УДК 004.056.5

В.А. Жеглов, А.А. Яковенко, Н.И. Кушниренко

Одесский национальный политехнический университет, Одесса

СТЕГАНОГРАФИЧЕСКАЯ ТЕХНИКА ДЛЯ ИЗОБРАЖЕНИЙ JPEG С ИСПОЛЬЗОВАНИЕМ ОПТИМАЛЬНЫХ ПАТТЕРНОВ ВНЕДРЕНИЯ

В данной статье была разработана новая стеганографическая система для работы с изображениями формата JPEG. Описаны основные стеганографические методы, алгоритм сжатия JPEG. Выделены основные недостатки в современных алгоритмах стеганографии. Описан новый метод, основной задачей которого является уменьшение заметности внедрения информации в изображение и добавление криптографической системы.

Ключевые слова: *цифровая стеганография, сокрытие информации, формат JPEG, наименьше значащий бит, цифровые водяные знаки.*

Введение

В современном мире, стеганография активно применяется не только в области защиты информации и информационной безопасности, но и в других областях. На данный момент, в США насчитывается более 100 патентов по стеганографии [1]. Существует множество стеганографических способов, начиная от LSB стеганографии, до продовольственной стеганографии (Food steganography), которая рассчитывает метод и систему добавления пищевой добавки [2].

В эксперименте будет использован один из самых популярных форматов изображения – JPEG. Алгоритм JPEG в наибольшей степени пригоден для сжатия фотографий и картин, содержащих реалистичные сцены с плавными переходами яркости и цвета. В этом алгоритме изображение преобразуется из цветового пространства RGB в YCbCr. Часто каналы Cb и Cr прореживают, то есть блоку пикселей присваивается усредненное значение. Например, после прореживания в 2 раза по вертикали и горизонтали, пиксели будут иметь соответствие.

Затем значения каналов разбиваются на блоки 8×8. Каждый блок подвергается дискретному косинусному преобразованию (ДКП), являющемся разновидностью дискретного преобразования Фурье. Получаем матрицу коэффициентов 8×8. Получившиеся коэффициенты квантуются, т.е. каждый умножается на коэффициент таблицы квантования. Затем они кодируются кодами Хаффмана [3].

Основной материал

Стеганографические алгоритмы для формата JPEG

Существует множество стеганографических алгоритмов с использованием формата JPEG. Наиболее популярные из них используют алгоритм с использованием наименьше значащих битов (НЗБ) в дискретном косинусном преобразовании (ДКП).

Одним из алгоритмов, которые использует НЗБ, является JSTEG [4]. Он представляет собой замену НЗБ в изображениях JPEG, сжатых с потерями. JSTEG заменяет младший бит полученных после квантования частотных коэффициентов ДКП на бит секретного сообщения. Этот метод имеет несколько преимуществ. Во-первых, формат изображения JPEG / JFIF стал фактическим стандартом для передачи через USENET и для хранения на FTP-сайтах. Во-вторых, стеганографические данные в JPEG-изображениях труднее обнаружить не вооруженным глазом, чем те же данные в сырых 8-битных или 24-битных изображениях. Кроме того, широкий контроль над квантование изображения сильно затрудняет установление того, действительно ли неточности, которые появляются, вызваны стеганографическими данными или низкокачественным квантованием.

Процедура кодирования JPEG делит изображение на 8×8 блоков пикселей в цветовом пространстве YCbCr. Затем они проходят через дискретное косинусное преобразование (ДКП) [5] и результирующие частотные коэффициенты масштабируются до обнаружения тех, которые человеческий глаз не обнаружит при нормальных условиях. Если стеганографические данные загружаются в JPEG изображения, загрузка происходит после этого шага. Биты младшего разряда всех ненулевых частотных коэффициентов заменяются последовательными битами из стеганографического исходного файла, и эти измененные коэффициенты сжимаются при помощи кода Хаффмана [3].

В каждом таком алгоритме существуют свои недостатки, которые исправлению которых посвящена эта работа. Среди главных недостатков, можно выделить заметность. Алгоритмы, которые мы описывали, не имеют механизма, определяющего изменение заметности для человеческого глаза. Соответственно в них, заменяются коэффициенты ДКП, имеющим малое значения, а это в свою очередь,

привод к заметным изменениям изображения. Так же алгоритм не учитывает значения, которые содержатся в соответствующих элементах, в которых происходит скрытие информации.

В данных алгоритмах, стеганографические приёмы никак не дополняются криптографией. Не происходит шифрование внедряемых данных.

Поэтому, нужно выделить несколько требований к новому стеганографическому алгоритму.

Требования к новому стеганографическому алгоритму

Первое требование это незаметность внедрения. В данном алгоритме добивается невысокое максимальное изменения пикселя в изображениях. Необходима оценка заметности изменения блока, с внедряемой информацией. Эта оценка производится на основе психовизуальной модели восприятия человеком изображения. Соответственно, в этой части есть возможность использования разных психовизуальных моделей JPEG. т.к. для формата JPEG существует больше количество надстроек сжатия в виде различных таблиц квантования, соответственно появляется возможность использования разных психовизуальных моделей JPEG [6].

Еще одним требование к алгоритму будет подбор оптимального блока внедрения. Эта процедура будет основываться на содержании блока изображения, в котором в данный момент происходит внедрение информации. К каждому блоку изображения будет осуществляться индивидуальный подход.

Будет внедрена возможность настройки подмножества коэффициентов ДКП, подверженных изменению в процессе внедрения. Эта настройка позволит регулировать заметность изменений и объём добавляемых данных.

Необходима возможность определения минимального значения квантованного коэффициента ДКП, для которого внедрение не производится. Это позволит как в предыдущем пункте, изменять объём внедряемой информации соответственно жертвуя при этом заметностью изменений в изображении.

Алгоритму необходимо использование криптографии в виде шифрование/дешифрования скрытого сообщения с помощью секретного ключа.

Так же, для еще большего уменьшение заметности изменения в изображении, необходимо добавить возможность пропуска JPEG-блоков, для которых внедрение будет слишком заметным.

Описание алгоритма внедрения

Для данного эксперимента берется чёрно-белое изображения размером 600 на 400 пикселей (рис. 1).

Для начала, определяется ёмкость внедрения *C*. Для этого, вначале, было определенно минимальное значение квантованного коэффициента ДКП. После, блок изображения, который не подходит по заданным параметрам, отсеивается. Это необходимо, для отсеивания блоков, в которых внедрение информации будет слишком заметным.

Рис. 1. Тестовое изображение

В данном алгоритме, внедряется не отдельные биты сообщения, а соответствующие ему битовые блоки. Размер данных блоков будет определяться заранее, и зависеть от значения, которое определяет количество битов, внедряемых в блок. Поэтому для начала, они генерируются и сортируются. Для этого необходим хеш SHA-512 [7]. Генерируется битовый блок, после чего, он проходит через хеш-функцию с добавлением к блоку секретного ключа *k*. После, получившаяся строка переводится в бинарный вектор. Первый бит хеш-значения, будет определять, к какому набору блоков (паттерну) принадлежит данный блок. Таким образом, все 2^n вариантов блока внедрения разделяются на 2 группы. Потенциально, есть возможность передавать больше одного бита на блок.

Алгоритм обработки блока JPEG

Для работы алгоритма, необходимо блок JPEG 8×8, поэтому из исходного изображения, вырезается такой блок. Далее все манипуляции, будут происходить с этим блоком.

После, выполняется алгоритм JPEG по сжатию. С блоком производится дискретное косинусное преобразование, после которого следует квантование. Далее производится фильтрация компонентов следующим образом. К квантованной матрицы 8×8 применяется маска, которая помечает, какие из ДКП-компонентов блока будут подвергаться изменению. Низкочастотные компоненты исключаются благодаря сильному влиянию на изменение заметности, а высокочастотные – по соображениям размера сжатого изображения. После чего, применяется дополнительная фильтрация. В этой фильтрации отсеиваются элементы, которые ниже заранее заданного порога T. В эксперименте, порог T соответствует единице, т.к. изменение 1 на 0 и 0 на 1 сильно отобразится на заметности изменений. После

фильтрования, определяется количество оставшихся элементов, и если оно меньше числа внедряемых битов, такой блок изображения отбрасывается.

Следующим этапом является внедрения информации. Для этого, берется соответствующий бит передаваемого сообщения. В соответствии с этим битом, программа определяет, с каким паттерном (паттерном «0» или паттерном «1») будет продолжаться работа. После, в компоненты блока, который прошёл фильтрацию, происходит запись данных алгоритмом LSB [8]. Цикл внедрения происходит до тех пор, пока из соответствующего контейнера не найдётся элемент, который привнесёт наименьшие изменения в блок. Т.к. в паттернах «1» и «0», находится все возможные вариации вектора битов, размер которого соответствует числу внедряемых битов в блок, то с 50% вероятностью, младше значащие биты компонентов блока, будут совпадать с паттерном из «правильной» группы. Что означает, что в будущем при извлечении информации, алгоритм выдаст правильный бит, хотя блок изображения никак не изменялся. В противном случае, определяется блок, который внесёт минимальные изменения заметности.

Далее, следуя требованиям к алгоритму, необходимо определение заметности, на основе психовизуальной модели JPEG. Преимущество данного алгоритма заключается в том, что определяется заметность изменений не всего изображения. Определяется заметность лишь вырезанного блока 8×8. Для этого необходимы два блока JPEG, с исходным изображением и с тем же блоком исходного изображения, но в который уже внедрена информация. С этими блоками производится дискретное косинусное преобразование, после чего полученные коэффициенты квантуются. Для определения разности заметности, находится «мощность блоков». После чего, находится мощность разности блоков. Соответственно, отношение мощности разности к средней мощности блоков и является коэффициентом заметности. Среди всех блоков паттерна, определяется тот, у которого наименьший коэффициент заметности.

После производится процедура воссоздание первоначального вида блока. Блок квантуется и происходит обратная функция ДКП.

Алгоритм извлечения данных

После того, как всё сообщение было внедрено в изображение, необходимо его извлечь. Алгоритм извлечения скрытой информации, похож на алгоритм её внедрения. Изображение также обрабатывается по блокам 8×8. Применяется ДКП, квантование и округление результата. После, происходит фильтрация компонентов, применяется минимальный порог T и маска M, пропуск неподходящих блоков. Из блока извлекаются наименьше значащие биты (LSB). Получившийся блок битов, проходит через хеш функцию с ключом, который определяет какой именно бит был внедрен. После этого, процедура повторяется, пока не закончится изображение. Из извлечённых битов формируется скрытое сообщение.

Результаты экспериментов

Одной из характеристик алгоритма является емкость внедрения *C*. Этот параметр отвечает за количество информации, которое можно внедрить в изображение. Этот параметр напрямую зависит от изображения, от его размера и от его характера. В данной работе приоритетным является незаметность внедрения информации. Соответственно, емкость изображений не такая большая, как могла бы быть. Этому способствует множественная фильтрация блоков изображения и их коэффициентов.

Алгоритм использует хеш SHA-512. Этим методом определяется стойкость шифрования. Шифрование стойкое настолько же, как и используемый алгоритм хеширования. Присутствует возможность изменения алгоритма, на иной. В данном случае, алгоритм SHA-512, получился наиболее подходящим под данный эксперимент.

В ходе эксперимента получено два изображения. Изначальное изображение без скрытой информации (рис. 2).

Рис. 2. Оригинальное изображение

Изображение с информацией, которая была внедрена (рис. 3).

Рис. 3. Изображение после обработки алгоритмом

Как видно из рис. 3, заметность внедрения информации в изображение минимальна. Для большей наглядности, необходим пример разницы изображений, что показан на рис. 4.

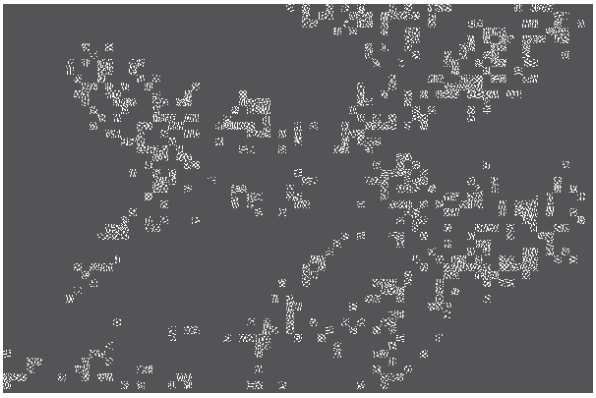

Рис. 4. Усиленная разность изображений

Из изображения видно, что изменения произошли не во всех блоках, а только в тех, которые подошли, под заданные ранее параметры.

На рис. 5 показана часть изображения, на которой видны блоки, для которых не потребовалось замены. С паттерна, нашёлся блок, при внедрении которого, не последовало никаких изменений. Центр этих блоков 8×8 отмечен точкой.

Рис. 5. Иллюстрация изменений в изображении, вызванных внедрением

Изменениям не подвергается та часть изображения, на которой нет чётких контуров. Это видно, из рисунков 3 и 4. В области изображения, где оно размытое либо не чёткое, алгоритм не внедряет информацию, считая, что внедрения в эти блоки будет слишком заметным.

В алгоритме используется маска M в виде матрицы 8×8. По заданной матрице, отсеиваются коэффициенты, которые значительным образом влияют на изображение. С помощью этого параметра, алгоритмом можно управлять наибольшей вместительности при этом жертвуя заметностью и наоборот. На рис. 6, а изображена маска 8×8.

С помощью этой маски M для изображения рис. 3 алгоритм определяет 1103 бита для записи. Для маски, изображённой на рис 6б, алгоритм определил ёмкость записи в 1703 бита. В обеих масках не были затронуты первые коэффициенты матриц, т.к. их изменение сильно влияет заметность изменений в изображении.

а	б	в
0 0 0 0 0 1 1 1	0 0 0 0 1 1 1 1	0 0 0 0 0 0 0 1;
0 0 0 0 0 1 1 1	0 0 0 1 1 1 1 1	0 0 0 0 0 0 1 1;
0 0 0 0 1 1 1 0	0 0 1 1 1 1 1 0	0 0 0 0 0 1 1 0;
0 0 0 1 1 1 0 0	0 1 1 1 1 1 0 0	0 0 0 0 1 1 0 0;
0 0 1 1 1 0 0 0	1 1 1 1 1 0 0 0	0 0 0 1 1 0 0 0;
1 1 1 1 0 0 0 0	1 1 1 1 0 0 0 0	0 0 1 1 0 0 0 0;
1 1 1 0 0 0 0 0	1 1 1 0 0 0 0 0	0 1 1 0 0 0 0 0;
1 1 0 0 0 0 0 0	1 1 0 0 0 0 0 0	1 1 0 0 0 0 0 0;

Рис. 6. Вариации маски: а – первая матрица; б – вторая матрица; в – третья матрица

Уменьшая количество затрагиваемых коэффициентов (рис. 6, в), получаем всего лишь ёмкость из 389 битов.

Так же для функции регулирования количества передаваемых битов, существует еще два параметра: количество внедряемых битов в блок и порог фильтрации коэффициентов T (минимальное значение коэффициента, которое будет изменено). В табл. 1 показаны зависимость ёмкости внедрения C от этих параметров, для тестового изображения.

Таблица 1

Зависимость ёмкости внедрения от параметров алгоритма

Количество внедряемых битов в блок	Порог, T	Ёмкость, C
8	1	1103
10	2	863
8	5	176
7	0	1211

Из табл. 1 можно сделать вывод, что на ёмкость значительным образом влияет порог фильтрации.

Оптимальные параметры для работы алгоритма приведены в табл. 2.

Таблица 2

Оптимальные параметры

Количество внедряемых битов в блок	Порог, *T*	Ёмкость, *C*
8	1	1103

Выводы

В данной работе был рассмотрен стеганографический алгоритм скрытия информации в изображении формата JPEG. В статье были описаны основные принципы современной стеганографии и принцип работы формата JPEG. Был произведён анализ существующих алгоритмов и определены их недостатки. На основе этого анализа, был создан алгоритм, который минимизирует недостатки ранее созданных алгоритмов. Главным преимуществом является его вариативность. В программе есть возможность изменения нескольких параметров для определения лучшей конфигурации алгоритма. Этими параметрами являются маска-матрица M, минимальный порог T для коэффициентов изображения, количество внедряемых битов в блок изображения. Отталкиваясь от поставленной цели, с их помощью, можно варьировать количество внедряемых битов в изображения жертвуя заметностью изменений. Были определенны оптимальные параметры алгоритма, руководствуясь целью минимизировать заметность изменений в изображении.

Список литературы

1. Patent lawyer directory [Electronic resource], Patent lawyer directory, (In English), Mode of access: www. URL: http://patents.com/search/?top_keyword=steganography (accessed 20.05.2017). Title from screen.

2. Kush R. Varshne, Lav R. Varshney Food steganography Patent United States Pub. No.: US 2015/0059438 Date: Mar. 5, 2015.

3. ITU: ISO/IEC 10918-1 : 1993(E) CCIT Recommendation T.81, http://www.w3.org/Graphics/JPEG/itu-t81.pdf, (1993).

4. Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani, (2012), Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm [Text], International Journal of Computer and Electrical Engineering, Vol. 4, No. 4. – Pp. 458-462.

5. Википедия свободная энциклопедия [Электронный ресурс] Дискретное косинусное преобразование. Режим доступа: www URL: https://en.wikipedia.org/wiki/Discrete_cosine_transform (Последний доступ 17.05.2017) Название с экрана.

6. Impulse Adventure JPEG [Electronic resource], Compression Quality from Quantization Tables, (In English), Mode of access: www. URL: http://impulseadventure.com/photo/ jpeg-quantization.html (accessed 10.05.2017). Title from screen.

7. Баричев С.Г. Основы современной криптографии [Текст] / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов // Учебный курс. – 2011. – С. 116-121.

8. Конахович Г.Ф. Компьютерная стеганография. Теория и практика [Текст] / Г.Ф. Конахович, А.Ю. Пузыренко; ред. Ю.А. Шпак. – К.: «МК-Пресс», 2006. – С. 76-89.

Поступила в редколлегию 5.05.2017

Рецензент: д-р техн. наук проф. Г.А. Кучук, Харьковский национальный университет Воздушных Сил им. И. Кожедуба, Харьков.

СТЕГАНОГРАФІЧНА ТЕХНІКА ДЛЯ ЗОБРАЖЕНЬ JPEG З ВИКОРИСТАННЯМ ОПТИМАЛЬНИХ ПАТЕРНІВ ВПРОВАДЖЕННЯ

В.О. Жеглов, О.О. Яковенко, Н.І. Кушніренко

У даній статті була розроблена нова стеганографічна система для роботи з зображеннями формату JPEG. Описано основні стеганографічні методи, алгоритм стиснення JPEG. Виділено основні недоліки в сучасних алгоритмах стеганографії. Описано новий метод, основним завданням якого є зменшення помітності впровадження інформації в зображення і додавання криптографічної системи.

Ключові слова: *цифрова стеганографія, приховування інформації, формат JPEG, найменше значущий біт, цифрові водяні знаки.*

STEGANOGRAPHIC TECHNIQUE FOR JPEG IMAGES USING OPTIMAL EMBEDDING PATTERNS

V. Zheglov O. Iakovenko N. Kushnirenko

In this article, a new steganographic system has been developed for JPEG images The main steganographic method relies on JPEG compression algorithm.The method is designed to address shortcomings of modern steganographic algorithims, namely, to reduce the visibility of embedded data and add a cryptographic layer to protect embedded message.

Keywords: *digital steganography, information concealment, JPEG format, least significant bit, digital watermarks.*