УДК 004.056.5
doi:10.31799/1684-8853-2018-5-44-56

Научные статьи
Articles

Адаптивный алгоритм встраивания информации в сжатые JPEG-изображения на основе операции замены

О. О. Шумская[а], *аспирант, orcid.org/0000-0002-8287-5032, shumskaya.oo@gmail.com*
М. Железны[б], *PhD, заместитель декана, orcid.org/0000-0003-1695-4370*
[а]*Санкт-Петербургский институт информатики и автоматизации РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ*
[б]*Западночешский университет, Университетская ул, 8, 2732, 301 00, Пльзень, Чешская Республика*

Введение: *один из эффективных подходов к обеспечению конфиденциальности передаваемой и хранимой информации основан на применении методов цифровой стеганографии. Для обеспечения устойчивости перед стегоанализом при встраивании информации в цифровое изображение необходимо, чтобы встраивание не приводило к появлению демаскирующих признаков.* ***Цель исследования:*** *разработка адаптивного алгоритма стеганографического встраивания информации в сжатые JPEG-изображения на основе операции замены с минимизацией вносимых искажений в информативные признаки.* ***Результаты:*** *определена значимость демаскирующих признаков в области стегоанализа и их применения для адаптивности алгоритмов сокрытия секретной информации в цифровых объектах. Приведены основные признаки в пространственной и частотной областях цифровых изображений, применяемые в современных методах стеганографического встраивания. Проведен отбор информативных признаков, исключающий линейно зависимые признаки или признаки, не несущие в себе какую-либо информацию об искажении цифрового объекта при встраивании. Полученный набор позволил повысить точность общей классификации изображений на 19 %. На основе сформированного набора информативных признаков разработана адаптивная модификация алгоритма встраивания информации в сжатые JPEG-изображения на основе замены, обеспечивающая минимизацию искажений изображения-контейнера при встраивании благодаря сформулированной целевой функции. Адаптивность алгоритма заключается в том, что выбор области сокрытия основывается на наборе информативных признаков, который характеризует естественную модель цифрового изображения. Был проведен ряд экспериментов с целью выявления наилучших значений параметров для достижения хорошей емкости встраивания и минимальных искажений признаков. По результатам вычислительных экспериментов разработанный адаптивный алгоритм показал повышенную устойчивость перед стегоанализом при внушительной емкости встраивания, а также высокие значения метрики качества стегоизображений, что говорит о повышенной незаметности как для человеческого глаза, так и для многих алгоритмов стегоанализа, так как значения признаков искажаются незначительно.*

Ключевые слова *— стеганография, стегоанализ, цифровые изображения, сжатые JPEG-изображения, операция замены, оптимизация, информативные признаки, демаскирующие признаки, классификация.*

Цитирование: Шумская О. О., Железны М. Адаптивный алгоритм встраивания информации в сжатые JPEG-изображения на основе операции замены. *Информационно-управляющие системы*, 2018, № 5, с. 44–56. doi:10.31799/1684-8853-2018-5-44-56
Citation: Shumskaya O. O., Zelezny M. Adaptive algorithm of replacement-based embedding of data into compressed JPEG images. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 5, pp. 44–56 (In Russian). doi:10.31799/1684-8853-2018-5-44-56

Введение

В настоящее время в различных сферах человеческой деятельности активно применяются информационно-аналитические технологии. Они реализуются в виде информационно-аналитических систем, предназначенных для накопления и комплексного анализа данных различного типа с целью поддержки принятия решений.

Важным составным элементом разработки и эксплуатации информационно-аналитических систем является обеспечение их информационной безопасности, прежде всего в части обеспечения конфиденциальности обрабатываемой и хранимой информации.

Один из подходов к обеспечению конфиденциальности передаваемой и хранимой информации основан на применении методов цифровой стеганографии (науки о способах передачи, хранения информации, обеспечивающих сокрытие факта наличия этой информации в некотором цифровом объекте [1]).

Методы цифровой стеганографии применимы в информационно-аналитических системах, оперирующих мультимедиа-данными, поскольку в качестве стегоконтейнеров в цифровой стеганографии преимущественно применяют цифровые изображения, аудио- и видеоданные. Чаще всего в качестве цифровых объектов-контейнеров используют цифровые изображения. Наиболее часто встречающийся графический формат на сегодня — сжатые JPEG-изображения. Именно в нем сохраняется основная часть всей графики, с которой работают пользователи информационно-аналитических систем.

Эффективность стеганографического встраивания информации в цифровые изображения оценивается с помощью различных показателей. Основным требованием является обеспечение устойчивости перед стегоанализом, что выражается в статистической неразличимости стегоизображений и изображений, не содержащих вложений. Для обеспечения устойчивости перед стегоанализом при встраивании информации в цифровое изображение необходимо, чтобы встраивание не приводило к появлению демаскирующих признаков.

Выявление демаскирующих признаков может быть произведено посредством анализа массивов изображений, обрабатываемых в информационно-аналитической системе (стегоизображений и изображений, не содержащих вложений).

Цель настоящей статьи заключается в разработке алгоритма сокрытия информации в сжатых JPEG-изображениях, позволяющего минимизировать величину вносимых искажений в информативные признаки цифровых изображений.

Стеганографическое встраивание информации в JPEG-изображения

JPEG — это самый распространенный формат изображений. Сжатые JPEG-изображения часто используют в стеганографии в качестве стегоконтейнеров с применением различных алгоритмов встраивания.

Стоит отметить, что большинство работ основаны на обработке изображения, разбитого на непересекающиеся блоки 8×8 пикселей, к каждому из которых применено дискретное косинусное преобразование (ДКП) с последующей квантизацией. Полученные матрицы коэффициентов состоят из DC-коэффициента, который располагается в левом верхнем углу матрицы и содержит основную информацию о блоке изображения, и AC-коэффициентов — остальные 63 коэффициента, в которые производится скрытое встраивание информации.

В статье [2] описывается применение алгоритма встраивания PM1 к JPEG-изображениям, позволяющего получить большую емкость и обеспечить высокую степень безопасности. В качестве области встраивания авторы используют матрицу ДКП-коэффициентов, перемешанных с помощью некоторого ключа. Вложение осуществляется в ненулевые AC-коэффициенты, авторы работы утверждают, что изменение DC-коэффициента или AC-коэффициентов, равных нулю, более заметно. Отрицательные четные и положительные нечетные коэффициенты соответствуют биту со значением «1», отрицательные нечетные и положительные четные — «0», если коэффициент соответствует биту сообщения по этим правилам, то коэффициент сохраняет свое значение, иначе коэффициент увеличивается или уменьшается в произвольном порядке на 1. Если изменение коэффициента приводит к значению «0», то его необходимо заменить на «1» или «–1» в соответствии со значением бита.

Авторы статьи [3] в качестве пространства сокрытия используют последовательности ДКП-коэффициентов равных нулю. Если длина последовательности 3 и более, то коэффициент с самой низкой частотой заменяется согласно правилу: на «0», если бит равен 0, и на «1» или «–1», если бит равен 1. Если последовательность «$x0$», то при $x > 0$ x заменяется на «$x+1$», иначе на «$x-1$». В случае последовательности вида «0x0» при $x > 0$ x заменяется на «$x+1$», иначе на «$x-1$».

В работе [4] пространством сокрытия выступают ненулевые ДКП-коэффициенты, представленные в виде последовательности. Встраивание заключается в увеличении или уменьшении коэффициента в зависимости от его начального значения, а также величины разности между значениями ДКП-коэффициента до округления и после.

Пространство сокрытия в статье [5] — нулевые ДКП-коэффициенты. Встраивание осуществляется путем увеличения или уменьшения коэффициента на 1. Выбор изменяемого коэффициента зависит от самого скрываемого сообщения, т. е. каждый раз высчитывается номер коэффициента в блоке, изменение которого будет свидетельствовать о встраивании именно этой последовательности бит. Данный подход к встраиванию основан на применении кода Хэмминга.

Авторы статьи [6] для встраивания рассматривают ненулевые ДКП-коэффициенты, представленные в виде последовательности. Встраивание осуществляется согласно формуле:

$$C'_i = \begin{cases} C_i + sign(C_i) \times b, \text{ если} |C_i| = 1, \\ C_i + sign(C_i), \text{ если} |C_i| > 1, \end{cases} \quad (1)$$

где C_i — i-й квантованный ДКП-коэффициент, b — встраиваемый бит сообщения,

$$sign(C_i) = \begin{cases} 1, \text{ если } C_i > 0, \\ 0, \text{ если } C_i = 0, \\ -1, \text{ если } C_i < 0. \end{cases}$$

Критерии эффективности стеганографического встраивания информации в JPEG-изображения

Критериями эффективности стеганографического встраивания являются емкость, незаметность (отсутствие видимых искажений цифровых

объектов-стегоконтейнеров) и устойчивость перед стегоанализом [1], представляющего собой науку о способах выявления фактов наличия скрытых сообщений в цифровых объектах. Стегоанализ в большинстве случаев заключается в поиске характеристик (признаков) цифрового объекта, которые изменяются в ходе стеганографического встраивания.

Известны методы стегоанализа, основанные на анализе признаков цифрового изображения в пространственной области, и методы, основанные на анализе признаков в частотной области. В каждом методе стегоанализа значения некоторого набора признаков объединяются в один вектор, с которым уже работает классификатор. Для того чтобы начать классификацию, прежде необходимо провести обучение: классификатор определяет для себя, какие интервалы значений признаков принадлежат «чистым» изображениям и изображениям с вложением. Сопоставляя полученные в ходе обучения данные с рассчитанным вектором признаков исследуемого изображения, классификатор определяет содержание изображения.

В работе [7] описан случай встраивания в ДКП-коэффициенты. Набор признаков для стегоанализа состоит из признаков в частотной области, основанных на соотношениях между энергией, собранной в отдельных частотных коэффициентах ДКП-спектра:

$$F_1 = \frac{E(f_0)}{E(f_{|\eta|=1})}, \qquad (2)$$

где $E(f_0)$ — среднее значение частот нулевых АС-коэффициентов изображения по блокам,

$$F_2 = \frac{\sum_{|\eta|>1} E(f_\eta)}{E(f_{|\eta|=1})}, \qquad (3)$$

где $E(f_{|\eta|=1})$ — среднее значение частот тех АС-коэффициентов изображения, абсолютная величина которых равна 1,

$$F_3 = \frac{En_{|\eta|>1}}{En_{|\eta|\le 1}}, \qquad (4)$$

где $En_{|\eta|>1}$ — энергия тех АС-коэффициентов изображения, абсолютная величина которых > 1.

В исследовании показано, что для аддитивного встраивания информации в квантованные ДКП-коэффициенты JPEG-изображения характерно увеличение значений $E(f_0)$, $\Sigma_{|\eta|>1}E(f_\eta)$, $En_{|\eta|>1}$ и уменьшение значений $E(f_{|\eta|=1})$, $En_{|\eta|\le 1}$.

Авторы объясняют свой выбор именно такого набора признаков тем, что данные величины концентрируют в себе максимальную информацию о внутреннем содержании изображения.

В качестве классификатора авторы выбрали линейный дискриминант Фишера. Такой классификатор достаточно часто встречается в современных работах, он гибкий относительно количества рассматриваемых признаков, так как проецирует весь вектор признаков на прямую. Суть классификации заключается в поиске лучшего направления данной проекции, чтобы величину можно было четко отнести к определенному классу.

Для изображений характерна межблочная корреляция. Во время встраивания вносятся изменения в блоки изображения, что может привести к нарушению связи между блоками

$$F_4 = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}}, \qquad (5)$$

где $\bar{x}$, $\bar{y}$ — средние значения АС-коэффициентов соседних блоков, x_i, y_i — i-й АС-коэффициент соседних блоков.

Исследования [8] показали, что добавление параметра межблочной корреляции АС-коэффициентов повышает вероятность обнаружения стеганографических вложений, что говорит об информативности признака в рамках стегоанализа цифровых изображений.

Авторы работ [9, 10] рассматривают в качестве основы стегоанализа 23 признака, как в частотной области, так и в пространственной:

— общая гистограмма ДКП-коэффициентов изображения;

— гистограммы первых пяти АС-коэффициентов, для каждого отдельно (5 признаков);

— двойные гистограммы АС-коэффициентов, значение которых находится в диапазоне [–5, 5], для каждого отдельная гистограмма (11 признаков);

— межблочные зависимости в разных направлениях в пространственной области (6 признаков).

Ранее отмечалось, что стеганографическое встраивание осуществляется преимущественно в АС-коэффициенты со значениями по модулю, близкими к нулю. Поэтому двойные гистограммы для коэффициентов со значениями в диапазоне [–5, 5] концентрируют в себе максимальную информацию о встраивании в частотной области.

Двойная гистограмма представляет собой матрицу, которая отражает, на каком месте сколько раз суммарно по всем блокам встретился коэффициент с определенным значением

$$f_5, \ldots, f_{15} = \frac{\sum_{k=1}^{B}\delta(d, d_k(i, j))}{\left\|\sum_{k=1}^{B}\delta(d, d_k(i, j))\right\|_{L_1}}, \qquad (6)$$

где d — фиксированное значение коэффициента, $d \in [-5, 5]$, B — количество блоков в изображе-

нии, i, j — координаты положения коэффициента в блоке, L_1 норма — максимальная из сумм элементов по столбцам, $\delta(d, d_k(i, j)) = \begin{cases} 1, & d_k(i, j) = d \\ 0, & else \end{cases}$.

Каждую характеристику авторы рассчитывают дважды: для исследуемого изображения (J_1) и для изображения, которое получают путем обрезания исследуемого изображения сверху и слева на 4 пикселя (J_2), как показано на рис. 1. Подобное действие авторы объясняют следующим образом: при обрезании изображения слева и сверху разделение изображения на блоки сдвигается, коэффициенты дискретного косинусного преобразования освобождаются от влияния прошлой квантизации и содержат только статистические данные изображения, которые как раз важны при стегоанализе.

Таким образом, конечным значением признака будет значение функционала:

$$F_5 \ldots F_{15} = \left\| f_5 \ldots f_{15}(J_1) - f_5 \ldots f_{15}(J_2) \right\|_{L_1}. \qquad (7)$$

В работах [9, 10] авторы также используют линейный дискриминант Фишера в качестве классификатора, но отмечают, что применение метода опорных векторов, возможно, повысит надежность обнаружения разработанного алгоритма.

Метод, представленный авторами [11], основан на законе Бенфорда: вероятность появления цифры на первом месте в числе тем выше, чем меньше эта цифра. Основываясь на выводах работы [12], посвященной исследованию справедливости закона Бенфорда в отношении ДКП-коэффициентов JPEG-изображений до и после квантования, авторы предложили частный случай закона Бенфорда, так как квантованные ДКП-коэффициенты не подчиняются строго закону Бенфорда

$$F_{16}, \ldots, F_{24} = N \log_{10}\left(1 + \frac{1}{s + x^q}\right), \qquad (8)$$

где $x = 1, ..., 9$, N, s, q — параметры, зависящие от качества JPEG-сжатия.

Если отклонение реальной величины от ожидаемой превышает некоторый порог, то принимается решение о наличии вложения в данном изображении.

Идея смещения изображения, применяемая в работах [9, 10], показалась довольно интересной. Было принято решение объединить смещение изображения и закон Бенфорда

$$F_{25}, \ldots, F_{33} = \left\| F_{16}, \ldots, F_{24}(J_1) - F_{16}, \ldots, F_{24}(J_2) \right\|_{L_1}. \qquad (9)$$

В приведенных работах идет речь о признаках, формируемых специально для проведения стегоанализа. Однако для решения данной задачи можно использовать и произвольные признаки, представляющие собой некоторые характеристики, рассчитываемые для цифровых изображений. В частности, в таблице представлены текстурные признаки, применяемые в различных задачах распознавания образов [13].

В общем случае стегоанализ цифровых объектов рассматривается как задача двухклассовой классификации, когда для каждого анализируемого объекта выбирается один из двух исходов: нет вложения, или объект содержит скрытые данные.

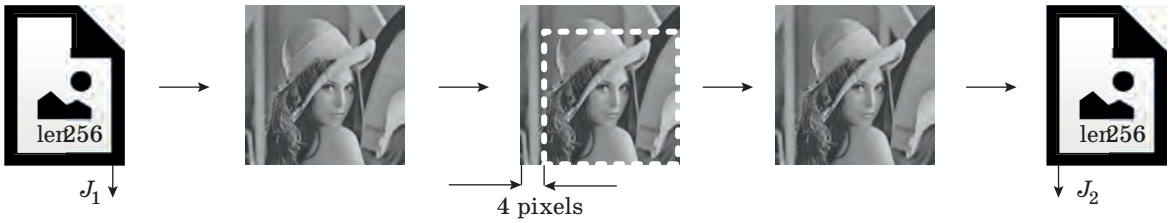
В ходе работы в качестве классификатора в стегоанализаторе применяется наивный байесовский классификатор, так как он показывает хорошие результаты [14, 15], компактен по сравнению с другими методами (в методах, основанных на опорных векторах, нейронных сетях, при увеличении набора признаков объем необходимой памяти возрастает в разы) и достаточно популярен среди ученых, работающих в данной области.

Предположение, что все особенности набора данных независимы, и является причиной такого названия классификатора. Ведь чаще всего характеристики набора данных не независимы.

Упрощенная формула для классификации:

$$P(\text{Класс}A \mid \text{Свойство1, Свойство2}) = \frac{P(\text{Свойство1} \mid \text{Класс}A) \times P(\text{Свойство2} \mid \text{Класс}A)}{P(\text{Свойство1}) \times P(\text{Свойство2})}. \qquad (10)$$

Если видны Свойства 1 и 2, это и есть вероятность того, что данные принадлежат Классу A.



■ ***Рис. 1.*** Исследуемое изображение J_1 и изображение J_2, полученное путем обрезания изображения J_1

■ ***Fig. 1.*** The researched image J_1 and the image J_2 received by trimming of the image J_1

- Признаки в пространственной области изображения
- Features in the spatial domain of image

Признак	Формула	Пояснение
Энергия	$F_{34} = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} P_{i,j}^2,$ где N — количество градаций яркости стегоизображения, P — матрица смежности	Характеризует однородность изображения и равномерность
Энтропия	$F_{35} = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} P_{i,j} \log P_{i,j}$	Выражает неравномерность распределения яркостных свойств элементов стегоизображения
Однородность	$F_{36} = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} \frac{P_{i,j}}{(1+\lvert i+j\rvert)}$	
Контраст	$F_{37} = \sum_{n=0}^{N-1} n^2 \left[\sum_{i=1}^{N}\sum_{j=1}^{N} P_{i,j}\right], \ \lvert i-j\rvert = n$	С увеличением числа локальных вариаций яркости стегоизображения контраст возрастает
Среднее по i	$F_{38} = \sum_{i=1}^{N}\sum_{j=1}^{N} iP_{i,j}$	
Среднее по j	$F_{39} = \sum_{i=1}^{N}\sum_{j=1}^{N} jP_{i,j}$	
Диспресия по i	$F_{40} = \sum_{i=1}^{N}\sum_{j=1}^{N} (i-F_{38})^2 P_{i,j}$	Мера отклонения случайной величины от ее математического ожидания
Диспресия по j	$F_{41} = \sum_{i=1}^{N}\sum_{j=1}^{N} (j-F_{39})^2 P_{i,j}$	
Ковариация	$F_{42} = \sum_{i=1}^{N}\sum_{j=1}^{N} (i-F_{38})(j-F_{39})P_{i,j}$	Мера линейной зависимости двух случайных величин
Корреляция	$F_{43} = \sum_{i=1}^{N}\sum_{j=1}^{N} \frac{(i-F_{38})(j-F_{39})P_{i,j}}{F_{40}}$	Показывает статистическую взаимосвязь двух или более величин

Ранее было отмечено, что важным критерием эффективности стеганографического встраивания является устойчивость перед стегоанализом. Обеспечить незаметность возможно, если организовать встраивание таким образом, чтобы оно не вносило заметных искажений в естественную модель цифрового изображения. С целью максимально возможной эффективности разрабатываемых методов стегоанализа исследователи строят достаточно большие признаковые пространства, включающие десятки и сотни тысяч признаков [16–18]. В совокупности данные признаки дают хорошие результаты, однако вопрос информативности этих признаков во многих исследованиях авторы обходят стороной. Поэтому выбор набора наиболее информативных признаков из большого множества является важной задачей [19–22].

Анализ информативности признаков

Ключевым этапом является выбор информативных признаков, анализ которых позволяет отделять изображения, содержащие встроенную информацию, от чистых изображений. В качестве признаков в задаче стегоанализа используются разнообразные статистические характеристики, рассчитываемые для элементов данных цифровых изображений в пространственной и частотной областях.

Набор признаков может содержать сотни и тысячи элементов, однако некоторые из них могут быть линейно зависимыми, какие-то признаки могут не подходить к решению конкретной задачи. Для того чтобы из огромного множества набранных признаков выделить информативные

для рассматриваемой задачи, необходимо провести эксперименты с применением алгоритма выбора информативных признаков.

Существует много алгоритмов отбора информативных признаков, основанных на выявлении статистических зависимостей (между элементами набора, между элементами набора и выходным значением), сравнительных экспериментах, сложных вычислениях.

Жадные алгоритмы поиска используются часто, так как быстры и дают хороший результат во многих задачах. Группа алгоритмов получила такое название из-за того, что если один из признаков был выбран в поднабор (или исключен), то в дальнейшем он остается в наборе (в случае жадного включения) или навсегда будет отсутствовать (в случае жадного исключения) [23].

Алгоритмы поочередного перебора оценивают важность каждого элемента набора признаков для результата, рассматривая каждый элемент отдельно «в вакууме», т. е. без учета влияния остальных элементов [23]. Однако это не позволяет однозначно отобрать информативные признаки (постановка границы отбора), также в качестве наиболее важных признаков (наиболее информативных) могут оказаться подобные признаки.

Генетический алгоритм — эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путем случайного подбора, комбинирования и вариации искомых параметров с использованием механизмов, аналогичных естественному отбору в природе [24].

Для дальнейшей работы принято решение использовать жадный алгоритм с исключением, так как данный метод довольно быстрый и эффективный согласно исследованиям [25, 26].

Эксперименты показали, что набор из 43 признаков в пространственной и частотной областях можно сократить на 17 элементов, при этом повысив общую точность классификации на 19 %.

В результате экспериментов был определен следующий набор из 26 информативных признаков: $\{F_1–F_5, F_8–F_{12}, F_{18}, F_{19}, F_{26}–F_{34}, F_{36}, F_{38}–F_{41}\}$.

Алгоритм встраивания информации в JPEG-изображения

За основу исследования был взят алгоритм, описанный в [27].

Введем общую схему встраивания информации в сжатые JPEG-изображения на основе операции замены квантованных ДКП-коэффициентов. Пусть изображение-контейнер содержит K блоков квантованных ДКП-коэффициентов. Пространство сокрытия представляет собой некоторую подпоследовательность последовательности всех ДКП-коэффициентов $C = c_1c_2...c_L$, $L < 64K$. Часть пространства сокрытия, образованную ДКП-коэффициентами одного блока, назовем областью встраивания данного блока. Будем считать, что нумерация коэффициентов блока осуществляется в порядке его «зигзагообразного» обхода. Секретное сообщение обозначим $M = m_1m_2...m_L$, $m_i \in \{0, 1\}$, $i = \overline{1, L}$. Количество бит, встраиваемых в один блок изображения, обозначим n. Если биты сообщения распределяются по блокам неравномерно, то можем записать $L = \sum_{j=1}^{K} n_j$, $n_j \geq 0$.

Значение, на которое будет заменен ДКП-коэффициент при встраивании в него бита секретного сообщения, назовем величиной замены и обозначим x. Тогда схему встраивания информации в JPEG-изображения на основе операции замены можно представить в виде формулы:

$$c'_i = \begin{cases} x, & m_i = 1, \\ -x, & m_i = 0, \end{cases} \qquad (11)$$

где c'_i — измененное значение ДКП-коэффициента.

Обозначим последовательность ДКП-коэффициентов изображения-контейнера, не входящих в пространство сокрытия, $D = d_1d_2...d_{64K-L}$, и введем дополнительную операцию для изменения данных коэффициентов:

$$d'_i = \begin{cases} x+1, & d_i = x, \\ -x-1, & d_i = -x, \\ d, & \text{иначе}. \end{cases} \qquad (12)$$

Дополнительная операция необходима, чтобы при извлечении опираться только на ДКП-коэффициенты, равные x и $-x$, которые будут соответствовать единичным и нулевым битам секретного сообщения.

Основное преимущество, которое дает представленная схема встраивания по сравнению с другими схемами, заключается в возможности произвольного выбора ДКП-коэффициентов, в которых будут размещены биты встраиваемого сообщения. При этом количество изменяемых коэффициентов для разных блоков изображения-контейнера может быть различным. Это позволит формировать пространство сокрытия для каждого конкретного контейнера наилучшим образом. Устойчивость введенной схемы встраивания перед стегоанализом будет зависеть от статистических характеристик сообщения, объема стеговложения и качества сжатия изображения-контейнера.

Распределение квантованных ДКП-коэффициентов JPEG-изображения близко к обобщен-

ному нормальному распределению [2]. Если распределение нулей и единиц в сообщении будет отлично от равномерного, то столбцы гистограммы ДКП-коэффициентов со значениями x и $-x$ будут иметь вид, не соответствующий нормальному распределению, что послужит демаскирующим признаком. Для предупреждения данной уязвимости сообщение перед встраиванием должно быть сжато или зашифровано. В этом случае столбцы со значениями x и $-x$ на гистограмме ДКП-коэффициентов будут иметь симметричный вид (с некоторой допустимой погрешностью), что соответствует модели исходного изображения.

Другим демаскирующим признаком может послужить изменение высоты данных столбцов. Для предупреждения данной уязвимости длину сообщения следует задавать такой, чтобы она совпадала с количеством ДКП-коэффициентов, по абсолютному значению соответствующих величине замены для данного качества JPEG-сжатия изображения-контейнера. При встраивании сообщения малого объема следует добавить в него поле, хранящее длину, и использовать только часть пространства сокрытия.

Таким образом, устойчивость перед стегоанализом может быть достигнута за счет подстройки параметров встраивания под длину секретного сообщения или характеристики конкретного изображения-контейнера.

Необходимость минимизации искажений естественной модели цифрового изображения в области квантованных ДКП-коэффициентов приводит к появлению задачи оптимизации.

Минимизация искажений естественной модели цифрового изображения в области квантованных ДКП-коэффициентов

В области стеганографии существует большое количество различных алгоритмов встраивания. Авторы работ придумывают новые идеи сокрытия информации в объекте, стараясь повысить незаметность встраивания. Однако тот факт, что вложение не видно человеческому глазу, не означает, что встраивание не внесло искажений в стегоконтейнер. Для оценки визуального качества изображения часто используется метрика PSNR (peak signal to noise ratio) — пиковое отношение сигнал/шум [28]. Чем меньше искажений внесено в стегоизображение, тем больше должна быть эта метрика (ее удобно называть «метрикой сходства»). Число PSNR безразмерно, поскольку единицами измерения и числителя, и знаменателя служат величины пикселей. Тем не менее, из-за использования логарифмов говорится, что число PSNR измеряется в децибелах (дБ).

Формула расчета PSNR:

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{\frac{1}{n}\sum_{i=1}^{n}(P_i - Q_i)^2}}\right), \quad (13)$$

где 255 — максимальное значение пикселя, n — общее количество пикселей, P_i — пиксели исходного изображения, Q_i — пиксели восстановленного изображения.

Помимо стремления минимизировать различие стегоизображения от исходного, важной является и устойчивость перед стегоанализом. Критерием в данном случае может выступать ошибка классификации стегоизображений.

Таким образом, целевая функция имеет вид:

$$f(x^*) = \max_{n\in N, x\in X}(1 - acc_{n,x}), \quad (14)$$

где $acc_{n,x}$ — точность классификации стегоизображений при встраивании n бит в блок с величиной замены x.

Появление целевой функции требует решения задачи оптимизации. На сегодняшний день существует большое множество алгоритмов оптимизации для различных научных областей, в том числе и для оптимизации стеганографических алгоритмов.

Метод дифференциальной эволюции — один из методов эволюционного моделирования, предназначенный для решения задачи многомерной оптимизации. По классификации оптимизационных методов он относится к классу стохастических методов. Метод дифференциальной эволюции — прямой метод оптимизации, т. е. в ходе его работы требуется только вычисление значения целевой функции, но не ее производных. В общем случае целевые функции, оптимизируемые с помощью данного метода, могут быть не дифференцируемые, нелинейные, с большим количеством переменных [29].

В работах последних лет все чаще применяются биоинспирированные алгоритмы оптимизации, т. е. вдохновленные природой: чаще всего такие методы основаны на действиях различных насекомых, животных. Например, алгоритм пчелиной колонии [30]: на первом шаге пчелы разлетаются и собирают информацию, на втором они собираются и решают, какие направления обладают большим потенциалом (в случае пчел, где больше нектара). Повтор данных шагов позволит выбрать оптимальное решение.

Генетический алгоритм — это эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путем случайного подбора, комбинирования и вариации искомых параметров с использованием механиз-

мов, аналогичных естественному отбору в природе [24]. Задача оптимизации решается благодаря применению методов, основанных на естественной эволюции: наследования, мутации, отбора, кроссовера, скрещивания.

Генетический алгоритм уже давно себя зарекомендовал в области стеганографии: многие исследователи выбирают его в качестве алгоритма оптимизации, получая хорошие результаты экспериментов. Преимущество генетического алгоритма в параллельной обработке множества альтернативных решений. Поэтому для дальнейшей работы в качестве алгоритма оптимизации выбран генетический алгоритм.

Ниже представлено описание разработанного алгоритма.

Вход: сообщение $M = m_1 m_2 ... m_L$, $m_i \in \{0, 1\}$, $i = \overline{1, L}$; пустой стегоконтейнер — цифровое изображение, сжатое по методу JPEG; величина замены x; количество бит, встраиваемых в блок, n; параметры генетического алгоритма (число поколений, особей в популяции).

Выход: стегоизображение.

Шаг 1. Изображение-контейнер разбить на K неперекрывающихся блоков размером 8×8 пикселей, вычислить квантованные ДКП-коэффициенты.

Шаг 2. Сгенерировать начальную популяцию из P особей вида $p^k = (p_1^k, p_2^k, \ldots, p_n^k)$, $p_u^k \in [0,63]$.

Шаг 3. Рассчитать значение целевой функции для каждой особи.

Шаг 4. Найти особь с наибольшим значением целевой функции и запомнить ее как p^{best}.

Шаг 5. Для $i = \overline{1, I}$ выполнить:

Шаг 5.1. Сформировать новую популяцию, исключая особей с одинаковыми значениями отдельных элементов в случае их появления.

Шаг 5.2. Рассчитать значение целевой функции для каждой особи.

Шаг 5.3. Обновить p^{best}.

Шаг 6. Осуществить встраивание в ДКП-коэффициенты стегоконтейнера с номерами, полученными в результате применения генетического алгоритма, согласно формуле (11), остальные коэффициенты обработать согласно формуле (12).

Шаг 7. Применить обратное дискретное косинусное преобразование коэффициентов, JPEG-сжатие.

Экспериментальное исследование разработанного алгоритма

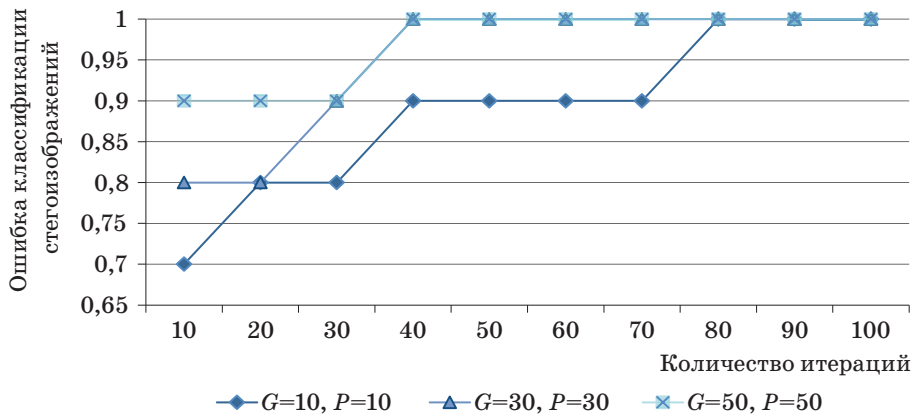
Вычислительные эксперименты проводились на выборке из 10 полутоновых тестовых JPEG-изображений разрешением 256×256 пикселей из базы USC-SIPI ID (University of Southern California Signal and Image Processing Institute Image Database) [31]. Встраиваемые сообщения представляли собой тексты на английском языке.

На рис. 2 показана зависимость ошибки классификации стегоизображений от числа итераций при встраивании сообщения длиной 2604 бита при $x = 3$ и $n = 4$.

Из проведенных экспериментов видно, что при малом числе поколений и особей в популяции алгоритму необходимо достаточно большое количество итераций (~80), чтобы достичь того минимума искажений, которое позволит скрыть от применяемого стегоанализатора факт наличия вложения в стегоизображениях.

Вполне закономерно, что при большом числе популяций и большом их размере необходимо меньше итераций (~30) для достижения поставленной цели. Однако большой объем популяций не оправдывается относительно малым количеством итераций.

Из приведенных результатов приемлем вариант с числом поколений и особей в популяции 30.



■ ***Рис. 2.*** Зависимость величины ошибки классификатора от числа итераций

■ ***Fig. 2.*** Dependence of value of the qualifier error on number of iterations

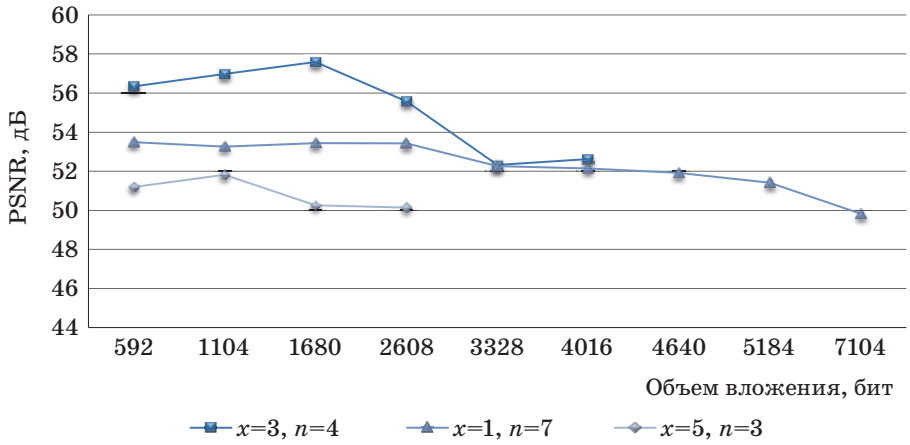
Такие параметры позволяют достичь незаметности встраивания для применяемого стегоанализатора при ~40 итерациях. В дальнейших экспериментах были применены именно эти параметры.

На рис. 3 показана зависимость значения PSNR от объема вложения для трех разных наборов параметров встраивания: величины замены x и количества бит n, встраиваемых в блок. В рассматриваемых изображениях 1024 блока, поэтому емкость стегоконтейнера ограничивается параметром n. Для каждого случая был проведен эксперимент с объемом, близким к максимальной емкости стегоконтейнера.

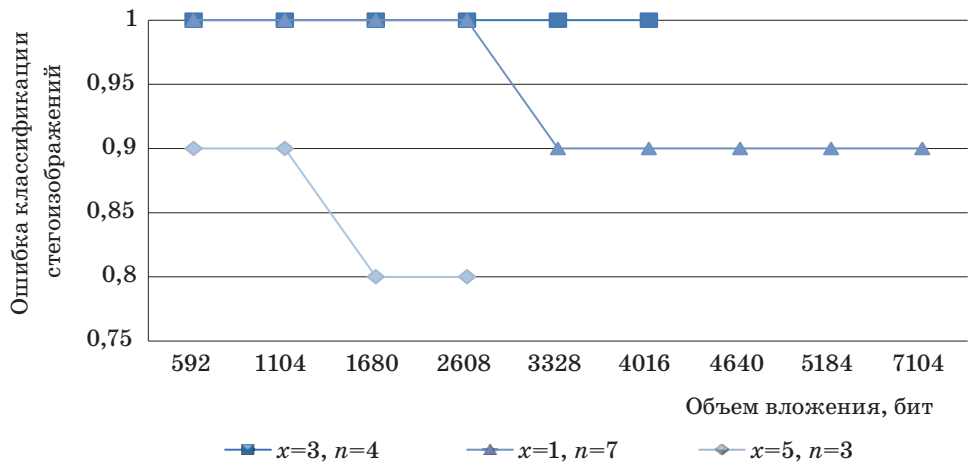
Многие авторы отмечали, что при встраивании желательно изменять коэффициенты, значения которых ближе к 0. В экспериментах с величиной замены, равной 5, значение PSNR всегда ниже, чем у аналогичных экспериментов с другими параметрами. Стоит заметить, что в матрице квантованных ДКП-коэффициентов относительно много коэффициентов со значениями, близкими к 0, и их изменение на величину 5 (не самое часто встречаемое значение в матрице) зачастую может понести большие искажения в конечном результате.

При величине замены, равной 1, значение PSNR ведет себя весьма спокойно, несмотря на увеличение объема вложения. Конечно, при большом вложении значение PSNR опускается ниже 50 дБ, но при этом в маленькое изображение встраивается достаточно большой объем данных.

При параметрах встраивания $x = 3$, $n = 4$ значение PSNR показывает очень хорошие результаты. В методе, который был взят за основу работы, при аналогичных параметрах значение PSNR опускается ниже 50 дБ при вложении порядка 3500 бит, при том, что там изображения в 4 раза больше. При малом объеме вложения адаптивный алгоритм показывает значение PSNR в среднем на 4 дБ ниже по сравнению с описанным в статье [27], но при больших вложениях пока-



■ ***Рис. 3.*** Зависимость значения PSNR от объема вложения
■ ***Fig. 3.*** Dependence of PSNR value on embedding capacity



■ ***Рис. 4.*** Зависимость ошибки классификации от объема вложения
■ ***Fig. 4.*** Dependence of value of the qualifier error on embedding capacity

зывает результаты выше. Однако стоит помнить, что целевая функция в данной работе не связана со значением PSNR, несмотря на то, что это основная метрика качества изображения, его схожести с исходным изображением, а в [27] целевой функцией является PSNR. Именно поэтому в экспериментах адаптивного алгоритма нет такой явной зависимости значения PSNR от объема вложения — «чем больше вложение, тем меньше PSNR».

■ ***Рис. 5.*** Пример работы алгоритма (исходное изображение — слева, стегоизображение — справа)

■ ***Fig. 5.*** Example of the algorithm's work (initial images — at the left, stego-images — on the right)

На рис. 4 показана зависимость ошибки классификации стегоизображений от объема вложения.

В статье [27] авторы проверяют устойчивость алгоритма к стегоанализу для величины замены, равной 3, на основе закона Бенфорда. При объеме встраивания 10 000 бит одно стегоизображение из 8 (разрешением 512×512 пикселей) было классифицировано верно.

При встраивании в изображение разрешением 256×256 пикселей 4016 бит с величиной замены $x = 3$, все стегоизображения были классифицированы неверно.

Эксперимент со встраиванием при $x = 5$ и $n = 3$ показал не только относительно плохой результат по значению PSNR, но и при проверке устойчивости перед стегоанализатором. Даже при малом вложении одно стегоизображение из 10 было классифицировано верно.

На рис. 5 представлены примеры работы алгоритма встраивания 3328 бит при $x = 3$ и $n = 4$.

Заключение

Сформирован набор признаков в пространственной и частотной областях сжатого JPEG-изображения, произведен анализ информативности стегоаналитических признаков, входящих в сформированный набор. Обучен стегоаналитический классификатор на массивах цифровых изображений, содержащих «чистые» изображения, и стегоизображения с использованием сформированного набора информативных признаков. Реализован алгоритм встраивания информации в сжатые JPEG-изображения на основе операции замены. Для минимизации искажений при встраивании была построена целевая функция на основе сформированного набора информативных признаков. Разработан адаптивный алгоритм встраивания информации в сжатые JPEG-изображения на основе операции замены с применением оптимизации. Адаптивность алгоритма заключается в том, что выбор области сокрытия основывается на наборе информативных признаков, который характеризует естественную модель цифрового изображения.

Вычислительные эксперименты показали, что можно встроить более 4 тысяч бит в полутоновое JPEG-изображение разрешением 256×256 пикселей, минимизируя искажения естественной модели цифрового изображения в области квантованных ДКП-коэффициентов настолько, что стегоанализатор на основе наивного байесовского классификатора с набором отобранных с помощью жадного алгоритма с исключением информативных признаков не выявляет факт сокрытия сообщения в изображении в 10 случаях из 10.

Литература

1. **Коханович Г. Ф., Пузыренко А. Ю.** Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
2. **Yu L., Zhao Y., Ni R., Zhu Zh.** PM1 steganography in JPEG images using genetic algorithm // Soft Computing. 2009. vol. 13(4). pp. 393–400.
3. **Yang Ch. N., Kim Ch., Lo Y. H.** Adaptive real-time reversible data hiding for JPEG images // Journal of Real-Time Image Processing. 2018. vol. 14(1). pp. 147–157. doi:10.1007/s11554-015-0555-x
4. **Guo L., Ni J., Shi Y. Q.** Uniform embedding for efficient JPEG steganography // IEEE Transactions on Information Forensics and Security. 2014. vol. 9(5). pp. 814–825.
5. **Sachnev V., Kim H. J., Shi Y., Barni M.** Ternary data hiding technique for JPEG steganography // Digital Watermarking. IWDW 2010. Lecture Notes in Computer Science. 2011. vol. 6525. pp. 202–210.
6. **Huang F., Qu X., Kim H. J., Huang J.** Reversible data hiding in JPEG images // IEEE Transactions on Circuits and Systems for Video Technology. 2015. vol. 26. doi:10.1109/TCSVT.2015.2473235
7. **Jia-Fa M., Xin-Xin M., Gang X., Wei-Guo Sh., Na-Na Zh.** A steganalysis method in the DCT domain // Multimedia Tools and Applications. 2016. № 75. pp. 5999–6019.
8. **Шумская О. О.** Метод стегоанализа JPEG-изображений на основе энергетических признаков в частотной области // Материалы международной научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР-2017». Томск: «В-Спектр». 2017. Ч. 6. С. 41–44.
9. **Fridrich J.** Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes // Proceedings of the Sixth International Workshop on Information Hiding, Lecture Notes in Computer Science. 2014. vol. 3200. pp. 67–81.
10. **Chen M. C.** Alpha-trimmed Image Estimation for JPEG Steganography Detection // Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics. San Antonio, Texas, USA. 2009. pp. 4581–4585.
11. **Andriotis P., Oikonomou G., Tryfonas T.** JPEG steganography detection with Benford's Law // Digital Investigation. 2013. vol. 9. pp. 246–257.
12. **Fu D. Shi Y. Q., Su W.** A generalized Benford's law for JPEG coefficients and its applications in image forensics // Proceedings of SPIE 6505, security, steganography, and watermarking of multimedia contents IX. USA, San Jose. 2007. pp. 1L1–1L11.
13. **Мицель А. А., Колодникова Н. В., Протасов К. Т.** Непараметрический алгоритм текстурного анализа аэрокосмических снимков // Известия Томского политехнического университета. 2005. Т. 308(1). С. 65–70.
14. **Berg G., Davidson I., Duan M. Y., Paul G.** Searching For Hidden Messages: Automatic Detection of Steganography // Proceedings of the 15th innovative applications of artificial intelligence conference (IAAI), August 12–14. Acapulco, Mexico. 2003. pp. 51–56.
15. **Maitra S., Paul G., Sarkar S., Lehmann M., Meier W.** New results on generalization of roos-type biases and related keystream of RC // Proceedings of the 6th International conference on cryptology in africa (AFRICACRYPT), June 22–24. Cairo, Egypt. 2013. vol. 7918. pp. 222–239.
16. **Liu Q., Sung A., Qiao M., Chen Z., Ribeiro B.** An improved approach to steganalysis of JPEG images // Inf Sci. 2010. № 180(9). pp. 1643–1655.
17. **Fusheng Y., Gao T.** Novel image splicing forensic algorithm based on generalized DCT coefficient-pair histogram // Proceedings of 10th chinese conference (IGTA 2015). China, Beijing. 2015. pp. 63–71.
18. **Kodovsky J., Fridrich J.** Steganalysis of JPEG images using rich models // Proceedings of SPIE, electronic imaging, media watermarking, security, and forensics XIV. USA, San Francisco. 2012. pp. 7–20.
19. **Орешин А. Н., Саитов И. А., Орешин Н. А.** Стратегия повышения качества услуг видеосвязи на основе фильтрации видеопотока, содержащего кадры-вставки с информационным шумом // Труды СПИИРАН. 2015. Т. 41. С. 57–80.
20. **Карпов А. А., Ронжин А. Л.** Многомодальные интерфейсы в автоматизированных системах управления // Известия высших учебных заведений. Приборостроение. 2005. Т. 48. № 7. С. 9–14.
21. **Ронжин А. Л., Карпов А. А., Леонтьева А. Б., Костюченко Б. Е.** Разработка многомодального информационного киоска // Труды СПИИРАН. 2007. № 5. С. 227–246.
22. **Ронжин А. Л., Будков В. Ю.** Технологии поддержки гибридных Е-совещаний на основе методов аудиовизуальной обработки // Вестник компьютерных и информационных технологий. 2011. № 4. С. 31–35.
23. **Cormen Th. H., Leiserson Ch. E., Rivest R. L., Stein C.** Introduction to algorithms. London: MIT Press. 2013. 1324 p.
24. **Гладков Л. А., Курейчик В. В., Курейчик В. М.** Генетические алгоритмы. — М.: Физматлит, 2006. — 320 с.
25. **Guyon I., Elisseeff A.** An introduction to variable and feature selection // Journal of Machine Learning Research. 2003. vol. 3. pp. 1157–1182.
26. **Molina L. C., Belanche L., Nebot A.** Feature selection algorithms: a survey and experimental evaluation // Proceedings of the 2002 IEEE International conference on data mining. IEEE Computer Society. 2002. pp. 306–313.
27. **Евсютин О. О., Шелупанов А. А., Мещеряков Р. В., Бондаренко Д. О.** Алгоритм встраивания информации в сжатые цифровые изображения на основе операции замены с применением оптимизации // Компьютерная оптика. 2017. Т. 41(3). С. 412–421.

28. **Сэломон Д.** Сжатие данных, изображения и звука. М.: Техносфера, 2004. 368 с.
29. **Storn R., Price K.** Differential evolution — a simple and efficient heuristic for global optimization over continuous spaces // Journal of Global Optimization. 1997. vol. 11. pp. 341–359.
30. **Karaboga D., Basturk B.** On the performance of artificial bee colony (ABC) algorithm // Applied Soft Computing. 2008. vol. 8. pp. 687–697.
31. SIPI Image Database. http://sipi.usc.edu/database/ (дата обращения: 18.04.2018).

UDC 004.056.5
doi:10.31799/1684-8853-2018-5-44-56

Adaptive algorithm of replacement-based embedding of data into compressed JPEG images

O. O. Shumskaya[a], PhD student, orcid.org/0000-0002-8287-5032, shumskaya.oo@gmail.com
M. Zelezny[b], PhD, Deputy Dean, orcid.org/0000-0003-1695-4370
[a]Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation
[b]University of West Bohemia, Pilsen, University Street, 8, no. 2732, 301 00, Plzeň, Czech Republic

Introduction: Digital steganography is an effective approach to ensuring the confidentiality of transferred and stored information. In order to provide stability before steganalysis when data are embedded into digital images, it is important to avoid the appearance of unmasking features caused by the embedding. **Purpose:** Developing an adaptive algorithm of steganographic embedding of data into compressed JPEG images based on a replacement operation, minimizing the distortions introduced to the informative features. **Results:** The paper discusses the importance of unmasking features in steganalysis and their application for adaptability of information concealment algorithms in digital objects. The main features in the spatial and frequency domains of digital images applied in modern steganographic embedding methods are specified. Informative features are selected, excluding linearly dependent features or features without any information about digital object distortion during the embedding. The resulting set has allowed us to increase the accuracy of general classification of images by 19%. On the base of the obtained set of informative features, a replacement-based adaptive modification has been developed for the algorithm of embedding data into compressed JPEG images. This modification minimizes the image container distortions during the embedding due to the use of a criterion function formulated in the article. The algorithm is adaptive because the concealment field is chosen based on the set of informative features which characterize a natural model of a digital image. Computing experiments allowed us to find the best parameter values in order to achieve good embedding capacity and the minimum distortions of the unmasking features. Experiments with the developed adaptive algorithm have demonstrated its increased stability before steganalysis and very good embedding capacity. Also, it has high values of the stego-image quality metrics, making the distortions less noticeable either for human eyes or for numerous steganalysis algorithms, because the values of unmasking features are distorted only slightly.

Keywords – steganography, steganalysis, digital images, compressed jpeg images, replacement operation, optimization, informative features, unmasking features, classification.

Citation: Shumskaya O. O., Zelezny M. Adaptive algorithm of replacement-based embedding of data into compressed JPEG images. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 5, pp. 44–56 (In Russian). doi:10.31799/1684-8853-2018-5-44-56

References

1. Kohanovich G. F., Puzyrenko A. Yu. *Computer steganography. Theory and practice*. K., MK-Press, 2006. 288 p. (In Russian).
2. Yu L., Zhao Y., Ni R., Zhu Zh. PM1 steganography in JPEG images using genetic algorithm. *Soft Computing*, 2009, vol. 13(4), pp. 393–400.
3. Yang Ch. N., Kim Ch., Lo Y. H. Adaptive real-time reversible data hiding for JPEG images. *Journal of Real-Time Image Processing*, 2018, vol. 14(1), pp. 147–157. doi:10.1007/s11554-015-0555-x
4. Guo L., Ni J., Shi Y. Q. Uniform embedding for efficient JPEG steganography. *IEEE Transactions on Information Forensics and Security*, 2014, vol. 9(5), pp. 814–825.
5. Sachnev V., Kim H. J., Shi Y., Barni M. Ternary data hiding technique for JPEG steganography. Digital watermarking. IWDW 2010. *Lecture Notes in Computer Science*, 2011, vol. 6525, pp. 202–210.
6. Huang F., Qu X., Kim H. J., Huang J. Reversible data hiding in JPEG images. *IEEE Transactions on Circuits and Systems for Video Technology*, 2015, vol. 26. doi:10.1109/TCSVT.2015.2473235
7. Jia-Fa M., Xin-Xin M., Gang X., Wei-Guo Sh., Na-Na Zh. A steganalysis method in the DCT domain. *Multimedia Tools and Applications*, 2016, № 75, pp. 5999–6019.
8. Shumskaya O. O. Steganalysis method of JPEG-images on the basis of energy features in frequency domain. *Nauchnaja sessija TUSUR-2017*, 2017, vol. 6, pp. 41–44 (In Russian).
9. Fridrich J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. Proceedings of the sixth international workshop on information hiding. *Lecture Notes in Computer Science*, 2014, vol. 3200, pp. 67–81.
10. Chen M. C. Alpha-trimmed image estimation for JPEG steganography detection. *Proceedings of the 2009 IEEE international conference on systems, man, and cybernetics*. San Antonio, Texas, USA. 2009, pp. 4581–4585.
11. Andriotis P., Oikonomou G., Tryfonas T. JPEG steganography detection with Benford's law. *Digital Investigation*, 2013, vol. 9, pp. 246–257.
12. Fu D., Shi Y. Q., Su W. A generalized Benford's law for JPEG coefficients and its applications in image forensics. *Proceedings of SPIE 6505, security, steganography, and watermarking of multimedia contents IX*. USA, San Jose. 2007, pp. 1L1–1L11.
13. Mitsel A. A., Kolodnokova N. V., Protasov K. T. Nonparametric algorithm of the textural analysis of space pictures. *News of the Tomsk Polytechnic University*, 2005, vol. 308(1), pp. 65–70 (In Russian).
14. Berg G., Davidson I., Duan M. Y., Paul G. Searching for hidden messages: automatic detection of steganography. *Proceedings of the 15th innovative applications of artificial intelligence conference* (IAAI), August 12–14. Acapulco, Mexico. 2003, pp. 51–56.

15. Maitra S., Paul G., Sarkar S., Lehmann M., Meier W. New results on generalization of roos-type biases and related keystream of RC. *Proceedings of the 6th international conference on cryptology in Africa* (AFRICACRYPT), June 22–24. Cairo, Egypt. 2013, vol. 7918, pp. 222–239.
16. Liu Q., Sung A., Qiao M., Chen Z., Ribeiro B. An improved approach to steganalysis of JPEG images. *Inf. Sci.*, 2010, № 180(9), pp. 1643–1655.
17. Fusheng Y., Gao T. Novel image splicing forensic algorithm based on generalized DCT coefficient-pair histogram. *Proceedings of 10th chinese conference* (IGTA 2015). China, Beijing. 2015, pp. 63–71.
18. Kodovsky J., Fridrich J. Steganalysis of JPEG images using rich models. *Proceedings of SPIE, electronic imaging, media watermarking, security, and forensics XIV*. USA, San Francisco. 2012, pp. 7–20.
19. Oreshin A. N., Saitov I. A., Oreshin N. A. Strategy of the video communication services quality enhancement based on the filtration of a video stream containing snap-insertions with information noise. *SPIIRAS Proceedings*. 2015, vol. 41, pp. 57–80.
20. Karpov A. A., Ronzhin A. L. Multimodal interfaces in automated control systems. *Journal of Instrument Engineering*, 2005, vol. 48, № 7, pp. 9–14 (In Russian).
21. Ronzhin A. L., Karpov A. A., Leontyeva An. B., Kostuchenko B. E. The development of the multimodal information kiosk. *SPIIRAS Proceedings*, 2007, vol. 5, pp. 227–245 (In Russian).
22. Ronzhin A. L., Budkov V. Yu. Support technologies of e-meetings based on methods for audiovisual processing. *Bulletin of Computer and Information Technologies*, 2011, no. 4, pp. 31–35 (In Russian).
23. Cormen Th. H., Leiserson Ch. E., Rivest R. L., Stein C. *Introduction to algorithms*. London, MIT Press, 2013, 1324 p.
24. Gladkov L. A., Kurejchik V. V., Kurejchik V. M. *Genetic algorithms*. 2006, 320 p. (In Russian).
25. Guyon I., Elisseeff A. An introduction to variable and feature selection. *Journal of Machine Learning Research*, 2003, vol. 3, pp. 1157–1182.
26. Molina L. C., Belanche L., Nebot A. Feature selection algorithms: a survey and experimental evaluation. *Proceedings of the 2002 IEEE International conference on data mining. IEEE Computer Society*, 2002, pp. 306–313.
27. Evsutin O. O., Shelupanov A. A., Mescherjakov R. V., Bondarenko D. O. Algorithm of information embedding into compressed digital images on the basis of replacement operation with use of optimization. *Computer optics*, 2017, vol. 41(3), pp. 412–421 (In Russian).
28. Salomon D. *Data compression methods*, 2004. 368 p. (In Russian).
29. Storn R., Price K. Differential evolution — a simple and efficient heuristic for global optimization over continuous spaces. *Journal of Global Optimization*, 1997, vol. 11, pp. 341–359.
30. Karaboga D., Basturk B. On the performance of artificial bee colony (ABC) algorithm. *Applied Soft Computing*, 2008, vol. 8, pp. 687–697.
31. *SIPI Image Database*. Available at: http://sipi.usc.edu/database/ (accessed 18 April 2018).

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12-ти языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org