

УДК: 004.9

Эффективное и безошибочное сокрытие информации в гибридном домене цифровых изображений с использованием метаэвристической оптимизации

А. С. Мельман^а, О. О. Евсютин

Национальный исследовательский университет «Высшая школа экономики»,
Россия, 101000, г. Москва, ул. Мясницкая, 20

E-mail: ^а amelman@hse.ru

Получено 01.11.2022.

Принято к публикации 23.12.2022.

Сокрытие информации в цифровых изображениях является перспективным направлением кибербезопасности. Методы стеганографии обеспечивают незаметную передачу данных по открытому каналу связи втайне от злоумышленника. Эффективность встраивания информации зависит от того, насколько незаметным и робастным является скрытое вложение, а также от емкости встраивания. Однако показатели качества встраивания являются взаимно обратными и улучшение значения одного из них обычно приводит к ухудшению остальных. Баланс между ними может быть достигнут с помощью применения метаэвристической оптимизации. Метаэвристики позволяют находить оптимальные или близкие к ним решения для многих задач, в том числе трудно формализуемых, моделируя разные природные процессы, например эволюцию видов или поведение животных. В этой статье предлагается новый подход к сокрытию данных в гибридном пространственно-частотном домене цифровых изображений на основе метаэвристической оптимизации. В качестве операции встраивания выбрано изменение блока пикселей изображения в соответствии с некоторой матрицей изменений. Матрица изменений выбирается адаптивно для каждого блока с помощью алгоритмов метаэвристической оптимизации. В работе сравнивается эффективность трех метаэвристик, таких как генетический алгоритм (ГА), оптимизация роя частиц (ОРЧ) и дифференциальная эволюция (ДЭ), для поиска лучшей матрицы изменений. Результаты экспериментов показывают, что новый подход обеспечивает высокую незаметность встраивания, высокую емкость и безошибочное извлечение встроенной информации. При этом хранение и передача матриц изменений для каждого блока не требуются для извлечения данных, что уменьшает вероятность обнаружения скрытого вложения злоумышленником. Метаэвристики обеспечили прирост показателей незаметности и емкости по сравнению с предшествующим алгоритмом встраивания данных в коэффициенты дискретного косинусного преобразования по методу QIM [Evsutin, Melman, Meshcheryakov, 2021] соответственно на 26,02 % и 30,18 % для ГА, на 26,01 % и 19,39 % для ОРЧ, на 27,30 % и 28,73 % для ДЭ.

Ключевые слова: стеганография, цифровые изображения, метаэвристическая оптимизация, генетический алгоритм, дифференциальная эволюция, оптимизация роя частиц

Данная работа является результатом исследовательского проекта, реализуемого в рамках Программы фундаментальных исследований Национального исследовательского университета «Высшая школа экономики».

UDC: 004.9

Efficient and error-free information hiding in the hybrid domain of digital images using metaheuristic optimization

A. S. Melman^a, O. O. Evsutin

National Research University Higher School of Economics,
20 Myasnitskaya st., Moscow, 101000, Russia

E-mail: ^a amelman@hse.ru

Received 01.11.2022.

Accepted for publication 23.12.2022.

Data hiding in digital images is a promising direction of cybersecurity. Digital steganography methods provide imperceptible transmission of secret data over an open communication channel. The information embedding efficiency depends on the embedding imperceptibility, capacity, and robustness. These quality criteria are mutually inverse, and the improvement of one indicator usually leads to the deterioration of the others. A balance between them can be achieved using metaheuristic optimization. Metaheuristics are a class of optimization algorithms that find an optimal, or close to an optimal solution for a variety of problems, including those that are difficult to formalize, by simulating various natural processes, for example, the evolution of species or the behavior of animals. In this study, we propose an approach to data hiding in the hybrid spatial-frequency domain of digital images based on metaheuristic optimization. Changing a block of image pixels according to some change matrix is considered as an embedding operation. We select the change matrix adaptively for each block using metaheuristic optimization algorithms. In this study, we compare the performance of three metaheuristics such as genetic algorithm, particle swarm optimization, and differential evolution to find the best change matrix. Experimental results showed that the proposed approach provides high imperceptibility of embedding, high capacity, and error-free extraction of embedded information. At the same time, storage of change matrices for each block is not required for further data extraction. This improves user experience and reduces the chance of an attacker discovering the steganographic attachment. Metaheuristics provided an increase in imperceptibility indicator, estimated by the PSNR metric, and the capacity of the previous algorithm for embedding information into the coefficients of the discrete cosine transform using the QIM method [Evsutin, Melman, Meshcheryakov, 2021] by 26.02% and 30.18%, respectively, for the genetic algorithm, 26.01% and 19.39% for particle swarm optimization, 27.30% and 28.73% for differential evolution.

Keywords: steganography, digital images, metaheuristic optimization, genetic algorithm, differential evolution, particle swarm optimization

Citation: *Computer Research and Modeling*, 2023, vol. 15, no. 1, pp. 197–210 (Russian).

This work is an output of a research project implemented as part of the Basic Research Program at the National Research University Higher School of Economics (HSE University).

1. Введение

Стремительная цифровизация различных видов деятельности ставит новые задачи перед разработчиками методов и средств защиты цифровых данных, в том числе цифровых изображений и видео. Во многих приложениях защита таких данных от несанкционированного доступа или неправомерного использования не должна мешать удобству пользователя и требовать выполнения дополнительных действий при обращении к контенту. В этих условиях эффективным решением проблемы обеспечения безопасности может стать незаметное внедрение дополнительной информации в цифровые изображения с помощью методов стеганографии и водяных знаков.

Методы цифровой стеганографии [Dhawan, Gupta, 2021] скрывают некоторую секретную информацию, например медицинские данные или другие конфиденциальные данные, в цифровой контейнер для последующей безопасной передачи по незащищенному каналу связи. Зная подходящий алгоритм извлечения и секретный ключ, законный пользователь может успешно извлечь встроенную информацию. При этом сам факт наличия какого-либо сообщения в контейнере остается тайной для злоумышленника. Методы цифровых водяных знаков [Егорова, Федосеев, 2019] добавляют специальные метки к цифровому контенту, позволяющие впоследствии подтвердить авторство на контент, проверить целостность и подлинность цифрового объекта. По аналогии со стеганографическим встраиванием такие метки обычно невидимы невооруженным глазом и могут быть обнаружены только при использовании программных средств.

Незаметность встраивания дополнительной информации является важным критерием эффективности алгоритмов сокрытия данных в цифровых изображениях. В первую очередь это актуально для стеганографического встраивания, поскольку потенциальный злоумышленник не должен даже подозревать о существовании скрытого канала передачи данных. В случае водяных знаков незаметность встраивания обеспечивает корректное восприятие исходного контента зрителем, а также не нарушает работу алгоритмов интеллектуальной обработки изображений, например распознавания образов. Другим важным критерием эффективности встраивания является емкость — количество информации, которое может быть скрыто в цифровом объекте. Робастность характеризует устойчивость извлечения данных. Встроенная информация должна извлекаться без искажений, если изображение с вложением не подвергалось дополнительной обработке. Это особенно важно в том случае, если в качестве секретного сообщения выступала сжатая или зашифрованная информация.

Перечисленные показатели качества являются взаимно обратными, и улучшение значения одного из них обычно приводит к ухудшению остальных. Баланс между незаметностью, емкостью и робастностью встраивания может быть достигнут с помощью алгоритмов метаэвристической оптимизации, моделирующих различные природные процессы, например эволюцию видов или поведение животных. Однако эффективность применения таких алгоритмов может существенно отличаться для разных операций встраивания и доменов встраивания. Поэтому целью этого исследования являются разработка нового подхода к встраиванию информации в цифровые изображения с использованием метаэвристической оптимизации и сравнение эффективности нескольких метаэвристик для повышения качества встраивания.

2. Обзор литературы

Методы сокрытия данных в цифровых изображениях разделяют на методы сокрытия в пространственной области и методы сокрытия в частотной области (в зависимости от того, какие элементы данных изменяются при встраивании). Пространственные методы работают в основном с пикселями изображений [Alhomoud, 2021], а частотные методы работают с коэффициентами частотных преобразований, таких как дискретное косинусное преобразование (ДКП) [Yuan

et al., 2020], дискретное вейвлет-преобразование (ДВП) [Giri et al., 2020], дискретное преобразование Фурье (ДПФ) [Fares, Amine, Salah, 2020] и другие. Основным преимуществом пространственного встраивания является низкая вычислительная сложность, в то время как вычислительно затратное частотное встраивание обычно отличается большей робастностью.

В последние годы исследователи нередко комбинируют обработку изображений в пространственной и частотной области. Некоторые схемы встраивают разные водяные знаки в разные домены изображений [Rakhmawati, Suwadi, Wirawan, 2020]. Однако в некоторых случаях работа с элементами частотной области выполняется без реального выполнения частотного преобразования. Отметим примеры таких исследований.

В основе алгоритма [Su, Chen, 2018] лежит вычисление DC-коэффициентов ДКП. Исходный квадратный бинарный водяной знак делят на четыре равные части и к каждой из получившихся частей применяют перемешивающее преобразование. В данном случае используется алгоритм псевдослучайной перестановки, основанный на хеш-функции MD5. Авторы применяют DC-коэффициенты, полученные в пространственной области, для контроля силы изменений блока пикселей. Похожий принцип реализован в исследованиях [Parah et al., 2018; Ali et al., 2020].

Другой пример описан в статье [Su et al., 2019]. Авторы предлагают внедрять водяной знак путем квантования пикселей цифрового изображения. Предварительно к каждой битовой плоскости ЦВЗ применяется преобразование Арнольда для повышения безопасности. Особенностью алгоритма является вычисление DC-коэффициентов ДПФ без выполнения реального ДПФ для сокращения времени работы алгоритма. DC-коэффициенты используются для вычисления границ квантования и получения новых значений пикселей.

В [Yuan et al., 2021] представлена слепая схема водяных знаков, использующая уникальные характеристики DC-коэффициентов ДКП и дискретного преобразования Хартли без реального выполнения данных преобразований.

Еще один подобный алгоритм описан в [Su et al., 2020]. Он основан на вычислении первого низкочастотного коэффициента ДВП в пространственной области.

Анализ актуальных исследований показал, что сокрытие данных в гибридном домене позволяет, с одной стороны, отказаться от вычислительно затратных операций перехода из одного домена в другой, с другой — сохранить присущую частотному домену устойчивость встраивания. Поэтому в этой работе также предлагается алгоритм в гибридном пространственно-частотном домене. В следующем разделе описаны соответствующие операции встраивания и извлечения данных и дана формальная постановка задачи.

3. Предлагаемый подход

Предлагаемый подход основан на методе модуляции индекса квантования (QIM) [Chen, Wornell, 2001]. Основным параметром метода QIM является шаг квантования q , который регулирует силу встраивания. При встраивании элементы данных изображения, например коэффициенты ДКП, квантуются в зависимости того, какой бит (ноль или единицу) сообщения необходимо встроить. Формула встраивания имеет вид

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

где c — это коэффициент ДКП до встраивания, c' — это коэффициент ДКП после встраивания, b_i — бит сообщения.

На этапе извлечения выполняется моделирование процедуры встраивания значений 0 и 1 в коэффициент ДКП и решение принимается в зависимости от разности между коэффициентом

после такого пробного встраивания и реальным значением. Формула извлечения бита выглядит следующим образом:

$$b_i = \arg \min_{p \in [0, 1]} |c'' - c'_p|, \tag{2}$$

где c'' — это коэффициент ДКП, содержащий встроенный бит; c'_p — это коэффициент ДКП после пробного встраивания.

Ранее в статье [Evsutin, Melman, Meshcheryakov, 2021] был предложен адаптивный алгоритм стеганографического встраивания информации в коэффициенты ДКП по методу QIM. Настоящая работа развивает некоторые идеи предшествующего исследования. Алгоритм [Evsutin, Melman, Meshcheryakov, 2021] скрывает биты сообщения в среднечастотных ДКП-коэффициентах блоков изображения размером 8×8 . Его отличительной особенностью является безошибочное извлечение встроенной информации. Это значит, что все биты, извлеченные из изображения, совпадают с соответствующими битами, встроенными в это изображение. Данное свойство обеспечивается благодаря методу итеративного исправления ошибок, который позволяет добиться безошибочности в большинстве случаев, но требует значительного числа переходов из пространственной области в частотную и обратно.

В качестве альтернативного метода в настоящем исследовании предлагается заменить квантование коэффициентов ДКП на прямое изменение значений пикселей изображения в пространственной области. Для этого необходимо сгенерировать матрицу изменений, каждый элемент которой соответствует одному из пикселей блока изображения-контейнера и принимает целое значение из отрезка $[-k; k]$. Тогда встраивание фрагмента информации в блок изображения будет выполняться путем небольших изменений всех исходных значений пикселей. Данная идея проиллюстрирована на рис. 1.

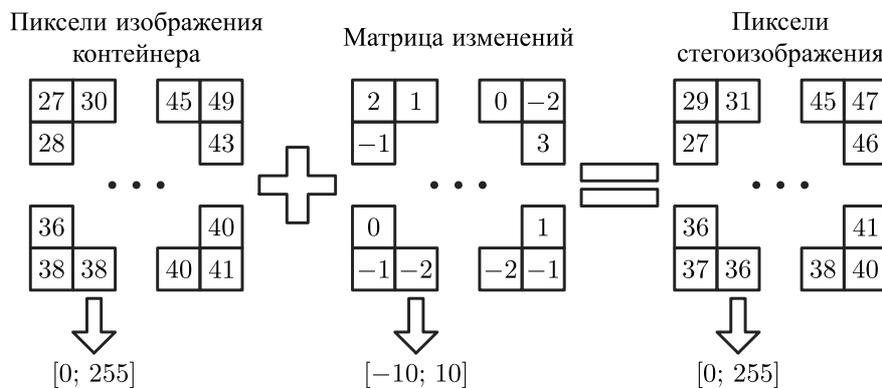


Рис. 1. Новая операция встраивания при $k = 10$

Чтобы обеспечить соответствие между элементами стегоизображения и секретного сообщения, матрица изменений должна быть адаптивно выбрана для каждого блока изображения и фрагмента секретного сообщения. Извлечение выполняется по формуле (2) из среднечастотных коэффициентов ДКП блока. Если вся встроенная информация была извлечена корректно, происходит переход к следующему блоку изображения. Если извлеченное сообщение не соответствует фрагменту информации, который должен быть скрыт в блоке, происходит корректировка матрицы изменений, и далее следует новая попытка встроить и извлечь информацию. Иллюстрация данной идеи представлена на рис. 2.

Таким образом, определим формальную постановку задачи. Пусть P — это цифровое изображение с разрешением $N_1 \times N_2$ и M — двоичная последовательность, подлежащая встраиванию. Разделим M на подпоследовательности M_1, M_2, \dots, M_L и представим P в виде множества парно непересекающихся квадратных блоков P_1, P_2, \dots, P_L размером $n \times n$. Необходимо найти

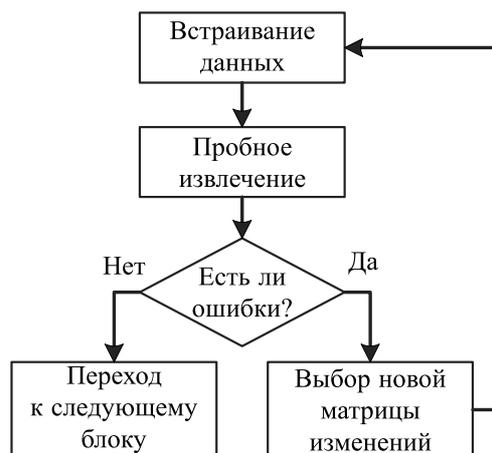


Рис. 2. Схема сокрытия данных с помощью матрицы изменений

для каждого из данных блоков матрицу изменений D_i такую, что

$$F[\text{DCT}(P'_i)] = M_i,$$

где F — функция извлечения по методу QIM, DCT — дискретное косинусное преобразование блока данных размером $n \times n$ и $P'_i = P_i + D_i$, $(p'_i)_{uv} \in [0; 255]$, $(d_i)_{uv} \in [-k; k]$.

Стоит отметить, что биты встраиваемой информации не используются непосредственно при встраивании, но используются при построении матрицы изменений. Процесс генерации матрицы изменений будет рассмотрен подробнее в следующем разделе статьи.

Важным условием эффективной работы предложенного метода является выбор подходящей матрицы изменений для каждого блока пикселей. Такая матрица должна не только обеспечивать безошибочное извлечение встроеной информации, но также приводить к наименьшим искажениям стегоизображения. Очевидно, что случайный выбор такой матрицы может привести к полному перебору вариантов, что является вычислительно сложной задачей. Поэтому хорошим решением, позволяющим соблюсти баланс между эффективностью встраивания и вычислительной сложностью, является применение алгоритмов метаэвристической оптимизации.

4. Метаэвристическая оптимизация

Оптимизация направлена на выбор наилучшего решения из множества вариантов в условиях определенных ограничений. В большинстве прикладных задач пространство решений проблемы слишком велико для полного перебора вариантов [Akyol, Alatas, 2017]. Метаэвристическая оптимизация представляет собой класс оптимизационных алгоритмов, позволяющих находить решения таких задач за приемлемое время с помощью механизма направленного поиска. Метаэвристические алгоритмы или метаэвристики не гарантируют нахождение оптимального решения, но во многих задачах выбор близкого к оптимальному решения является хорошим компромиссом между качеством оптимизации и вычислительной сложностью.

Существует большое количество различных метаэвристик, отличающихся разными особенностями. В этом исследовании мы анализируем эффективность трех классических метаэвристик, таких как генетический алгоритм (ГА), дифференциальная эволюция (ДЭ) и оптимизация роя частиц (ОРЧ), для обеспечения эффективного встраивания информации в гибридный частотно-пространственный домен цифровых изображений.

Данные метаэвристики имеют схожий принцип работы. Множество возможных решений задачи оптимизации называется популяцией. В данном исследовании каждая особь популяции

соответствует одному из возможных вариантов матрицы изменений. Для каждой особи популяции вычисляется соответствующее значение целевой функции. В процессе оптимизации особи популяции подвергаются различным изменениям в соответствии с конкретной метаэвристикой. Особь, соответствующая лучшему значению целевой функции после заданного числа поколений оптимизации, становится итоговым решением.

ГА [Goldberg, 1989] — это один из наиболее известных эволюционных алгоритмов. Он моделирует процесс естественного отбора в природе, и отдельная особь популяции отождествляется с хромосомой. Формирование нового поколения особей выполняется путем применения операций кроссовера и мутации с вероятностями p_{cross} и p_{mut} соответственно. Операция кроссовера представляет собой получение новых особей путем совмещения частей хромосом двух различных особей текущей популяции. Мутация изменяет выбранный случайным образом ген полученной в результате кроссовера особи.

ДЭ [Storn, Price, 1997] также относится к вдохновленным природой эволюционным алгоритмам. В ходе выполнения алгоритма каждая особь подвергается скрещиванию с другой случайно выбранной особью с вероятностью DE_{cross} . Перед выполнением скрещивания родительская особь подвергается мутации по формуле

$$\vec{x} = \vec{x}_1 + \alpha \times (\vec{x}_2 - \vec{x}_3),$$

где \vec{x}_1 , \vec{x}_2 и \vec{x}_3 — это случайно выбранные особи популяции, α определяет силу мутации.

Алгоритм ОРЧ [Kennedy, Eberhart, 1995] был вдохновлен поведением стай птиц. В отличие от ГА и ДЭ, на начальном этапе ОРЧ необходимо сгенерировать не саму популяцию особей, а их местоположения и скорости. На каждой итерации определяется лучшее известное положение каждой частицы по отдельности и всего роя частиц в целом. Они используются для вычисления новых значений скорости частиц. Скорость частицы изменяется по формуле

$$\vec{s} = w\vec{s} + c_1\vec{r}_p \times (\vec{x}_p - \vec{x}) + c_2\vec{r}_g \times (\vec{x}_g - \vec{x}),$$

где \vec{r}_p и \vec{r}_g — случайные векторы, w , c_1 и c_2 — параметры алгоритма, \vec{x}_p — лучшее положение частицы, \vec{x}_g — лучшее положение роя в целом.

Положение частицы изменяется по следующей формуле:

$$\vec{x} = \vec{x} + \vec{s}.$$

В данном исследовании предлагается подход к применению метаэвристической оптимизации для повышения эффективности стеганографического встраивания.

Для ускорения сходимости и уменьшения различий между блоками контейнера и стегоизображения начальная популяция генерируется следующим образом. Сначала выполняется встраивание фрагмента информации в среднечастотные ДКП-коэффициенты блока изображения I по формуле (1) и формируется пробный блок пикселей стегоизображения S^{try} . Каждая особь популяции IND формируется по следующему правилу:

$$IND_i = \begin{cases} r_1, & \text{если } r_2 > \delta, \\ DIF_i, & \text{если иначе,} \end{cases}$$

где r_1 — случайное целое число, $r_1 \in [-k; k]$, r_2 — случайное вещественное число, $r_2 \in [0; 1]$, δ — значение вероятности, $DIF_i = S_i^{try} - I_i$.

Эффективность метаэвристической оптимизации напрямую зависит от конструкции целевой функции. В данном исследовании она конструируется таким образом, чтобы обеспечить

наилучшее визуальное качество стегоизображения при полностью безошибочном извлечении встроенной информации. Целевая функция максимизируется в процессе оптимизации.

Для оценки незаметности встраивания используется стандартная метрика «пиковое отношение сигнала к шуму» (PSNR):

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right),$$

$$MSE = \frac{1}{8 \times 8} \sum_{i=1}^{8 \times 8} (I_i - S_i)^2,$$

где I_i — это пиксель оригинального изображения, S_i — это пиксель стегоизображения.

Для оценки количества ошибок используется метрика Bit Correct Rate (BCR), которая вычисляется по следующей формуле:

$$BCR = 1 - \frac{B_{er}}{B_{block}}, \quad (3)$$

где B_{block} — это общая емкость блока, B_{er} — это количество неправильно извлеченных битов.

Безошибочному извлечению информации соответствует значение $BCR = 1$. Чтобы обеспечить безошибочное извлечение данных, используется дополнительная проверка после завершения всех поколений оптимизации. Если итоговое значение целевой функции превышает значение 1, значит, был найден безошибочный вариант. В противном случае блок изображения подвергается процедуре обработки пустого блока, которая включает в себя повторную оптимизацию для встраивания дополнительного бита в заранее заданный коэффициент ДКП, который соответствует метке «пропустить блок» при извлечении.

Составная целевая функция представляет собой сумму величин $PSNR$ и BCR . Чтобы итоговое значение целевой функции превышало 1 только при полном отсутствии ошибок, необходимо использовать весовой коэффициент для значения $PSNR$. При одной ошибке выражение (3) дает значение 0,9677. $PSNR$ блока стегоизображения составляет в среднем около 30–50 дБ. Следовательно, чтобы суммарное значение не превышало 1 при наличии 1 ошибки, необходимо дополнительно ввести весовой коэффициент, равный 10^{-4} .

Тогда целевая функция выглядит следующим образом:

$$f = 10^{-4} PSNR + BCR.$$

Общая схема нового алгоритма представлена на рис. 3.

5. Результаты экспериментов и обсуждение

Для экспериментов использовались 8 стандартных изображений из базы [SIPI Image Database, 2022], таких как Airplane, Baboon и т. д. Все изображения полутоновые и имеют размер 512×512 пикселей.

Размер популяции составил 128 особей во всех экспериментах. Число поколений оптимизации равно 300. Размерность задачи соответствует размеру блока изображения и равна 64. Вероятность δ равна 0,8. Эксперименты повторялись по 20 раз. Для каждого блока изображения использовался разный шаг квантования q . Соответствующая последовательность значений q рассматривается как секретный ключ. Параметр $k = 10$.

Рис. 4 иллюстрирует выбор значений параметров для ГА. Рис. 4, а демонстрирует зависимость $PSNR$ и емкости от вероятности кроссовера p_{cross} . Значение $PSNR$ увеличивается до $p_{cross} = 0,8$ и далее почти не изменяется. В то же время наибольшее значение емкости достигается при $p_{cross} = 0,9$, поэтому в экспериментах используется это значение параметра. Рис. 4, б

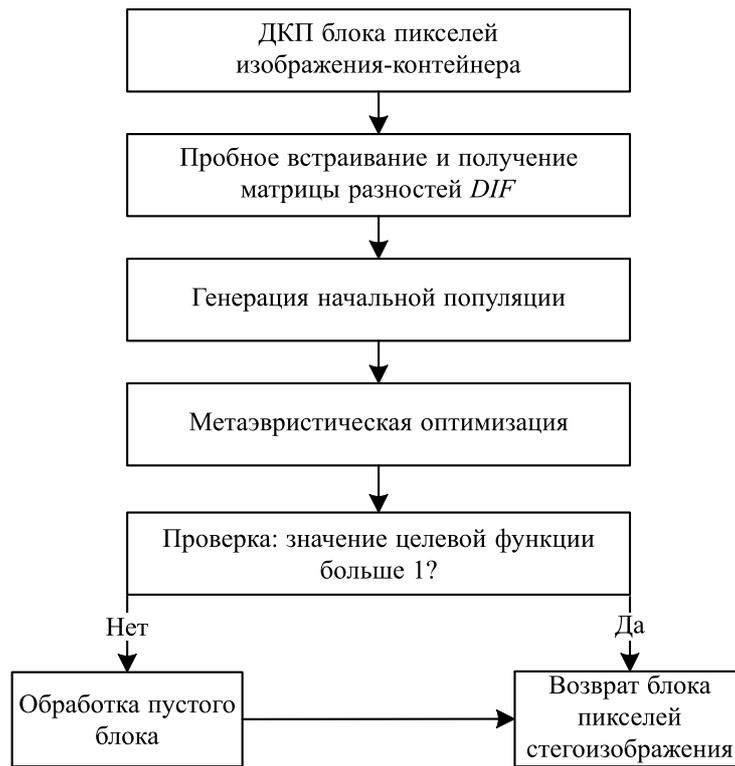


Рис. 3. Общая схема нового алгоритма сокрытия данных

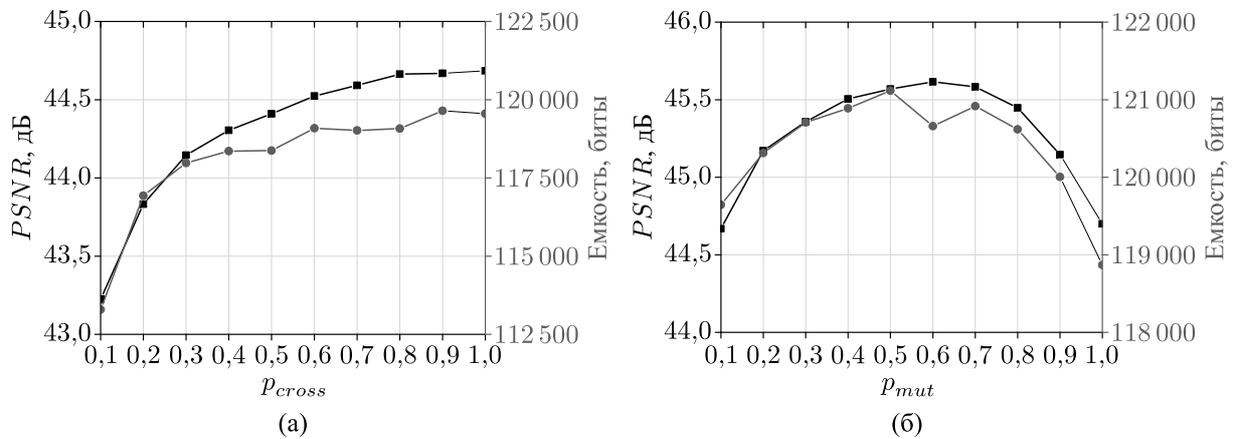


Рис. 4. Выбор значений параметров генетического алгоритма: а) вероятность кроссовера p_{cross} ; б) вероятность мутации p_{mut}

демонстрирует зависимость $PSNR$ и емкости от вероятности мутации p_{mut} . С увеличением значения p_{mut} значение $PSNR$ также увеличивается. Значение емкости увеличивается до $p_{mut} = 0,5$ и далее уменьшается, поэтому для экспериментов используется $p_{mut} = 0,5$.

Рис. 5 иллюстрирует выбор значений параметров оптимизации для ОРЧ. Рис. 5, а демонстрирует зависимость $PSNR$ и емкости от параметра w . Как следует из рисунков, баланс между незаметностью и емкостью обеспечивают значения $w = 0,4$ и $w = 0,5$. В экспериментах использовался параметр $w = 0,4$, поскольку он соответствует наибольшему значению $PSNR$. Рис. 5, б демонстрирует зависимость $PSNR$ и емкости от параметров c_1 и c_2 . В данной работе принимается $c_1 = c_2$, как в большинстве аналогичных исследований. После достижения $c_1 = c_2 = 1$ значе-

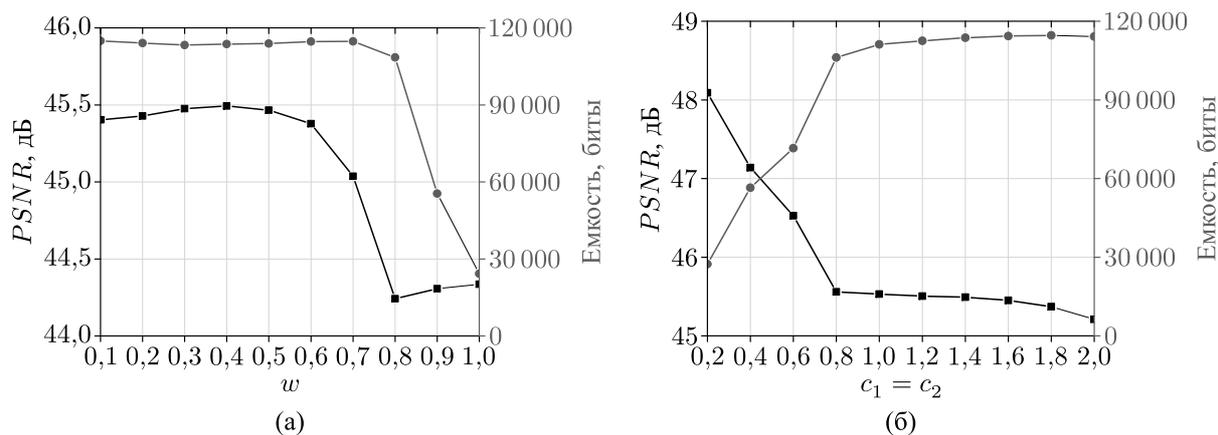


Рис. 5. Выбор значений параметров алгоритма оптимизации роя частиц: а) параметр w ; б) параметры $c_1 = c_2$

ния $PSNR$ и емкости почти не изменяются с увеличением параметров, поэтому в экспериментах используется $c_1 = c_2 = 1$.

Рис. 6 иллюстрирует выбор значений параметров оптимизации для ДЭ. Рис. 6, а демонстрирует зависимость $PSNR$ и емкости от вероятности кроссовера DE_{cross} . Баланс между незаметностью и емкостью обеспечивают значения $DE_{cross} = 0,2$ и $DE_{cross} = 0,3$. В работе используется значение $DE_{cross} = 0,3$, так как оно дает небольшой выигрыш по критерию незаметности. Рис. 6, б демонстрирует зависимость $PSNR$ и емкости от коэффициента α . Как следует из графиков, наибольшие значения по обоим критериям достигаются при $\alpha = 0,1$.

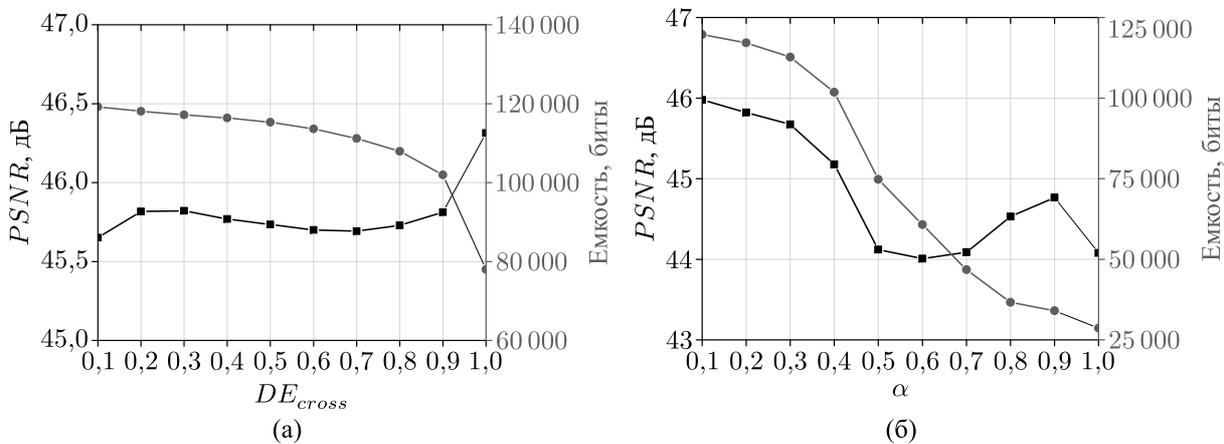


Рис. 6. Выбор значений параметров алгоритма дифференциальной эволюции: а) вероятность кроссовера DE_{cross} ; б) параметр α

На рис. 7 показан пример изображения-контейнера, а также представлены соответствующие стегоизображения, полученные с помощью трех рассмотренных метаэвристик с выбранными значениями параметров. Как видно по рисункам, встраивание дополнительной информации не вызывает возникновения каких-либо заметных невооруженным глазом искажений изображения.

На рис. 8 сравнивается эффективность применения трех рассмотренных метаэвристик для встраивания информации в гибридный домен цифровых изображений с использованием предложенного подхода. Как показывает рис. 8, а, все метаэвристики обеспечивают высокую неза-

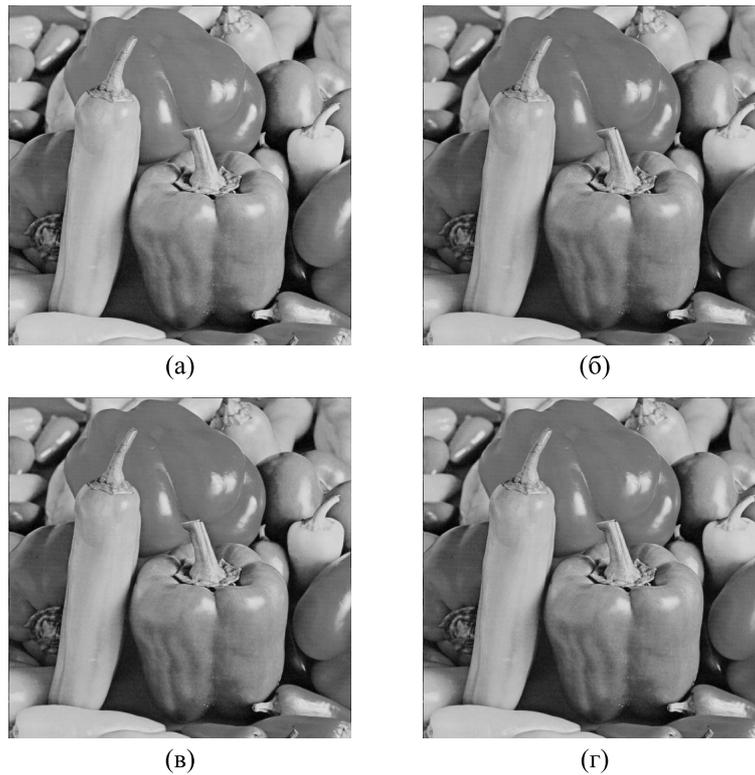


Рис. 7. Пример встраивания для изображения Peppers: а) контейнер; б) стегоразложение, полученное с помощью генетического алгоритма; в) стегоразложение, полученное с помощью алгоритма оптимизации роя частиц; г) стегоразложение, полученное с помощью алгоритма дифференциальной эволюции

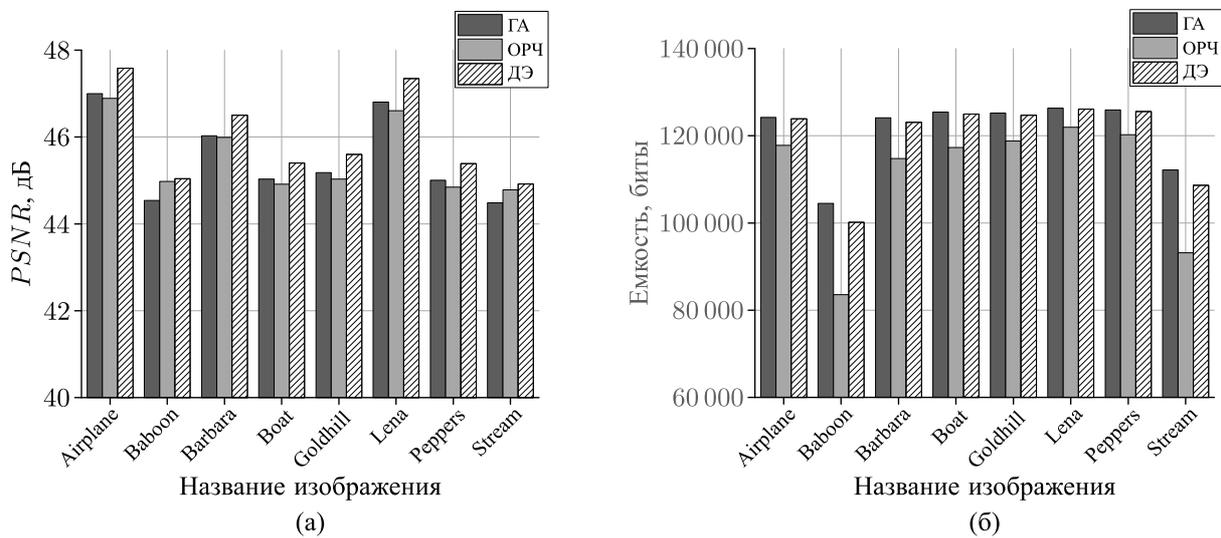


Рис. 8. Сравнение метаэвристик: а) по критерию PSNR; б) по критерию емкости

метность встраивания. Отметим, что порогом незаметности встраивания принято считать значение 35–37 дБ. Во всех случаях ДЭ обеспечивает наибольшее значение $PSNR$. В среднем по всем изображениям использование ГА позволило достичь значения $PSNR$ 45,51 дБ, ОРЧ — 45,51 дБ, ДЭ — 45,97 дБ. Рис. 8, б также демонстрирует эффективность рассмотренных метаэвристик для обеспечения высокой емкости встраивания. В среднем при использовании ГА емкость встраи-

вания составила 120 985,44 бит, при использовании ОРЧ — 110 951,71 бит, при использовании ДЭ — 119 636,36 бит. Таким образом, алгоритм ОРЧ показал худшие результаты.

Применение метаэвристической оптимизации существенно улучшило качество встраивания по сравнению с ранее предложенным алгоритмом встраивания информации в частотный домен ДКП по методу QIM [Evsutin, Melman, Meshcheryakov, 2021]. В среднем этот алгоритм обеспечивал значение $PSNR$ 36,13 дБ и емкость 92 934,13 бит. Таким образом, прирост незаметности и емкости составил соответственно 26,02 % и 30,18 % для ГА, 26,01 % и 19,39 % для ОРЧ, 27,30 % и 28,73 % для ДЭ.

Важно отметить, что предложенный подход сохранил основную особенность исходного алгоритма [Evsutin, Melman, Meshcheryakov, 2021] — безошибочное извлечение. Вся встроенная информация извлекается без ошибок во всех случаях. При этом хранение и передача матриц замен для каждого блока не требуются, поскольку безошибочное извлечение информации при данном значении шага квантования q формируется на уровне целевой функции. Передача большого объема информации, необходимой для успешного извлечения и уникальной для каждой пары «контейнер–вложение», может быть демаскирующим признаком и компрометировать наличие скрытого канала передачи данных. Предлагаемый подход лишен этого недостатка.

Можно сделать вывод, что использование метаэвристической оптимизации является эффективным методом повышения качества встраивания информации в цифровые изображения. В рамках решаемой задачи алгоритмы ГА и ДЭ показали лучший результат, ОРЧ — худший.

Из полученных результатов можно сделать вывод, что округление значений при формировании особей популяции не влияет на качество оптимизации, поскольку и ГА, работающий с целыми числами, и ДЭ и ОРЧ, работающие с вещественными значениями, позволили значительно улучшить эффективность встраивания и повысить одновременно незаметность и емкость. Это говорит о целесообразности исследования других метаэвристик разных классов, в том числе современных, с точки зрения их применимости в области стеганографии и цифровых водяных знаков.

6. Заключение

В данном исследовании был предложен новый подход к стеганографическому встраиванию информации в гибридный пространственно-частотный домен. Непосредственное встраивание битов данных в коэффициенты ДКП, реализованное ранее в работе [Evsutin, Melman, Meshcheryakov, 2021], было заменено на внесение небольших изменений в блок пикселей изображения в пространственной области в соответствии с некоторой матрицей изменений. Соответствие между битами сообщения и измененным блоком устанавливалось путем извлечения информации из коэффициентов ДКП по методу QIM. Для поиска лучшей матрицы изменений использовались алгоритмы метаэвристической оптимизации, моделирующие природные явления. В данном исследовании было реализовано сравнение эффективности трех классических метаэвристик для решения поставленной задачи: ГА, ДЭ и ОРЧ. Результаты экспериментов показали, что все три алгоритма оптимизации обеспечивают высокую незаметность и емкость встраивания. При этом во всех случаях сохранилось безошибочное извлечение встроенной информации, а хранение найденных матриц изменения после завершения процедуры встраивания не требовалось. Алгоритм ОРЧ показал худший результат, однако метаэвристики обеспечили прирост показателей производительности исходного алгоритма [Evsutin, Melman, Meshcheryakov, 2021] на 19–30 %.

Список литературы (References)

- Егорова А. А., Федосеев В. А.* Классификация и сравнительное исследование систем аутентификации JPEG-изображений, основанных на встраивании полухрупких водяных знаков // Компьютерная оптика. — 2019. — Т. 43, № 3. — С. 419–433. — DOI: 10.18287/2412-6179-2019-43-3-419-433
- Egorova A. A., Fedoseev V. A.* Klassifikatsiya i sravnitel'noe issledovanie sistem autentifikatsii JPEG-izobrazhenii, osnovannykh na vstraivanii polukhrupkikh vodyanykh znakov [A classification of semi-fragile watermarking systems for JPEG images] // Computer Optics. — 2019. — Vol. 43, No. 3. — P. 419–433 (in Russian). — DOI: 10.18287/2412-6179-2019-43-3-419-433
- Akyol S., Alatas B.* Plant intelligence based metaheuristic optimization algorithms // Artificial Intelligence Review. — 2017. — Vol. 47, No. 4. — P. 417–462. — DOI: 10.1007/s10462-016-9486-6
- Alhomoud A. M.* Image steganography in spatial domain: Current status, techniques, and trends // Intelligent Automation and Soft Computing. — 2021. — Vol. 27, No. 1. — P. 69–88. — DOI: 10.32604/iasc.2021.014773
- Ali M., Ahn C. W., Pant M., Kumar S., Singh M. K., Saini D.* An optimized digital watermarking scheme based on invariant dc coefficients in spatial domain // Electronics. — 2020. — Vol. 9, No. 9. — P. 1–17. — DOI: 10.3390/electronics9091428
- Chen B., Wornell G. W.* Quantization index modulation: A class of provably good methods for digital watermarking and information embedding // IEEE Transactions on Information Theory. — 2001. — Vol. 47, No. 4. — P. 1423–1443. — DOI: 10.1109/18.923725
- Dhawan S., Gupta R.* Analysis of various data security techniques of steganography: A survey // Information Security Journal. — 2021. — Vol. 30, No. 2. — P. 63–87. — DOI: 10.1080/19393555.2020.1801911
- Evsutin O., Melman A., Meshcheryakov R.* Algorithm of error-free information embedding into the DCT domain of digital images based on the QIM method using adaptive masking of distortions // Signal Processing. — 2021. — Vol. 179. — 107811. — DOI: 10.1016/j.sigpro.2020.107811
- Fares K., Amine K., Salah E.* A robust blind color image watermarking based on Fourier transform domain // Optik. — 2020. — Vol. 208. — 164562. — DOI: 10.1016/j.ijleo.2020.164562
- Giri K. J., Quadri S. M. K., Bashir R., Bhat J. I.* DWT based color image watermarking: a review // Multimedia Tools and Applications. — 2020. — Vol. 79, No. 43–44. — P. 32881–32895. — DOI: 10.1007/s11042-020-09716-6
- Goldberg D. E.* Genetic algorithms in search, optimization and machine learning. — USA: Addison-Wesley Longman Publishing Co., Inc., 1989.
- Kennedy J., Eberhart R.* Particle swarm optimization // Proceedings of IEEE International Conference on Neural Networks. — USA: IEEE, 1995. — No. 4. — P. 1942–1948.
- Parah S. A., Loan N. A., Shah A. A., Sheikh J. A., Bhat G. M.* A new secure and robust watermarking technique based on logistic map and modification of DC coefficient // Nonlinear Dynamics. — 2018. — Vol. 93, No. 4. — P. 1933–1951. — DOI: 10.1007/s11071-018-4299-6
- Rakhmawati L., Suwadi S., Wirawan W.* Blind robust and self-embedding fragile image watermarking for image authentication and copyright protection with recovery capability // International Journal of Intelligent Engineering and Systems. — 2020. — Vol. 13, No. 5. — P. 197–210. — DOI: 10.22266/ijies2020.1031.16
- SIPI Image Database. — URL: <https://sipi.usc.edu/database/> (accessed: 10.10.2022).
- Storn R., Price K.* Differential evolution — a simple and efficient heuristic for global optimization over continuous spaces // Journal of Global Optimization. — 1997. — Vol. 11, No. 4. — P. 341–359. — DOI: 10.1023/A:1008202821328
- Su Q., Chen B.* Robust color image watermarking technique in the spatial domain // Soft Computing. — 2018. — Vol. 22, No. 1. — P. 91–106. — DOI: 10.1007/s00500-017-2489-7

- Su Q., Liu D., Yuan Z., Wang G., Zhang X., Chen B., Yao T.* New rapid and robust color image watermarking technique in spatial domain // *IEEE Access*. – 2019. – Vol. 7. – P. 30398–30409. – DOI: 10.1109/ACCESS.2019.2895062
- Su Q., Wang H., Liu D. C., Yuan Z., Zhang X.* A combined domain watermarking algorithm of color image // *Multimedia Tools and Applications*. – 2020. – Vol. 79, No. 39–40. – P. 30023–30043. – DOI: 10.1007/s11042-020-09436-x
- Yuan Z., Liu D., Zhang X., Wang H., Su Q.* DCT-based color digital image blind watermarking method with variable steps // *Multimedia Tools and Applications*. – 2020. – Vol. 79, No. 41–42. – P. 30557–30581. – DOI: 10.1007/s11042-020-09499-w
- Yuan Z., Su Q., Liu D., Zhang X.* A blind image watermarking scheme combining spatial domain and frequency domain // *Visual Computer*. – 2021. – Vol. 37, No. 7. – P. 1867–1881. – DOI: 10.1007/s00371-020-01945-y