного цифрового изображения по базисным функциям этого ортогонального преобразования.

Предваряет вычисление дискретного косинусного преобразования этап прореживания цветовых компонент, которые разбиваются на блоки размером 8 × 8 пикселей. Для вычисления дискретного косинусного преобразования матрицы значений размером 8 × 8 существует быстрый алгоритм, основанный на умножении матриц. Вычисление дискретного косинусного преобразования производится раздельно для каждой из цветовых компонент *Y*, *Cb* и *Cr*. В случае, когда размеры исходного цифрового изображения не кратны 8, то с целью заполнения недостающих данных добавляется соответствующее количество строк и/или столбцов.

Рис. 1. Алгоритм JPEG

Обозначим через I – исходный или пустой стегоконтейнер, W – цифровой водяной знак, $W = \{\omega_{ij} \mid \omega_{ij} \in \{0,1\}\}$, а I_W – результирующее изображение с внедренным в него цифровым водяным знаком, тогда I_{xy} – значение интенсивности пикселя с координатами x и y, и прямое преобразование запишется в следующем виде:

$$d_{ij} = \frac{1}{4} C_i C_j \sum_{x=0}^{7} \sum_{y=0}^{7} I_{xy} \cos\left(\frac{(2y+1) j\pi}{16}\right) \cos\left(\frac{(2x+1) i\pi}{16}\right), \quad (1)$$

где $C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0 \\ 1, f > 0, & i \geq 0, j \leq 7 \end{cases}$.

В результате вычисления этого ортогонального преобразования получается матрица спектральных коэффициентов d_{ij} размером 8 × 8, величины которых убывают от левого верхнего угла матрицы по направлению к правому нижнему углу, а многие коэффициенты, как показано на рис. 2, либо близки по значению, либо равны нулю.

Рис. 2. Результат вычисления дискретного косинусного преобразования в блоках размером 8 × 8 пикселей

При встраивании в стегоконтейнер цифрового водяного знака необходимо учитывать особенности вычисления декорелирующего преобразования, в том числе дискретного косинусного, когда в низкочастотном спектральном коэффициенте, который располагается в левом верхнем углу каждого блока 8 × 8 пикселей, содержится основная доля информации данного блока.

Функция E_{mb} непосредственно встраивания стегосообщения осуществлялась в алгоритме JPEG на этапе квантования с помощью метода модуляции индекса квантования [15], являющегося одним из популярных методов маркирования графической информации [16]. Основная идея модуляции индекса квантования заключается в изменении квантованного с заданным шагом значения спектрального коэффициента в зависимости от значения бита ω_{ij} стегосообщения W [17].

Использование модуляции индекса квантования в приложениях с цифровыми водяными знаками для защиты авторских прав на графическую информацию с помощью внедрения заданного цифрового водяного знака в структуры данных изображения обеспечивает хороший компромисс высокой полезной нагрузки, уровня искажений и робастности.

Детектор осуществляет сравнение по кодовому расстоянию извлеченного значения со значениями квантователя. Модифицированные с помощью метода модуляции индекса квантования спектральные коэффициенты используются для замены соответствующих исходных коэффициентов d_{ij} в каждом блоке 8 × 8 при выполнении процедуры реконструкции с помощью вычисления обратного преобразования [18] для последующего получения изображения I_W со встроенным цифровым водяным знаком:

$$b_{xy} = \frac{1}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} C_i C_j d_{ij} \cos\left(\frac{(2y+1) j\pi}{16}\right) \cos\left(\frac{(2x+1) i\pi}{16}\right). \quad (2)$$

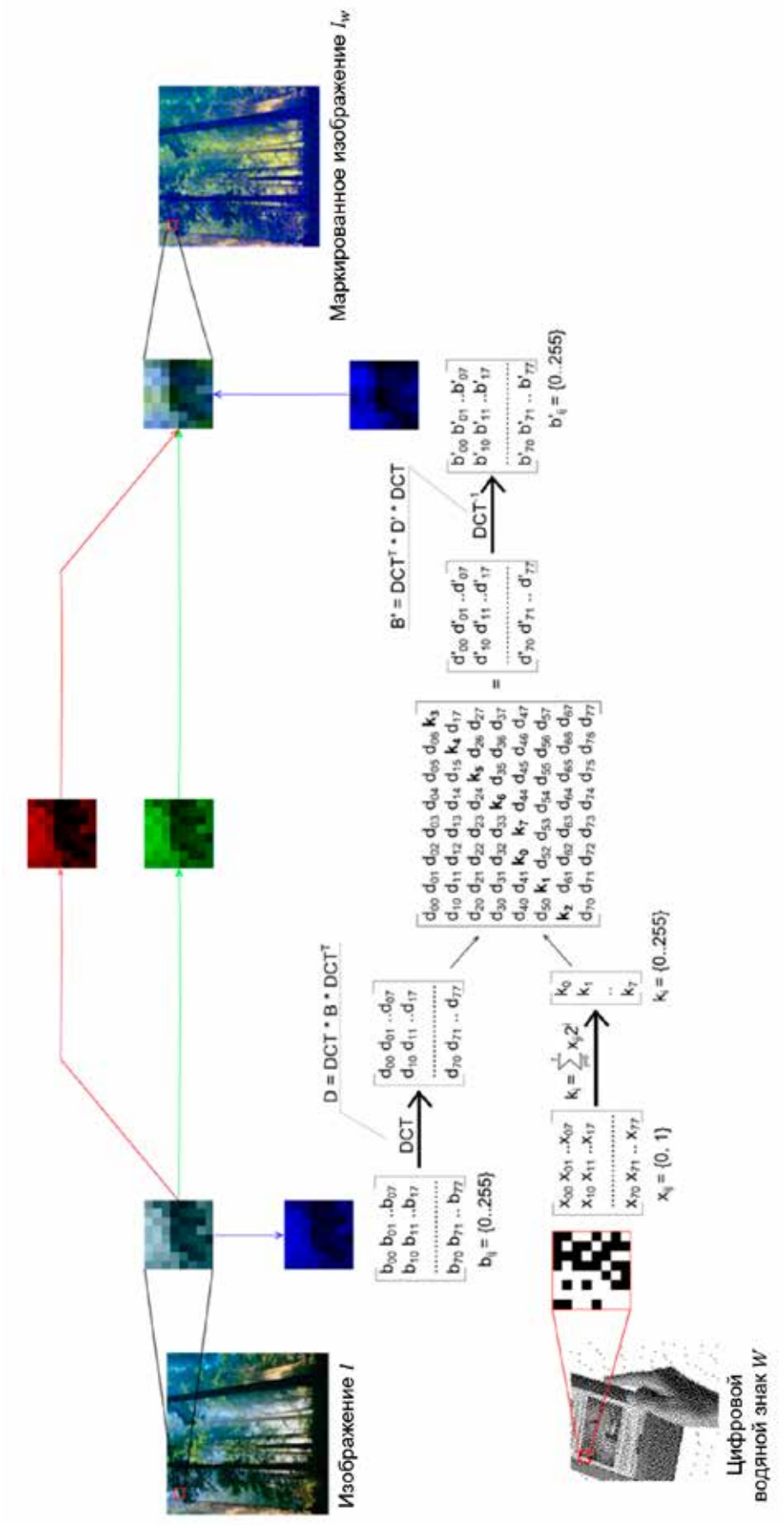

Рис. 3. Схема внедрения стегосообщения в спектральные коэффициенты

На рис. 3 представлена обобщенная схема внедрения данных в спектральные коэффициенты дискретного косинусного преобразования.

Необходимо отметить, что также был разработан вариант реализации, совместимый со стандартизованными декодерами, когда для выделения требуемых для выполнения встраивания цифрового водяного знака областей на изображении осуществляется путем анализа и обработки массива яркостной компоненты, для чего в предлагаемом алгоритме структуры графической информации в исходном цветовом пространстве *RGB* производится преобразование в пространство *YCbCr* [19]:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.29900000 & 0.58700000 & 0.11400000 \\ -0.16873600 & -0.33126400 & 0.50000000 \\ 0.50000000 & -0.4186680 & -0.08131200 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}, \quad (3)$$

где в *Y* хранится яркостная компонента, в *Cb* и *Cr* кодируются, соответственно, синяя и красная цветоразностные компоненты.

Обратное преобразование из цветового пространства *YCbCr* в исходное пространство *RGB* осуществляется умножением вектора *YCbCr* на обратную матрицу:

$$\begin{vmatrix} R \\ G \\ B \end{vmatrix} = \begin{vmatrix} 1 & 0 & 1.402 \\ 1 & -0.34414 & -0.71414 \\ 1 & 1.772 & 0 \end{vmatrix} \cdot \begin{vmatrix} Y \\ C_b - 128 \\ C_r - 128 \end{vmatrix}. \quad (4)$$

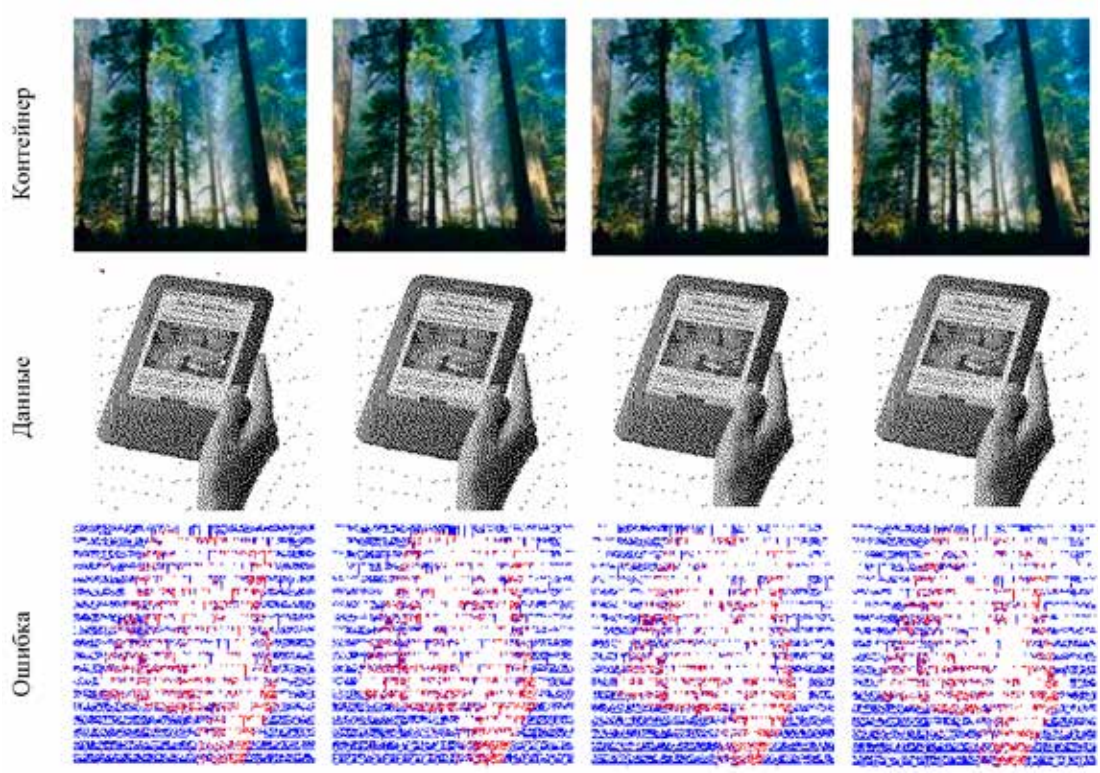

Рис. 4. Результаты встраивания и извлечения цифровых водяных знаков

Результаты экспериментов

Для любого метода защиты цифровых изображений от неправомерного использования важно, чтобы встраивание стегоданных в структуры данных графической информации не вызывало значительного ухудшения их качества, и в то же время встраивание должно характеризоваться достаточной надежностью извлечения, чтобы выдерживать злонамеренные атаки, а также типовую обработку данных, производящуюся в промежуточных и конечных устройствах.

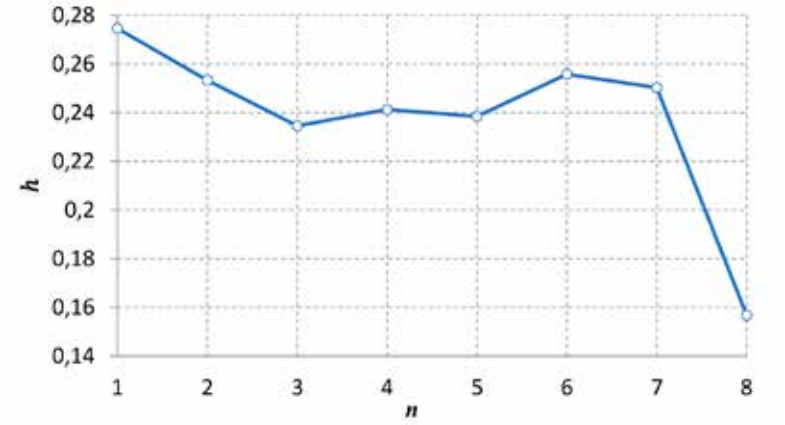

Рис. 5. Зависимость h от n

Защита графической информации от неправомерного использования маркированием в частотной области неизбежно приводит к искажению исходного стегоконтейнера. Оценка искажений особенно важна в силу того, что может дать подсказки для повышения эффективности использования водяных знаков. Кроме того, оценка искажений является мерой противодействия злонамеренным скрытым сетевым взаимодействиям.

В результате проведения исследования было установлено, что наличие стегосообщения, встроенного с помощью метода модуляции индекса квантования, может быть обнаружено на основе анализа гистограмм коэффициентов. Примеры результатов встраивания и извлечения маркированием графической информации стегоданными в частотной области представлены на рис. 4.

На рис. 5 показана зависимость коэффициента битовых ошибок h от места встраивания n. Емкость встраивания составила от одного бита до 8 битов на блок 8 × 8 пикселей. Встраивая более одного бита в блок пикселей, можно увеличить емкость встраивания, но в этом случае робастность будет меньше. Необходимо отметить, что при проведении экспериментов в качестве меры искажений, вносимых в структуру графической информации алгоритмом кодирования, были использованы принятые в теории связи показатели, такие как среднее квадратическое отклонение

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

и пиковое отношение сигнала к шуму

$$PSNR = 10\log_{10}\left(N_1 N_2 \frac{\max\limits_{x,y} I_{x,y}^2}{\sum_{x,y}\left(I_{x,y} - I_{Wx,y}\right)^2}\right)$$ [20].

Размеры N_1 и N_2 исследуемого исходного изображения I указаны в пикселях, $I_{x,y}$ – яркость пикселя с координатами x,y в исходном изображении, $I_{Wx,y}$ – яркость пикселя в модифицированном изображении.

В случае геометрических атак нарушаются границы блоков 8 × 8 пикселей, что приводит к существенному искажению матриц спектральных коэффициентов дискретного косинусного преобразования и резкому увеличению количества битовых ошибок, особенно с увеличением емкости встраиваемого цифрового водяного знака.

Заключение

Предложен алгоритм защиты графической информации от неправомерного использования в частотной области на основе метода модуляции индекса квантования с высокой полезной нагрузкой и достаточной робастностью. Алгоритм целесообразно использовать в приложениях и сервисах, ориентированных на хранение, обработку и передачу цифровых изображений, при реализации правомерного доступа к которым представляется вероятным нарушение права собственности на цифровые изображения. Дополнительно было установлено, что стегосообщения, внедренные в спектральные коэффициенты дискретного косинусного преобразования с помощью метода модуляции индекса квантования, чувствительны к подмешиванию данных. Подмешиваемые данные сглаживают специфичные искажения гистограммы изображения, являющиеся следствием процесса квантования с помощью метода модуляции индекса квантования, существенно искажающего гистограммы спектральных коэффициентов. С помощью анализа гистограммы спектральных коэффициентов можно обнаружить присутствие в стегоконтейнере данных, встроенных с помощью метода модуляции индекса

квантования. Кроме того, при подмешивании данных стегосообщение полностью стирается с незначительным ухудшением или без ухудшения качества изображения.

Список литературы

1. Коржик В.И., Красов А.В. Цифровая стеганография: учебник. М.: ООО «КноРус». 2023. 324 с.

2. Земцов А.Н. Методы цифровой стеганографии для защиты авторских прав: монография. Saarbrucken: LAP Lambert, 2012. 148 с.

3. Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д.В. Построение доверенной вычислительной среды: монография. СПб.: ИП Петрив Роман Богданович, 2019. 108 с.

4. Земцов А.Н. Робастный метод стеганографической защиты звуковых данных // Известия Волгоградского государственного технического университета. 2011. № 11 (84). С. 138–140.

5. 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.

6. Земцов А.Н. Стеганографические алгоритмы в электронном обучении // Информационные технологии. Радиоэлектроника. Телекоммуникации. 2012. № 2–2. С. 112–118.

7. Wang H., Su Q. A color image watermarking method combined QR decomposition and spatial domain // Multimedia Tools and Applications. 2022. Vol. 81. P. 37895–37916.

8. Земцов А.Н., Чан Зунг Хань. Защита графической информации от неправомерного использования маркированием в пространственной области // Современные наукоемкие технологии. 2022. № 12–2. С. 211–216.

9. Gupta S., Saluja K., Solanki V., Kaur K., Singla P., Shahid M. Efficient methods for digital image watermarking and information embedding. Measurement: Sensors. 2022. Vol. 24. DOI: 10.1016/j.measen.2022.100520.

10. Wang Y., Luo Y., Wang Z., Pan H. A Hidden DCT-Based Invisible Watermarking Method for Low-Cost Hardware Implementations // Electronics. 2021. Vol. 10, Is. 12. DOI: 10.3390/electronics10121465.

11. Annadurai C., Nelson I., Devi K.N., Manikandan R., Gandomi A.H. Image Watermarking Based Data Hiding by Discrete Wavelet Transform Quantization Model with Convolutional Generative Adversarial Architectures // Applied Sciences. 2023. Vol. 13, Is. 2. DOI: 10.3390/app13020804.

12. Cedillo-Hernandez M., Cedillo-Hernandez A., Garcia-Ugalde F.J. Improving DFT-Based Image Watermarking Using Particle Swarm Optimization Algorithm // Mathematics. 2021. Vol. 9, Is. 15. DOI: 10.3390/math9151795.

13. 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.

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

15. Chen B., Wornell G.W. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding // IEEE Trans. Inf. Theory. 2001. Vol. 47. P. 1423–1443.

16. Yu X., Wang C., Zhou X. A Survey on Robust Video Watermarking Algorithms for Copyright Protection // Applied Sciences. 2018. Vol. 8, Is. 10. DOI: 10.3390/app8101891.

17. Wu Z., Li R., Yin P., Li C. Steganalysis of Quantization Index Modulation Steganography in G.723.1 Codec // Future Internet. 2020. Vol. 12, Is. 1. DOI: 10.3390/fi12010017.

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

19. 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. Vol. 1303. P. 1303–1309.

20. Panwar P., Dhall S., Gupta S. A multilevel secure information communication model for healthcare systems // Multimedia Tools and Applications. 2021. Vol. 80. P. 8039–8062.