Алгоритм встраивания информации в пары блоков ДКП-коэффициентов сжатого цифрового изображения

О.О. Евсютин[1], Р.В. Мещеряков[1], А.В. Ращупкина[1]
eoo@keva.tusur.ru|mrv@keva.tusur.ru|angelinara@mail.ru
[1]Томский государственный университет систем управления и радиоэлектроники, Томск, Россия

Один из известных способов защиты конфиденциальной информации основан на использовании стеганографического кодирования, когда защищенная передача данных реализуется с сокрытием самого факта передачи. В данной работе предлагается новый стеганографический алгоритм, работающий со сжатыми цифровыми изображениями. Отличительной особенностью данного алгоритма является использование пар схожих блоков ДКП-коэффициентов JPEG-изображения для встраивания частей сообщения. Операция встраивания отдельных битов сообщения состоит в задании определенной разности между соответствующими коэффициентами двух блоков. Для повышения эффективности стеганографического встраивания использована модификация генетического алгоритма, основанная на троичной логике. С помощью генетического алгоритма определяется наилучший вариант распределения изменений между соответствующими элементами каждой пары блоков, выбранной при встраивании. Целевой функцией является величина PSNR. Полученный алгоритм обеспечивает высокое качество встраивания и позволяет избежать существенных искажений модели исходного изображения при встраивании секретного сообщения за счет использования пар схожих блоков.

Ключевые слова: *информационная безопасность, защита данных, цифровая стеганография, сокрытие данных, JPEG.*

Algorithm of the information embedding into the pairs of blocks of the compressed digital image DCT-coefficients

O.O. Evsutin[1], R.V. Meshcheryakov[1], A.V. Rashchupkina[1]
eoo@keva.tusur.ru|mrv@keva.tusur.ru|angelinara@mail.ru
[1]Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russia

One of the known methods of the confidential information protection is based on the steganographic coding use when the protected data transfer is implemented with concealment of the fact of transmission. The new steganographic algorithm working with the compressed digital images is offered in this paper. The difference of this algorithm is use of pairs of the similar blocks of the JPEG image DCT-coefficients for the message parts embedding. Operation of the message separate bits embedding consists in specifying of a certain difference between the appropriate coefficients of two blocks. The modification of the genetic algorithm based on ternary logic is used for increase in the steganographic embedding efficiency. By means of the genetic algorithm is defined the best version of distribution of changes between the appropriate elements of each blocks pair selected in the embedding process. Value of PSNR is the object function. The received algorithm provides the high embedding quality and allows to avoid essential distortions of the initial image model in the process of the confidential message embedding due to use of pairs of the similar blocks.

Keywords: *information security, data protection, digital steganography, data hiding, JPEG.*

1. Введение

Одно из современных направлений защищенной передачи данных в информационных системах основано на использовании методов цифровой стеганографии, реализующих встраивание в цифровые объекты скрытых информационных последовательностей различного назначения.

Стеганографические методы защиты информации позволяют решать такие задачи, как обеспечение конфиденциальности информации и обеспечение аутентификации цифровых объектов [6].

В настоящем исследовании речь идет о встраивании информации в сжатые JPEG-изображения. При работе с такими изображениями встраивание осуществляется посредством внесения изменений в квантованные коэффициенты дискретного косинусного преобразования (ДКП-коэффициенты). Соответствующие алгоритмы можно разделить на два класса: алгоритмы, оперирующие отдельными ДКП-коэффициентами, и алгоритмы, оперирующие группами ДКП-коэффициентов. Во втором случае для встраивания одного элемента данных секретного сообщения используется два и более ДКП-коэффициента, и встраивание заключается в установлении определенного соотношения между данными коэффициентами в зависимости от значения встраиваемого элемента данных.

Основной целью данной работы является получение алгоритма встраивания информации в сжатые JPEG-изображения, обеспечивающего высокое качество стегоизображения за счет адаптации встраивания к изображению–контейнеру при использовании для встраивания элементов сообщения групп ДКП-коэффициентов.

2. Предшествующие работы

Большинство алгоритмов, работающих с JPEG-изображениями, относится к первому классу, когда элементы сообщения независимым образом распределяются по отдельным ДКП-коэффициентам. В качестве примеров можно отметить алгоритмы, основанные на методе PM1 [1, 12], различные LSB-подобные алгоритмы [2, 9], алгоритмы, основанные на методе QIM [3, 10] и т.д.

Классическим примером алгоритма, реализующего встраивание элементов сообщения в группы ДКП-коэффициентов, является алгоритм, представленный в работе [13]. Он встраивает один бит сообщения (цифрового водяного знака) в пару среднечастотных ДКП-коэффициентов. Встраивание заключается в изменении данных коэффициентов таким образом, чтобы модуль их

разности был больше или меньше некоторой фиксированной величины в зависимости от значения встраиваемого бита.

Схожий алгоритм, встраивающий два бита сообщения в пару ДКП-коэффициентов, представлен в работе [7]. В данном случае встраивание изменяет соотношение между выбранными коэффициентами и знак их среднего арифметического значения.

В настоящее время в рассматриваемом направлении цифровой стеганографии появляются работы, в которых встраивание сообщения осуществляется более чем в одно изображение.

В работах [4, 5] предлагается встраивать сообщение в несколько изображений одной сцены, например, в несколько последовательно полученных фотоизображений. В [5] предлагается использовать два изображения, в более позднем исследовании [4] – произвольное количество изображений.

В [11] предлагается алгоритм встраивания информации в схожие между собой блоки ДКП-коэффициентов стереопар. Схожесть блоков определяется сопоставлением низкочастотных областей ДКП-спектра, а встраивание осуществляется в области средних частот.

Необходимо отметить, что в данных исследованиях не идет речь о схемах разделения секрета, когда секретное сообщение распределяется между некоторым количеством различных изображений. В рассматриваемом случае предполагается передача всех использованных для встраивания цифровых изображений одному получателю.

Преимущество использования нескольких изображений для встраивания одного сообщения заключается в уменьшении количества изменений, приходящихся на одно изображение, за счет чего повышается устойчивость перед стегоанализом.

3. Методы исследования

В данном разделе представлены основные положения, лежащие в основе проведенного исследования.

3.1 Встраивание информации в пары блоков ДКП-коэффициентов

Рассмотрим алгоритм встраивания, представленный в статье [11]. Кроме отмеченного преимущества подход, реализуемый данным алгоритмом, обладает также и недостатком, связанным с нетипичностью использования стереоизображений в обычной переписке пользователей, привлекающей нежелательное внимание к стегоконтейнеру. Однако данный подход может быть легко перенесен на встраивание информации в одиночные изображения.

Встраивание сообщения в стереопару в соответствии с [11] осуществляется следующим образом.

В блоках ДКП-коэффициентов выделяется область поиска, состоящая из 6 низкочастотных элементов, и область встраивания, состоящая 21 среднечастотного элемента. Для каждого блока левого изображения, входящего в стереопару, находится наиболее похожий на него блок в правом изображении. Поиск ведется в квадратной области, состоящей из $K \times K$ блоков. Критерием схожести является минимальность суммы квадратов разностей соответствующих ДКП-коэффициентов, рассчитанной для областей поиска пары блоков.

После нахождения парного блока вычисляются разности между парами соответствующих ДКП-коэффициентов, принадлежащих областям встраивания. Пары равных друг другу ДКП-коэффициентов используются далее для встраивания элементов сообщения, а все прочие пары ДКП-коэффициентов изменяются таким образом, чтобы разности между ними увеличились на единицу по абсолютному значению.

Перед встраиванием каждые три бита сообщения представляются в виде двух чисел из множества $\{-1, 0, 1\}$. Каждое из таких чисел встраивается в пару соответствующих ДКП-коэффициентов двух схожих блоков стереопары. Для этого между данными коэффициентами устанавливается разность, соответствующая встраиваемому числу.

Необходимо отметить, что область поиска не изменяется при встраивании сообщения, поэтому поиск схожих блоков может быть безошибочно повторен на этапе извлечения встроенного сообщения.

Описанный подход к встраиванию сообщения в стереопару может быть перенесен на встраивание в одиночные изображения достаточно простым образом, если вести поиск парных блоков ДКП-коэффициентов по единственному имеющемуся изображению.

3.2 Оптимизация встраивания с помощью генетического алгоритма

Для повышения эффективности работы стеганографических алгоритмов во многих исследованиях ставятся задачи оптимизации, решаемые с помощью метаэвристик, как это можно увидеть, например, из обзорной работы [8]. Достаточно часто для этого применяется генетический алгоритм.

В рассматриваемом подходе к встраиванию информации в сжатые JPEG-изображения возможность для оптимизации появляется при выборе конкретного способа установления необходимого разностного соотношения между парой ДКП-коэффициентов.

Пример представлен на рис. 1 для случая, когда встраивание производится в пары коэффициентов с произвольным исходным значением разности.

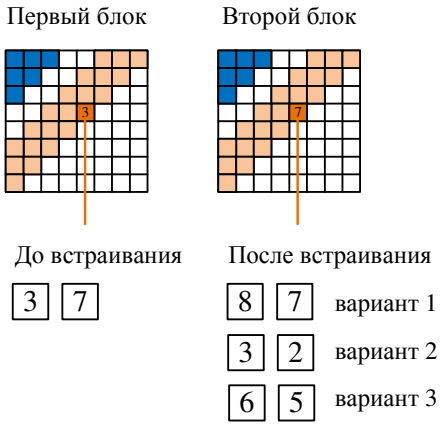

Рис. 1. Выбор способа изменения разности между парами ДКП-коэффициентов

Для решения соответствующей задачи оптимизации в настоящем исследовании используется модификация генетического алгоритма, оперирующая векторами–особями, записанными в троичном алфавите. Длина вектора для данной пары ДКП-блоков соответствует количеству пар ДКП-коэффициентов, используемых для встраивания, а значения, принимаемые отдельными элементами, имеют следующий смысл:

1) 0 – изменяется коэффициент первого блока;
2) 1 – изменяется коэффициент второго (парного) блока;
3) 2 – равные изменения вносятся в оба коэффициента.

В качестве целевой функции принимается величина PSNR.

4. Предлагаемый алгоритм

В данном разделе представлен алгоритм, реализующий встраивание информации в пары блоков ДКП-коэффициентов сжатого цифрового изображения с использованием генетического алгоритма.

Вход:

сообщение $M = m_1 m_2 \ldots m_L$, $m_i \in \{0,1\}$, $i = \overline{1, L}$; пустой стегоконтейнер — цифровое изображение, сжатое по методу JPEG; параметр глубины поиска K; порог схожести блоков T; размер области встраивания u; параметры генетического алгоритма.

Выход:

заполненный стегоконтейнер.

Шаг 1. Преобразовать сообщение M, записанное в двоичном алфавите {0, 1}, в сообщение M', записанное в алфавите {–1, 0, 1}.

Шаг 2. Восстановить из JPEG-файла блоки квантованных ДКП-коэффициентов для трех компонент цветового пространства YCbCr.

Шаг 3. Создать пустой список S для хранения номеров заполненных ДКП-блоков.

Шаг 4. Для $i = \overline{1, N}$, где N — количество ДКП-блоков, выполнить следующее:

Шаг 4.1. Выбрать очередной ДКП-блок $\mathbf{C}_i$.

Шаг 4.2. Если номер выбранного блока содержится в списке S, пропустить данный блок. В противном случае перейти к следующему шагу.

Шаг 4.3. В окрестности Мура порядка K выбрать первый найденный ДКП-блок $\mathbf{C}_j$, $i \neq j$, такой, что $d(\mathbf{C}_i, \mathbf{C}_j) < T$, где $d(\mathbf{C}_i, \mathbf{C}_j) = \sum_{l=0}^{5} \left(c_i^l - c_j^l\right)^2$ и номер данного блока отсутствует в списке S. Если блок, удовлетворяющий данному условию, отсутствует в окрестности блока $\mathbf{C}_i$, то принять в качестве $\mathbf{C}_j$ блок с наименьшим значением $d(\mathbf{C}_i, \mathbf{C}_j)$.

Шаг 4.4. Сгенерировать популяцию генетического алгоритма, состоящую из r особей вида $\mathbf{p}^k = (p_1^k, p_2^k, \ldots, p_u^k)$, $p_l^k \in \{0, 1, 2\}$.

Шаг 4.5. Развивать популяцию генетического алгоритма в течение τ итераций, приняв за целевую функцию значение PSNR, рассчитываемое для блоков пикселей, восстанавливаемых из ДКП-блоков $\mathbf{C}_i$ и $\mathbf{C}_j$.

Шаг 4.6. Выбрать особь с наибольшим значением целевой функции $\mathbf{p}^{\text{best}} = (p_1^{\text{best}}, p_2^{\text{best}}, \ldots, p_u^{\text{best}})$.

Шаг 4.7. Встроить часть последовательности M' в пару ДКП-блоков $\mathbf{C}_i$ и $\mathbf{C}_j$ следующим образом:

$\forall\, l = \overline{1, u}$,

если $p_l^{\text{best}} = 0$, то

$\tilde{c}_i^l = c_i^l + \Delta$,

$\tilde{c}_j^l = c_j^l$,

если $p_l^{\text{best}} = 1$, то

$\tilde{c}_i^l = c_i^l$,

$\tilde{c}_j^l = c_j^l + \Delta$,

если $p_l^{\text{best}} = 2$, то

$\tilde{c}_i^l = c_i^l + \Delta/2$,

$\tilde{c}_j^l = c_j^l + \Delta/2$,

где Δ – это величина изменений, необходимых для установления заданной разности между коэффициентами c_i^l и c_j^l, зависящая от значения встраиваемого элемента последовательности M'.

Шаг 4.8. Добавить номера блоков $\mathbf{C}_i$ и $\mathbf{C}_j$ в список S.

Шаг 5. Осуществить статистическое кодирование ДКП-коэффициентов и завершить алгоритм.

Можно увидеть, что в представленном алгоритме встраивание осуществляется в пары ДКП-коэффициентов независимо от исходного значения разности между ними. Это позволяет более точно оценивать емкость изображения–контейнера до начала встраивания.

Алгоритм извлечения является достаточно очевидным и в настоящей статье не приводится.

5. Вычислительные эксперименты и их обсуждение

Вычислительные эксперименты с полученным алгоритмом проводились на выборке из 9 полноцветных тестовых JPEG-изображений разрешением 512×512 пикселей: «Airplane», «Baboon», «Earth», «House», «Lenna», «Peppers», «Sailboat», «Splash», «Tiffany» [14]. Встраиваемые сообщения представляли собой тексты на русском языке, сжатые с помощью программы–архиватора.

Примеры тестовых изображений приведены на рис. 2.

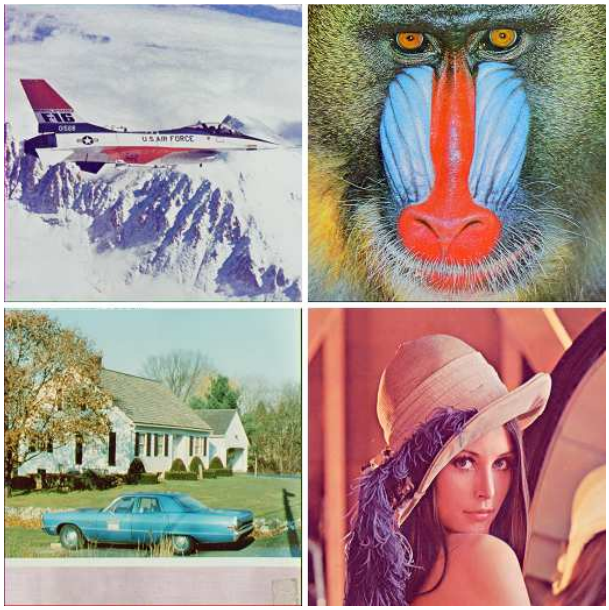

Рис. 2. Примеры тестовых изображений.

На рис. 3 представлена зависимость значения PSNR от длины встраиваемого сообщения, полученная для разработанного алгоритма посредством усреднения результатов экспериментов по всей тестовой выборке.

Для оценки влияния генетического алгоритма на качество встраивания на этом же графике представлена аналогичная зависимость для упрощенной версии разработанного алгоритма. В этой версии выбор пар схожих ДКП-блоков осуществлялся так же, как и в основном алгоритме, но решение об изменении того или

иного коэффициента в каждой паре принималось случайным образом.

Можно увидеть, что применение генетического алгоритма позволяет существенно повысить качество встраивания, улучшение составляет более 1 дБ.

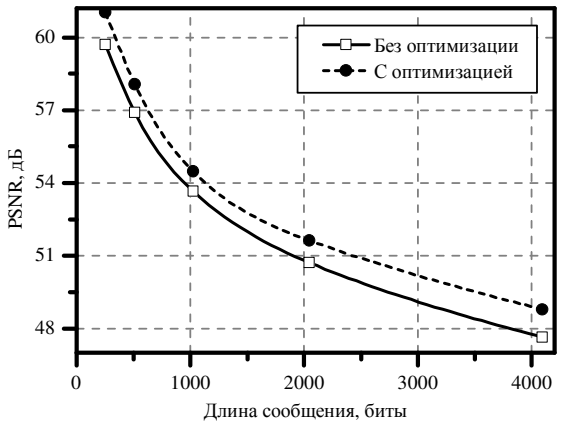

Рис. 3. Зависимость качества стегоконтейнера от объема встраиваемого сообщения.

На рис. 4 представлены примеры стегоизображений, полученных с помощью предложенного алгоритма. Объем встраиваемой информации в каждом случае составлял 4096 битов. Можно увидеть, что встраивание не приводит к появлению на стегоизображениях заметных артефактов.

Рис. 4. Примеры стегоизображений

В качестве недостатка нашего алгоритма в сравнении с известными аналогами можно отметить меньшую максимальную емкость. Однако это характерно для всех стеганографических алгоритмов, которые используют для встраивания отдельных битов сообщения группы ДКП-коэффициентов, либо осуществляют встраивание битов сообщения в одиночные ДКП-коэффициенты, выбирая их по некоторому критерию из множества имеющихся ДКП-коэффициентов.

Примеры подобных алгоритмов представлены в работах [7, 13]. Результаты вычислительных экспериментов с данными алгоритмами показаны в табл. 1. В данных экспериментах использовались те же тестовые изображения, что и при исследовании алгоритма, полученного в настоящей работе.

Длина сообщения, биты	PSNR, дБ		
	Алгоритм [7]	Алгоритм [13]	Полученный алгоритм
2 712	40,71	—	50,65
4 096	—	34,41	48,79

Табл. 1. Сравнение полученного алгоритма с аналогами

Можно увидеть, что предложенный алгоритм обеспечивает значительное преимущество по сравнению с алгоритмами–аналогами. Данное преимущество объясняется тем, что операция встраивания, на которой основывается предложенный алгоритм, вносит меньшее количество искажений в изображение–контейнер по сравнению с операциями, используемыми в [7, 13]. Дополнительное преимущество достигается за счет применения генетического алгоритма для оптимизации встраивания.

6. Заключение

В данной работе представлен новый алгоритм встраивания информации в сжатые JPEG-изображения, отличающийся использованием пар схожих блоков ДКП-коэффициентов для формирования пространства сокрытия и применением генетического алгоритма для повышения качества встраивания.

Предлагаемый подход к встраиванию информации в сжатые JPEG-изображения, реализованный в представленном алгоритме, дает потенциал для новых исследований, направленных на получение новых эффективных стеганографических алгоритмов. В частности, можно предложить новые решения по выбору пар схожих ДКП-блоков и ввести более сложные критерии схожести. Развитию данного подхода будут посвящены новые исследования авторов работы.

Отдельно необходимо отметить, что сформулированная в разделе 3.2 задача оптимизации может быть перенесена на иные подходы к встраиванию сообщения в наборы изображений, представленные в известных исследованиях.

7. Благодарности

Данная работа выполнена при поддержке РФФИ (проект № 16-47-700350 р_а).

8. Литература

[1] Евсютин О.О. Алгоритм встраивания информации в сжатые цифровые изображения на основе операции замены с применением оптимизации / О.О. Евсютин, А.А. Шелупанов, Р.В. Мещеряков, Д.О. Бондаренко // Компьютерная оптика. – 2017. – Т. 41, № 3. – С. 412–421.

[2] Chang C.C. A steganographic method based upon JPEG and quantization table modification / C.C. Chang, T.S. Chen, L.Z. Chung // Information Sciences. – 2002. – Vol. 141(1–2). – P. 123–138.

[3] Chen B. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding / B. Chen, G.W. Wornell // IEEE Transactions on Information Theory. – 2001. –Vol. 47(4). – P. 1423–1443.

[4] Denemark T. Steganography with Multiple JPEG Images of the Same Scene / T. Denemark, J. Fridrich // IEEE Transactions on Information Forensics and Security. – 2017. – Vol. 12(10). – P. 2308–2319.

[5] Denemark T. Steganography with Two JPEGs of the Same Scene / T. Denemark, J. Fridrich // Proceedings of the 42nd International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2017). — USA, New Orleans, LA. – 2017.
[6] Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. – Cambridge: Cambridge University Press, 2010. – 437 p.
[7] Fujimura M. New data hiding scheme using method of embedding two bits data into two DCT coefficients / M. Fujimura, T. Takano, S. Baba, H. Kuroda // Proceedings of the International Conferences on Signal Processing, Image Processing and Pattern Recognition (SIP 2010) and Multimedia, Computer Graphics and Broadcasting (MulGraB 2010). – Korea Jeju, Island. – 2010. – P. 156–164.
[8] Huang H.C. Survey of Bio-inspired Computing for Information Hiding // Journal of Information Hiding and Multimedia Signal Processing. – 2015. – Vol. 6(3). — P. 430–443.
[9] Li X. A steganographic method based upon JPEG and particle swarm optimization algorithm / X. Li, J. Wang // Information Sciences. – 2007. – Vol. 177(15). – P. 3099–3109.
[10] Noda H. High-performance JPEG steganography using quantization index modulation in DCT domain / H. Noda, M. Niimi, E. Kawaguchi // Pattern Recognition Letters. – 2006. – Vol. 27(5). – P. 455–461.
[11] Yang W. Reversible DCT-based data hiding in stereo images / W. Yang, L. Chen // Multimedia Tools and Applications. – 2015. – Vol. 74(17). – P. 7181–7193.
[12] Yu L. PM1 steganography in JPEG images using genetic algorithm / L. Yu, Y. Zhao, R. Ni, Z. Zhu // Soft Computing. – 2009. – Vol. 13(4). – P. 393–400.
[13] Zhao J. Embedding robust labels into images for copyright protection / J. Zhao, E. Koch // Proceedings of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies (KnowRight'95). – Austria, Vienna. – 1995. – P. 242–251.
[14] SIPI Image Database [Электронный ресурс]. – URL: http://sipi.usc.edu/database/ (дата обращения 01.12.2016).

Об авторах

Евсютин Олег Олегович, канд. техн. наук, доцент кафедры безопасности информационных систем факультета безопасности Томского государственного университета систем управления и радиоэлектроники. Его e-mail eoo@keva.tusur.ru.

Мещеряков Роман Валерьевич, д-р техн. наук, заведующий кафедрой безопасности информационных систем факультета безопасности Томского государственного университета систем управления и радиоэлектроники. Его e-mail mrv@keva.tusur.ru.

Ращупкина Анжелика Владимировна, инженер кафедры безопасности информационных систем факультета безопасности Томского государственного университета систем управления и радиоэлектроники. Ее e-mail angelinara@mail.ru.