УДК 004.056.5

А.С. Мельман, П.О. Петров, А.А. Шелупанов, А.В. Аристов, Ю.П. Похолков

Встраивание информации в JPEG-изображения с маскировкой искажений в частотной области

Стеганография позволяет обеспечивать конфиденциальность информации за счёт организации скрытых каналов передачи данных. Однако эффективность стеганографической защиты информации напрямую зависит от незаметности вложения как для глаза человека, так и для методов стегоанализа. В статье предлагается подход к решению проблемы уязвимости популярного метода встраивания QIM к статистическому стегоанализу. Для этого предлагается использовать переменный шаг квантования, который адаптивно выбирается для каждого блока изображения-контейнера в формате JPEG. Результаты экспериментов демонстрируют повышение уровня безопасности стеганографического встраивания за счёт применения предложенного подхода.

Ключевые слова: защита информации, стеганография, стегоанализ, цифровые изображения, JPEG.
doi: 10.21293/1818-0442-2020-23-4-45-50

Цифровая стеганография – одно из актуальных направлений информационной безопасности. Методами цифровой стеганографии может быть создан скрытый канал передачи данных для обеспечения их конфиденциальности. Скрытие данных выполняется путём их встраивания в цифровые объекты.

Большое количество стеганографических алгоритмов работает с цифровыми изображениями. Обмен изображениями в Интернете в настоящее время является привычным делом, что позволяет без лишних подозрений передавать секретную информацию. Данное исследование также фокусируется на сокрытии информации в цифровых изображениях. В качестве контейнеров для секретных сообщений рассматриваются JPEG-изображения, поскольку большое количество изображений хранится и передаётся в сети именно в формате JPEG.

Стеганографическое встраивание должно быть незаметным, в том числе и для методов стегоанализа. Поэтому целью настоящей работы является разработка алгоритма сокрытия данных, обеспечивающего незаметность встраивания. В работе предлагается адаптивный алгоритм встраивания информации в сжатые JPEG-изображения, основанный на известном стеганографическом методе модуляции индекса квантования (QIM) и позволяющий снизить уязвимость встраивания к стегоанализу.

Обзор литературы

Методы стеганографического сокрытия информации в цифровых изображениях принято разделять на пространственные и частотные. Пространственные методы [1, 2] оперируют непосредственно значениями пикселей изображения. В основе многих подобных методов лежит замена младших битов битами секретного сообщения. Частотные методы предусматривают встраивание фрагментов сообщения в коэффициенты, полученные в результате некоторого частотного преобразования, например, дискретного косинусного преобразования (ДКП) [3, 4], дискретного вейвлет-преобразования [5, 6] и др.

Популярность метода сжатия JPEG позволяет выделять исследования, посвящённые сокрытию данных в JPEG-изображениях, в отдельное большое направление в рамках частотного встраивания. Отметим несколько подобных работ последних лет.

Многие алгоритмы для JPEG-стеганографии используют оценку стоимости искажений различных коэффициентов, т.е. влияния вносимых изменений на итоговое изображение. Например, в работе [7] предлагается алгоритм сокрытия данных в JPEG-изображениях, в котором для оценки стоимости искажений используются статистические характеристики в пространственной области.

Распространённым приёмом повышения эффективности встраивания является выбор местоположения битов сообщения в контейнере в зависимости от его характеристик. В статье [8] предлагается при заполнении контейнера отдавать предпочтение блокам с меньшим количеством нулевых коэффициентов. Авторы [9] используют сдвиг гистограммы для сокрытия информации в JPEG-изображениях. Биты сообщения встраиваются в высокочастотные коэффициенты, а наилучшее местоположение для встраивания определяется пороговым значением.

Многие алгоритмы для JPEG-изображений являются обратимыми, т.е. позволяют восстановить контейнер после извлечения сообщения. Например, в [10] представлен алгоритм, отличающийся оригинальным подходом к выбору коэффициентов ДКП, изменение которых приводит к меньшему искажению изображения-контейнера при встраивании. Другой пример обратимого встраивания в изображения JPEG представлен в [11]. В этом случае авторы предлагают использовать нулевые коэффициенты ДКП для встраивания, чтобы увеличить емкость.

Таким образом, разработка алгоритмов встраивания данных в JPEG-изображения является актуальной и активно исследуется в настоящее время.

Сжатие по методу JPEG

Рассмотрим метод сжатия JPEG подробнее. JPEG является одним из наиболее популярных методов сжатия изображений с потерями. Уменьшение размера файла происходит за счёт удаления из изображения некоторой части избыточной информации.

Этапами JPEG-сжатия являются преобразование цветового пространства изображения к виду

YCbCr, «прореживание» каналов Cb и Cr, ДКП, квантование и кодирование. С точки зрения сокрытия данных наибольший интерес представляют этапы ДКП и квантования.

После применения ДКП к матрице значений пикселей изображения (преобразование выполняется блоками 8×8) получается матрица того же размера, элементами которой являются частотные коэффициенты. Коэффициент в левом верхнем углу называется DC-коэффициентом, остальные коэффициенты – AC-коэффициентами. Наиболее значимая информация содержится в низкочастотных (ближе к верхнему левому углу) коэффициентах. Средне- и высокочастотные (ближе к нижнему правому углу) коэффициенты менее важны для последующего восстановления изображения, поэтому именно они чаще всего используются для встраивания дополнительной информации.

Непосредственно сжатие информации происходит на этапе квантования. При этом коэффициенты ДКП делят на определённые значения из матрицы квантования, зависящей от выбранной степени сжатия. Результат деления округляется, в результате чего происходит необратимая потеря информации.

Некоторые алгоритмы сокрытия данных в JPEG-изображениях изменяют коэффициенты ДКП до квантования либо совмещают встраивание с процедурой квантования, например алгоритм [12]. Однако в большинстве случаев изменениям подвергаются уже квантованные AC-коэффициенты. В данной работе реализован именно этот подход.

Метод встраивания QIM

Метод QIM [13] является одним из известных методов встраивания информации в цифровые изображения. Его основная идея заключается в изменении элемента данных изображения (значения пикселя либо частотного коэффициента) в зависимости от значения бита секретного сообщения. Изменяемое число делится на заранее определённый коэффициент, а затем округляется. Этот коэффициент называется шагом квантования q. Формула встраивания бита сообщения b_i при этом имеет вид

$$c' = q \cdot \left\lfloor \frac{c}{q} \right\rfloor + \frac{q}{2} \cdot b_i, \qquad (1)$$

где c – коэффициент ДКП до встраивания, c' – коэффициент ДКП после встраивания, b_i – бит секретного сообщения, $\lfloor ... \rfloor$ – целая часть от деления.

Извлечение выполняется по формуле

$$b_i' = \arg\min_{p \in [0,1]} \left| c'' - c_p' \right|, \qquad (2)$$

где c'' – коэффициент ДКП, содержащий бит сообщения, $c_0'' = q \cdot \left\lfloor \frac{c''}{q} \right\rfloor$, $c_1'' = q \cdot \left\lfloor \frac{c''}{q} \right\rfloor + \frac{q}{2}$.

Эффективность встраивания в значительной степени зависит от величины шага квантования. Чем больше значение q, тем больше устойчивость встраивания к искажениям стегоизображения, но больше уязвимость к стегоанализу, в том числе даже визуальному.

Адаптивный выбор шага квантования

Встраивание информации в JPEG-изображения по методу QIM существенно искажает гистограммы квантованных AC-коэффициентов. На рис. 1 представлены примеры гистограмм до (см. рис. 1, *а*) и после (см. рис. 1, *б*) встраивания информации в JPEG-изображение. Очевидно, что данные гистограммы существенно отличаются. Гистограмма, представленная на рис. 1, *б*, содержит характерные «провалы», поскольку из-за применения формулы (1) частота возникновения отдельных значений AC-коэффициентов меняется.

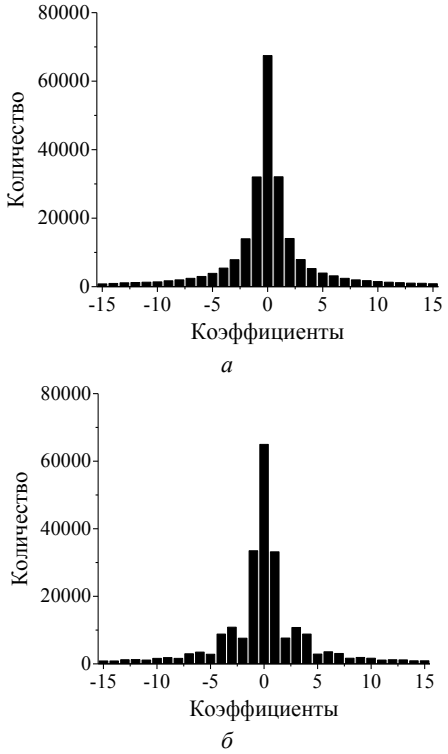

Рис. 1. Гистограммы AC-коэффициентов: *а* – до встраивания; *б* – после встраивания

Эта проблема является характерной для классического метода QIM. Для решения этой проблемы можно использовать переменный шаг квантования для каждого блока изображения. Например, в работе [12] подобный подход позволяет обеспечить статистическую незаметность встраивания. Серьёзным недостатком такого решения является необходимость использования некоторой дополнительной информации при встраивании. В частности, в данном случае речь идёт о вспомогательных последовательностях для генерации шагов квантования. Передача такой информации отдельно от стегоизображения создаёт угрозу обнаружения вложения, поскольку она привлечёт внимание злоумышленника и проинформирует его о наличии скрытого канали передачи данных. Также в случае, когда дополнительная информация уникальна для каждой пары контейнер – вложение, при каждом сеансе связи необходимо

решать проблему её защиты, например шифрованием. В этом случае использование стеганографии становится нецелесообразным, поскольку удобнее применять шифрование к самому секретному сообщению.

Отметим, что передача фиксированной ключевой информации не представляет такой же серьёзной проблемы, поскольку выбирается единожды для группы собеседников.

В работе [14] одного из авторов настоящего исследования было предложено решение, лишённое данного недостатка. Для выбора шага квантования предлагалось использовать часть ДКП-коэффициентов блока, не использовавшихся для сокрытия сообщения (для несжатых изображений). Шаг квантования определяется как наименьший из наименее часто встречаемых коэффициентов по области невстраивания. Область невстраивания – это диапазон коэффициентов, которые не изменяются при встраивании информации. Область встраивания – это диапазон коэффициентов, которые будут изменены. Области встраивания и невстраивания в блоке коэффициентов ДКП представлены на рис. 2.

Рис. 2. Области встраивания и невстраивания в блоке коэффициентов ДКП

В данной работе для выбора шага квантования для каждого блока JPEG-изображения также предлагается выбирать наименьшее значение квантованного AC-коэффициента по области невстраивания из самых редких. Это позволит перераспределить «провалы» на гистограмме и повысить безопасность встраивания. Такой выбор шага квантования обладает двумя преимуществами. Во-первых, это делает встраивание адаптивным, т.е. учитывающим особенности конкретного контейнера. Во-вторых, это позволяет не передавать дополнительную информацию, уникальную для каждого случая встраивания и служащую демаскирующим вложение признаком.

Опишем последовательность этапов встраивания информации в JPEG-изображения:

1. Открыть изображение-контейнер в формате JPEG, восстановить массив квантованных коэффициентов ДКП.

2. Последовательно обходя блоки квантованных коэффициентов, выполнить следующее:

2.1. Определить значение шага квантования q как наименьшее значение из самых редких по области невстраивания.

2.2. Отделить от секретного сообщения фрагмент, равный количеству коэффициентов в области встраивания, т.е. 10 битов.

2.3. Встроить фрагмент сообщения в блок по формуле (1) с шагом квантования q, определённым на шаге 2.1.

3. Осуществить кодирование коэффициентов и сформировать стегоизображение.

При извлечении информации биты сообщения извлекаются по формуле (2) из области встраивания после предварительного вычисления шага квантования q по области невстраивания. Поскольку область невстраивания не изменяется при сокрытии секретного сообщения, значение q при извлечении совпадает со значением q при встраивании и встроенные данные извлекаются без каких-либо ошибок.

Результаты экспериментов

Для оценки эффективности встраивания были выполнены вычислительные эксперименты. Для экспериментов использовались 10 стандартных изображений из базы USC-SIPI [15] с разрешениями 512×512, таких как «Airplane», «Lena» и др. Каждое изображение было сжато в JPEG-формат с качеством 95.

На рис. 3 представлен усреднённый по всей выборке изображений график зависимости показателя пиковое отношение сигнала к шуму (PSNR), используемого для численной оценки визуального качества стегоизображений, от ёмкости встраивания. Метрика PSNR вычисляется по формуле

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{255}{\mathrm{RMSE}}\right), \qquad (3)$$

где $\mathrm{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(P_i - Q_1\right)^2}$; n – общее количество пикселей; P_i – значение пикселя контейнера; Q_i – значение пикселя стегоизображения.

Стеганографическое встраивание считается незаметным, если величина PSNR составляет 30–35 дБ, предложенный алгоритм обеспечивает необходимый уровень качества. При этом достигается приемлемый уровень максимальной ёмкости около 50 000 битов.

На рис. 4 представлен график зависимости коэффициента структурного сходства (SSIM) для аналогичных значений ёмкости. Метрика SSIM вычисляется по формуле (4). Даже при максимальном объёме вложения величина SSIM близка к единице, что говорит о полной незаметности вложения.

$$\mathrm{SSIM} = \frac{\left(2\mu_c\mu_s + K_1\right)\cdot\left(2\sigma_{cs} + K_2\right)}{\left(\mu_c^2 + \mu_s^2 + K_1\right)\cdot\left(\sigma_c^2 + \sigma_s^2 + K_2\right)}, \qquad (4)$$

где μ_c – среднее значение пикселей контейнера; μ_s – среднее значение пикселей стегоизображения; σ_c^2 – дисперсия пикселей контейнера; σ_s^2 – дисперсия пикселей стегоизображения; σ_{cs} – ковариация пикселей обоих изображений; K_1 и K_2 – константы.

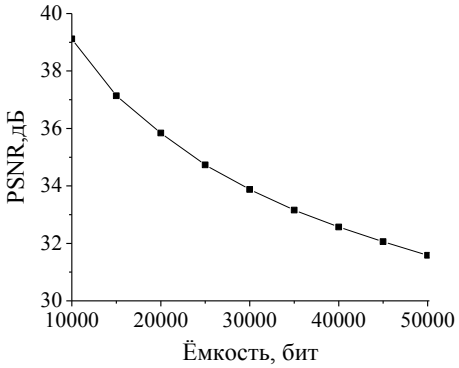

Рис. 3. Зависимость PSNR от ёмкости

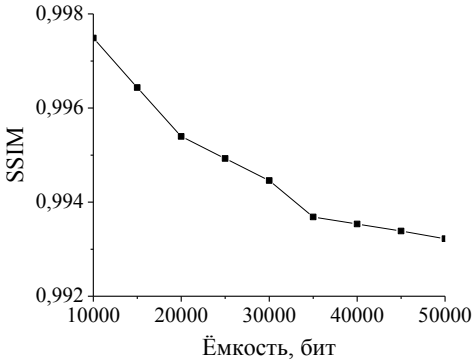

Рис. 4. Зависимость SSIM от ёмкости

Рисунок 5 показывает, как выглядит гистограмма ДКП-коэффициентов стегоизображения после встраивания по описанному алгоритму. Сравнивая рис. 1, *б* и рис. 5 очевидно, что адаптивный выбор шага квантования позволил избежать существенных искажений гистограммы.

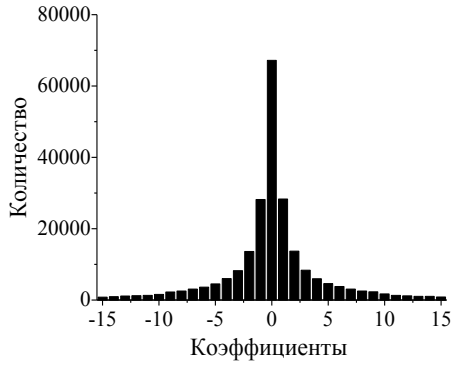

Рис. 5. Гистограмма АС-коэффициентов стегоизображения при переменном шаге квантования

Была также исследована устойчивость встраивания к методу стегоанализа, основанному на законе Бенфорда. Согласно закону Бенфорда, для реальных величин вероятность цифры $x \neq 0$ располагается на первом месте в числе тем выше, чем меньше эта цифра. Эта вероятность выражается формулой

$$P(x) = \log_{10}\left(1+\frac{1}{x}\right). \qquad (5)$$

В работе [16] предлагается применять данный закон для цифр квантованных коэффициентов ДКП. Для принятия решения о том, содержит ли некоторое изображение стеганографическое вложение, необходимо сравнить реальное распределение вероятностей с теоретическим. Если отклонение рассчитанных величин от теоретических превышает некоторый порог, изображение считается содержащим встроенную информацию.

На рис. 6 представлена гистограмма, отражающая вероятности возникновения различных цифр на первом месте чисел квантованных АС-коэффициентов. По данной гистограмме видно, что увеличение разброса значений шага квантования не оказывает существенного влияния на распределение вероятности по сравнению с малым фиксированным значением (q = 3). Метод стегоанализа, предложенный в работе [16], сравнивает фактическую вероятность для цифры «2» с фиксированным пороговым значением. Результаты экспериментов с новым алгоритмом показали, что во всех случаях стегоанализатор не обнаружил наличие вложения.

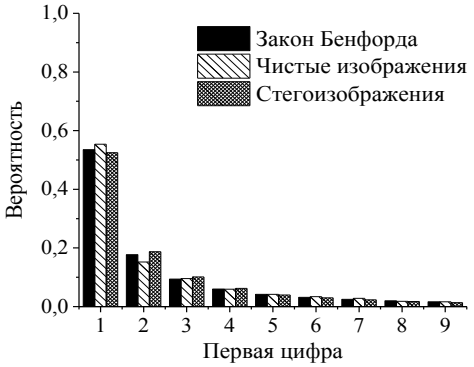

Рис. 6. Вероятности возникновения различных цифр на первом месте чисел квантованных АС-коэффициентов

Заключение

В работе был предложен и исследован алгоритм стеганографического встраивания информации в сжатые JPEG-изображения на основе метода QIM. Отличительной особенностью предложенного алгоритма является адаптивный выбор шага квантования в зависимости от конкретного изображения-контейнера. Результаты экспериментов показывают не только высокие значения метрик визуального качества PSNR и SSIM, но и устойчивость к анализу гистограмм, а также к стегоанализу на основе закона Бенфорда.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУРа на 2020–2022 гг. (проект № FEWM-2020-0037).

Литература

1. Image steganography in spatial domain: A survey / M. Hussain, A.W.A. Wahab, Y.I.B. Idris, A.T.S. Ho, K.-H. Jung // Signal Processing: Image Communication. – 2018. – Vol. 65. – P. 46–66.

2. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research / I.J. Kadhim, P. Premaratne, P.J. Vial, B. Halloran // Neurocomputing. – 2019. – Vol. 335. – P. 299–326.

3. Biswas R. Random selection based GA optimization in 2D-DCT domain color image steganography / R. Biswas, S.K. Bandyapadhay // Multimedia Tools and Applications. – 2020. – Vol. 79, No. 11. – P. 7101–7120.

4. A steganographic approach for secure communication of medical images based on the DCT-SVD and the compressed sensing (CS) theory / R. Thanki, S. Borra, V. Dwivedi, K. Borisagar // The Imaging Science Journal. – 2017. – Vol. 65, No. 8. – P. 457–467.

5. Miri A. Adaptive image steganography based on transform domain via genetic algorithm / A. Miri, K. Faez // Optik. – 2017. – Vol. 145. – P. 158–168.

6. Fakhredanesh M. Steganography in discrete wavelet transform based on human visual system and cover model / M. Fakhredanesh, M. Rahmati, R. Safabakhsh // Multimedia Tools and Applications. – 2019. – Vol. 78. – P. 18475–18502.

7. Liu G. Designing adaptive JPEG steganography based on the statistical properties in spatial domain / G. Liu, F. Huang, Z. Li // Multimedia Tools and Applicatios. – 2019. – Vol. 78. – P. 8655–8665.

8. Улучшенный алгоритм встраивания информации в сжатые цифровые изображения на основе метода PM1 / О.О. Евсютин, А.С. Кокурина, А.А. Шелупанов, И.И. Шепелев // Компьютерная оптика. – 2015. – Т. 39, № 4. – С. 572–581.

9. A High-Imperceptibility and Histogram-Shifting Data Hiding Scheme for JPEG Images / Y. Li, S. Yao, K. Yang, Y. Tan, Q. Zhang // IEEE Access. – 2019. – Vol. 7. – P. 73573–73582.

10. Reversible data hiding in JPEG image based on DCT frequency and block selection / D. Hou, H. Wang, W. Zhang, N. Yu // Signal Processing. – 2018. – Vol. 148. – P. 41–47.

11. Reversible data hiding in JPEG images based on zero coefficients and distortion cost function / F. Di, M. Zhang, F. Huang, J. Liu, Y. Kong // Multimedia Tools and Applications. – 2019. – Vol. 78, No. 24. – P. 34541–34561.

12. Noda H. Application of QIM with dead zone for histogram preserving JPEG steganography / H. Noda, M. Niimi, E. Kawaguchi // Proceedings of the IEEE International Conference on Image Processing. – Italy, Genova, 2005. – P. 1082–1085.

13. Митекин В.А. Алгоритмы встраивания информации на основе QIM, стойкие к статистической атаке / В.А. Митекин, В.А. Федосеев // Компьютерная оптика. – 2018. – Т. 42, № 1. – С. 118–127.

14. A new approach to reducing the distortion of the digital image natural model in the DCT domain when embedding information according to the QIM method / O.O. Evsutin, A.S. Melman, R.V. Meshcheryakov, A.O. Ishakova // CEUR Workshop Proceedings. – 2019. – Vol. 2485. – P. 268–272.

15. The USC-SIPI image database [Электронный ресурс]. – Режим доступа: http://sipi.usc.edu/database/ (дата обращения: 17.08.2020).

16. Andriotis P. JPEG steganography detection with Benford's Law / P. Andriotis, G. Oikonomou, T. Tryfonas // Digital Investigation. – 2013. – Vol. 9. – P. 246–257.

Мельман Анна Сергеевна
Аспирант каф. безопасности информационных систем (БИС) Томского государственного ун-та
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, д. 40, г. Томск, Россия, 634050
ORCID 0000-0001-6444-7774
Тел.: +7-923-434-11-18
Эл. почта: annakokurina94@yandex.ru

Петров Павел Олегович
Студент каф. комплексной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Ленина пр-т, д. 40, г. Томск, Россия, 634050
Тел.: +7-960-912-94-04
Эл. почта: 725_ppo@fb.tusur.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, зав. каф. КИБЭВС ТУСУРа
Ленина пр-т, д. 40, г. Томск, Россия, 634050
ORCID: 0000-0003-2393-6701
Тел.: +7 (382-2) 90-71-55, внут. 10-20
Эл. почта: saa@fb.tusur.ru

Аристов Анатолий Владимирович
Д-р техн. наук, профессор Инженерной школы энергетики Национального исследовательского
Томского политехнического университета (НИ ТПУ)
Ленина пр-т, д. 30, г. Томск, Россия, 634050
Тел.: +7 (382-2) 56-32-55
Эл. почта: aristovav@tpu.ru

Похолков Юрий Петрович
Д-р техн. наук, профессор, рук. учебно-научного центра «Организация и технологии высшего профессионального образования» НИ ТПУ
Ленина пр-т, д. 30, г. Томск, Россия, 634050
Тел.: +7 (382-2) 60-62-81
Эл. почта: pyp@tpu.ru

Melman A.S., Petrov P.O., Shelupanov A.A.,
Aristov A.V., Pokholkov Y.P.

Embedding information into JPEG images with distortion masking in frequency domain

Steganography allows to ensure the confidentiality of information by organizing covert data transmission channels. However, the effectiveness of steganographic information protection directly depends on the invisibility of a secret message, both for the human eye and for steganalysis methods. The paper proposes an approach that allows solving the problem of vulnerability of the popular QIM embedding method to statistical steganalysis. For this, it is proposed to use a variable quantization step, which is adaptively selected for each block of the JPEG cover image. The experimental results demonstrate an increase in the security level of steganographic embedding due to the application of the proposed approach.

Keywords: information security, steganography, steganalysis, digital images, JPEG.
doi: 10.21293/1818-0442-2020-23-4-45-50

References

1. Hussain M., Wahab A.W.A., Idris Y.I.B., Ho A.T.S., Jung K.-H. Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, 2018, vol. 65, pp. 46–66.

2. Kadhim I.J., Premaratne P., Vial P.J., Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, 2019, vol. 335, pp. 299–326.

3. Biswas R., Bandyapadhay S.K. Random selection based GA optimization in 2D-DCT domain color image steganography. *Multimedia Tools and Applications*, 2020, vol. 79, no. 11, pp. 7101–7120.

4. Thanki R., Borra S., Dwivedi V., Borisagar K. A steganographic approach for secure communication of medical images based on the DCT-SVD and the compressed sensing

(CS) theory. *The Imaging Science Journal*, 2017, vol. 65, no. 8, pp. 457–467.

5. Miri A., Faez K. Adaptive image steganography based on transform domain via genetic algorithm. *Optik*, 2017, vol. 145, pp. 158–168.

6. Fakhredanesh M., Rahmati M., Safabakhsh R. Steganography in discrete wavelet transform based on human visual system and cover model. *Multimedia Tools and Applications*, 2019, vol.78, pp. 18475–18502.

7. Liu G., Huang F., Li Z. Designing adaptive JPEG steganography based on the statistical properties in spatial domain. *Multimedia Tools and Applications*, 2019, vol. 78, pp. 8655–8665.

8. Evsutin O.O., Kokurina A.S., Shelupanov A.A., Shepelev I.I. An improved algorithm for data hiding in compressed digital images based on PM1 method. *Computer Optics*, 2015, vol. 39, no. 4, pp. 572–581 (in Russ.).

9. Li Y., Yao S., Yang K., Tan Y., Zhang Q. A High-Imperceptibility and Histogram-Shifting Data Hiding Scheme for JPEG Images. *IEEE Access*, 2019, vol. 7, pp. 73573–73582.

10. Hou D., Wang H., Zhang W., Yu N. Reversible data hiding in JPEG image based on DCT frequency and block selection. *Signal Processing*, 2018, vol. 148, pp. 41–47.

11. Di F., Zhang M., Huang F., Liu J., Kong Y. Reversible data hiding in JPEG images based on zero coefficients and distortion cost function. *Multimedia Tools and Applications*, 2019, vol. 78, no. 24, pp. 34541–34561.

12. Noda H., Niimi M., Kawaguchi E. Application of QIM with dead zone for histogram preserving JPEG steganography. *Proceedings of the IEEE International Conference on Image Processing*, 2005, pp. 1082–1085.

13. Mitekin V.A., Fedoseev V.A. New secure QIM-based information hiding algorithms. *Computer Optics*, 2018, vol. 42, no. 1, pp. 118–127 (in Russ.).

14. Evsutin O.O., Melman A.S., Meshcheryakov R.V., Ishakova A.O. A new approach to reducing the distortion of the digital image natural model in the DCT domain when embedding information according to the QIM method. *CEUR Workshop Proceedings*, 2019, vol. 2485, pp. 268–272.

15. The USC-SIPI image database. Available at: http://sipi.usc.edu/database/ (Accessed: August 17, 2020).

16. Andriotis P. JPEG steganography detection with Benford's Law / P. Andriotis, G. Oikonomou, T. Tryfonas // Digital Investigation, 2013, vol. 9, pp. 246–257.

Anna S. Melman
Postgraduate student, Department of Information Systems Security, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID 0000-0001-6444-7774
Phone: +7-923-434-11-18
Email: annakokurina94@yandex.ru

Pavel O. Petrov
Student, Department of Complex Information Security of Computer Systems, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-960-912-94-04
Email: 725_ppo@fb.tusur.ru

Alexander A. Shelupanov
Doctor of Engineering Sciences, Professor,
Head of Department of Complex Information Security of Computer Systems TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0003-2393-6701
Phone: +7 (382-2) 90-71-55, ext. 10-20
Email: saa@fb.tusur.ru

Anatoly V. Aristov
Doctor of Engineering Sciences,
National Research Tomsk Polytechnic University (NR TPU)
30, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 56-32-55
Email: aristovav@tpu.ru

Yuri P. Pokholkov
Doctor of Engineering Sciences, Professor,
Head of Educational and Scientific Center «Organization and Technologies of Higher Professional Education» NR TPU
30, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 60-62-81
Email: pyp@tpu.ru