УДК 004.056.5

С.А. Сейеди, Р.Х. Садыхов

СРАВНЕНИЕ МЕТОДОВ СТЕГАНОГРАФИИ В ИЗОБРАЖЕНИЯХ

Стеганография – это метод сокрытия информации в объектах различных форматов (контейнерах). Существует большое разнообразие методов для конкретных контейнеров, в которые скрытно записывается информация. Наиболее часто в качестве контейнера используются цифровые изображения, которые без искажений могут пересылаться по компьютерным сетям. Исследуется основная методика стеганографии, ее сильные и слабые стороны. Дается сравнительная оценка основных алгоритмов стеганографии.

Введение

Назначение компьютерной безопасности состоит в защите информации от несанкционированного доступа, случайного или целенаправленного искажения данных без изменения основных свойств файлов. Криптография создавалась как методика для защиты систем связи методами кодирования и последующей расшифровки данных. Стеганография дополняет криптографию, скрывая сам факт наличия сообщения в передаваемом потоке данных. Стеганографию можно рассматривать как создание скрытого канала связи. Если криптография маскирует сообщение, то стеганография пытается скрыть наличие такого сообщения.

В табл. 1 дается сравнение трех подходов к передаче секретной информации. В криптографии для расшифровки сообщения используется секретный ключ. При перехвате сообщения недоброжелатель, если и не сможет прочесть его, то в большинстве случаев сможет исказить. Цифровая подпись подтверждает подлинность сообщения, она может быть удалена. Если недоброжелатель не знает метода инкапсуляции, стеганографическое сообщение нельзя удалить без значительного искажения контейнера.

Таблица 1

Сравнение секретных техник связи

Техника связи	Конфиденциальность	Целостность	Неустранимость
Криптография	Да	Нет	Да
Цифровая сигнатура	Нет	Да	Нет
Стеганография	Да / Нет	Да / Нет	Да / Нет

1. Обзор методов стеганографии

1.1. Различные алгоритмы инкапсуляции сообщения

Почти все форматы файлов годятся для стеганографических вставок, но формат файла-контейнера ограничивает допустимые методы стеганографии. Во всех форматах изображений существуют излишние биты, по крайней мере такие, значения которых практически не сказываются на качестве изображения. В эти биты файла изображения можно вставить скрытую информацию. Многие форматы изображений и аудиофайлов пригодны для вставки скрытой информации. На рис. 1 показаны категории файлов, для которых можно применять стеганографию.

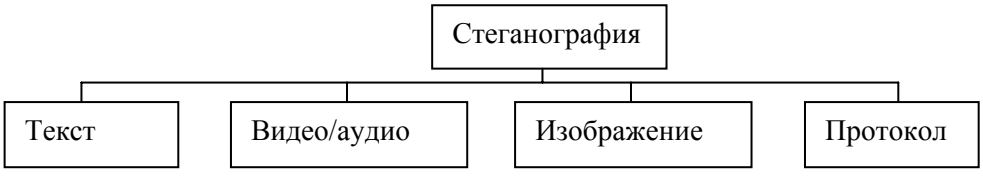

Рис.1. Различные виды приложений

1.2. Стеганографические системы

Стеганографическая система в общем виде состоит из двух компонентов: вставки и извлечения сообщения (рис. 2).

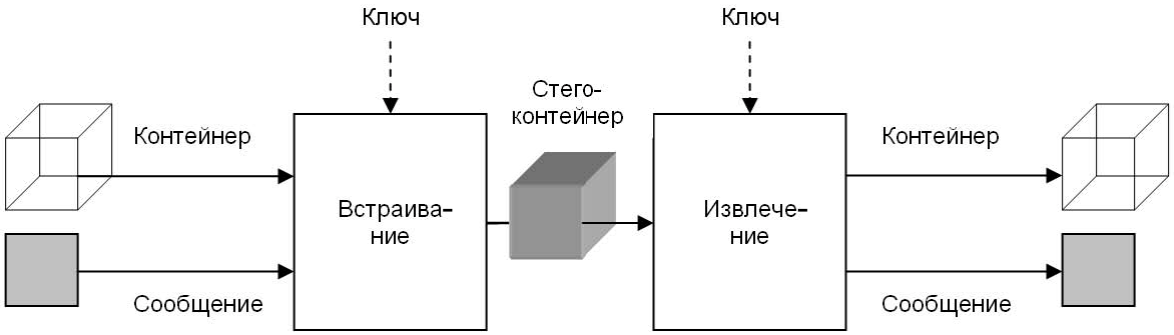

Рис. 2. Структура стеганографии

Процесс обработки стеганографического сообщения включает следующие объекты:

сообщение – данные любого типа;

контейнер – любая информация, пригодная для сокрытия в ней сообщений;

стегоконтейнер – контейнер, содержащий скрытое сообщение;

ключ (стегоключ) – секретный ключ, необходимый для шифрования (расшифровки) сообщения с целью усиления защиты.

Для обработки сообщения может использоваться пароль. Это ключевое слово, применяемое для записи и расшифровки скрытого сообщения.

2. Стеганографические изображения

Скрытое сообщение можно инкапсулировать практически во все виды данных. Большинство инструментов стеганографии ориентируется на передачу сообщения в Интернете, где значительная часть информации передается в виде изображений. При обработке изображения-контейнера учитывают формат файла, в частности методы сжатия. От этого зависят как методы инкапсуляции, так и объем стеганограммы, которую можно вставить в файл. Сложность процедур стеганографии также зависит от формата контейнера.

2.1. Классификация методов стеганографии для изображений-контейнеров

В течение всего периода развития стеганографии было разработано множество методов, зависящих от форматов изображений и от применяемого аппаратного обеспечения. Методы стеганографии для изображений можно разделить на два класса: методы для временной области [1, 2] и методы для частотной области [1–3]. Для временной области основные процедуры инкапсулируют скрытое сообщение в младшие биты цифрового кода пикселов изображения. Для частотных процедур стеганограмма вставляется в частотную характеристику изображения. Временные процедуры включают следующие методы:

– внедрение цифрового кода сообщения в изображение: незначащий или малозначащий младший бит цвета или палитры изображения заменяется битом вставляемого сообщения;

– статистические методы замены: бит изображения заменяется по некоторому статистическому закону; например биты фрагмента сообщения вставляются в псевдослучайно выбранные патчи изображения;

– частотные процедуры состоят в замене малозначащих частотных характеристик изображения, например замене некоторых коэффициентов в дискретном косинус-преобразовании (ДКП).

В частотных процедурах кроме ДКП используется дискретное вейвлет-преобразование (ДВП), эти и некоторые другие методы обычно применяются в патчах и методах расширения спектра.

3. Методы для временной области

Существуют различные методы встраивания секретного сообщения во временной области контейнера:

Метод наименее значащего бита (LSB). Во временных процедурах наиболее часто применяется метод LSB. Так, в формате градаций серого цвета с 8-битным кодированием пиксела в некоторых заданных пикселах заменяется младший бит кодировки (рис. 3).

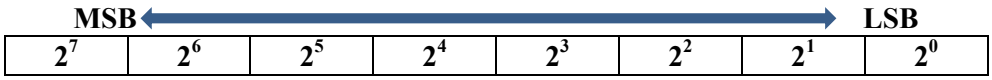

Рис. 3. Взвешивание 8-битных пикселов

При замене некоторых младших битов пикселов изображения само изображение изменяется незначительно. Математическая формула замены имеет вид [4]

$$x_i' = x_i - x_i \bmod 2^k + m_i, \tag{1}$$

где x – i-й пиксел стегограммы; x – пиксел исходного изображения; m – десятичное значение i-го блока сообщения. Номер заменяемого бита обозначен k. Процедура раскодировки очевидна – нужно собрать последние биты измененных пикселов. Формула извлечения определяется выражением

$$m_i = x_i' \bmod 2^k. \tag{2}$$

Таким образом, перестановка извлеченных m даст исходное пересылаемое сообщение. При использовании 24-битного цветового формата RGB в стеганограмме можно использовать цветовые байты. Всего можно использовать 3 бита на один пиксел. В картинку размером 800x600 пикселов можно записать скрытое сообщение объемом около 180 КБ. Например, если представление трех пикселов такого изображения представляет собой последовательность

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011),

то число 200 с двоичным кодом 11001000 будет вставлено как

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011).

Замена потребовалась только в трех подчеркнутых из восьми битов записи. Можно заменять один или два последних бита цвета, при этом глаз человека не распознает искажения параметров изображения. Предполагая равномерность распределения числовых значений заменяемых битов, получаем, что при инкапсуляции сообщения замена в среднем потребуется только в половине младших битов контейнера.

В этом методе такие параметры, как формат файла, метод сжатия изображения (предполагая сжатие без потерь) и положение бита в байте, играют важную роль. Объем сообщения и его скрытность в формате RGB лучше по сравнению с форматом градаций серого цвета. Существует

множество методов LSB инкапсуляции сообщения в формат градаций серого цвета с различными степенями успеха. Контейнер должен скрыть сообщение, LSB с одним битом применяется в форматах GIF и BMP контейнера. Файлы GIF сжимаются без потерь, они имеют небольшой размер и широко используются в Интернете. В формате GIF можно заменять младший бит в каждом байте файла. Формат BMP не использует сжатия, и файлы этого формата имеют большой объем. К сожалению, для скрытия сообщения требуется файл BMP большого объема. В наше время файлы формата BMP не передаются по Интернету и их применение может вызвать подозрение. Поэтому в стеганографии используются другие форматы.

Существуют методы LSB, заменяющие два, три и даже четыре бита цвета в формате RGB. Эти методы зависят от приложений, в которых они применяются, и здесь важно найти равновесие между качеством изображения и объемом вставляемого сообщения.

Для того чтобы затруднить выявление сообщения в стеганограмме, используются специальные методы вставки сообщения в цвета изображения, например циклическая перестановка битов сообщения, вставка только в красный байт цвета.

Цветовая палитра и LSB. В изображения, использующие заданную цветовую палитру, цвет пиксела записывают в виде индекса, обычно это 8-битное число. Например, созданный для Интернета формат GIF использует 8-битную нумерацию цветов, т. е. контейнер содержит пикселы из заданного набора 256 цветов. Для того чтобы сократить время поиска цвета по индексу в цветовой таблице, цвета упорядочивают по частоте их появления в картинке. Поэтому при однобитном методе LSB результат зависит от того, соответствует ли малое изменение индекса малому изменению цвета, неразличимому для глаз человека. Для разрешения этой проблемы существуют два способа: первый – переупорядочивание цветов по их плавному изменению, второй – добавление новых цветов, близких к табличным. Первый способ применим к изображению с градациями серого цвета [6]. В этом случае картинки практически неразличимы и выявление скрытого сообщения затруднено [5]. Для выявления скрытого сообщения и в первом и во втором случаях достаточно переупорядочить цветовую таблицу, после чего низкое качество изображения укажет на наличие вставки.

Псевдослучайные перестановки (ПП). В этом методе биты скрытого сообщения распределены по изображению случайным образом. Такой подход увеличивает трудоемкость выявления скрытого сообщения, особенно если псевдослучайный датчик генерирует последовательность сложным алгоритмом. Здесь могут возникнуть коллизии, т. е. повторение адреса заменяемого бита, что означает попытку вставки двух значений в один бит контейнера. Чтобы преодолеть коллизию, используется специальный файл, в который записываются адреса заменяемых битов. Если генерируется адрес, уже содержащийся в этом файле, то он не используется и генерируется следующее псевдослучайное число. Применение дополнительного файла усложняет как обработку стеганограммы, так и попытку выявления скрытого сообщения. Если при этом биты случайно выбираются для замены из всего поля контейнера, то такой метод может создать стеганограмму с большими и ясно различимыми повреждениями контейнера. Случай, когда старшие биты загружаются в MSB, показан на рис. 4 [6].

Псевдослучайные числа: 1, 7, 10, 13, 20, 26, 29, 35, ….

Контейнер	Секретное сообщение	Стегоконтейнер
(00101101 00011100 11011100)		(0**1**10110**1** 00**0**11**0**00 1101**0**100)
(10100110 11000100 00001100)		(10**1**00**0**10 110**1**0100 00001100)
(11010010 10101101 01100011)	ADD 11000101	(11010010 10101101 01100011)

Рис. 4. Метод псевдослучайных перестановок

Метод с использованием патчей (ИП). Этот метод является статистическим кодированием информации путем изменения некоторых статистических свойств контейнера (добавляет излишние данные к скрытому сообщению и затем размывает его по изображению с применением гауссового распределения) и использует проверку гипотез при извлечении сообщения. Секретный ключ применяется к случайно выбранному подмножеству пикселов из изображения, затем подмножество разделяется по двум патчам – A и B. Яркость одного подмножества пиксе-

лов из одного патча смещается на положительное число, а яркость пикселов из другого патча – на противоположное (отрицательное) число (рис. 5). Содержимое контейнера не зависит от изменения патчей. Контрастность в пикселах изменяется на один бит, изменение очень мало и не воспринимается визуально, тем более что средняя освещенность не изменяется [7, 8].

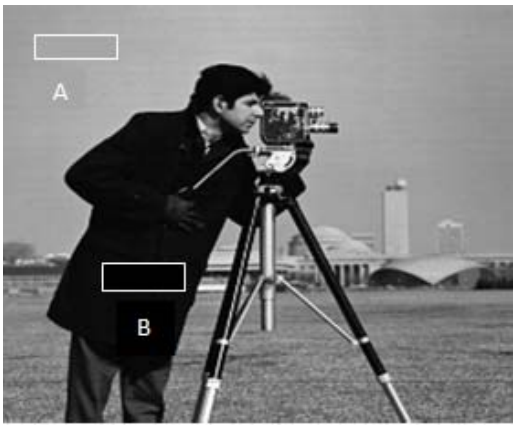

Рис. 5. Патч-метод с двумя областями

Метод расширения спектра (PC). В этом методе скрытое сообщение распределяется по контейнеру, что затрудняет выявление стеганограммы [9]. Метод предложен Марвелом для маскировки сообщения. Он комбинирует расширение спектра, кодирование с исправлением ошибок и обработку изображений для скрытия вставляемого сообщения [10]. Метод описывает расширение спектра с представлением сигнала в узкой полосе на широкополосное представление. Это может сопровождаться переносом и изменением профиля колебания с узкой полосы на широкую, что напоминает добавление шума. После расширения полосы передачи энергия сигнала на узкой полосе уменьшается, что еще больше затрудняет выявление скрытого сообщения [11].

Скрытое сообщение в данном методе может предварительно размываться шумом, а затем инкапсулироваться в изображение. Энергия этого сигнала будет гораздо ниже энергии контейнера, что создает дополнительные трудности выявления стеганограммы, которая становится практически незаметной для глаза человека. Без наличия исходного изображения компьютерный анализ изображения с вставкой такой стеганограммы требует больших ресурсов [10].

4. Методы преобразования области определения

Некоторые методы, например расширения спектра и использования патчей, как во временной области, так и в частотной очень похожи.

Методы, использующие частотное представление: быстрое преобразование Фурье, ДКП, ДВП [12], вначале преобразуют изображение, получая частотные коэффициенты или функцию плотности и применяя подходящий математический подход. Затем в частотную характеристику вставляется скрытое сообщение. После этого проводится обратное преобразование, возвращающее сигнал во временную область. Преимущество такого подхода заключается в возможности обработки сигналов или шума. Однако такие методы имеют высокую вычислительную сложность и вследствие этого низкую скорость работы.

Чтобы дать понятие стеганографических методов такого типа, необходимо вначале рассмотреть форматы файлов, которые преобразуются в частотную область. Одним из широко используемых форматов является JPEG, который многократно сжимает изображение. Это метод сжатия с потерей данных, несущественных для визуального восприятия [13].

4.1. Дискретное косинус-преобразование

Одна из идей стеганографии состоит в том, что скрытое сообщение маскируют заменой несущественных параметров изображения, но в формате JPEG в процессе сжатия возможно изменение или даже удаление таких параметров. Алгоритм сжатия формата JPEG состоит из по-

следовательности шагов, одна часть которых изменяет данные, а другая – сохраняет их. Шаги ДКП и квантизации изменяют данные, другие шаги, например кодировка по Хаффману, сохраняют их. Сообщение следует вставлять между этими шагами.

Алгоритм сжатия состоит из шести шагов (рис. 6) [14, 15]:

1) разложить изображение RGB по составляющим цветам: красному, зеленому и синему;
2) преобразовать цвета в формат YCdCr;
3) разделить матрицы интенсивности каждого цвета на блоки 8x8 пикселов;
4) выполнить квантизацию интенсивностей каждого блока по таблице квантизации;
5) произвести кодировку с учетом энтропии;
6) выполнить обратное ДКП.

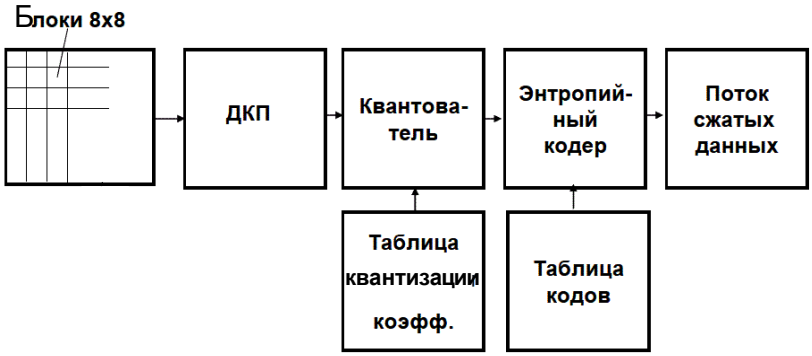

Рис. 6. Процесс ДКП изображения в формате JPEG

4.2. Дискретное вейвлет-преобразование

Вейвлет-преобразования широко применяются в обработке сигналов и сжатии изображений. Ввиду возможности анализа сигнала в выделенном интервале спектра они являются мощным инструментом для исследования особенностей поведения сигнала на различных частотных интервалах. Один из современных форматов кодирования JPEG-2000 основан на ДВП [16].

Несмотря на все положительные стороны классического JPEG с применением ДКП, а именно простоту использования, достаточно хорошее сжатие и возможность построения специализированной аппаратуры кодировки в этом формате, классический формат обладает и некоторыми недостатками. Так как исходное изображение разделяется на блоки, возможно высокое коррелирование интенсивности блоков. Этот феномен влияет на качество изображения и известен как «блоковые искажения», он особенно заметен на пикселах с низкой интенсивностью (рис. 7). Перекрывающееся ортогональное преобразование (LOT) [13] частично решает эту проблему, сглаживая границы блоков. Несмотря на очевидные улучшения, вычислительная сложность не позволила в алгоритме сжатия полностью заменить ДКП на LOT.

а) *б)*

Рис. 7. Изображение «Лена»: *а)* оригинальное; *б)* реконструированное блокированием артефактов

5. Сравнение стеганографичеких методов

Каждый стеганографичекий метод обладает как сильными, так и слабыми сторонами. Пользователю важно выбрать метод, который в наибольшей степени соответствует поставленной задаче. Существует несколько критериев для сравнения и выбора наиболее подходящего пользователю метода стеганографии. Все алгоритмы стеганографии должны удовлетворять нескольким основным требованиям. Наиболее важно, чтобы алгоритм давал малозаметное изменение изображения-контейнера. Рассмотрим критерии сравнения:

– *незаметность или уровень восприятия (нез.).* Это главное требование – стеганограмма не должна распознаваться глазом человека. Человек не должен видеть различие между исходным изображением и тем же изображением со вставленным сообщением. Выполнение данного требования зависит от объема сообщения и формата изображения [17];

– *вместимость (вмест.).* Это требование определяет размер вставляемого сообщения, который зависит от формата контейнера [18];

– *робастность*. Вставляемое сообщение не должно быть повреждено процессами обработки и передачи, присущими данному формату. Существует два типа робастности, один – для статистической обработки, второй – для целенаправленного повреждения стеганограммы:

• *робастность для защиты от статистической атаки (РПСА).* Статистические тесты применяются для выявления наличия стеганограммы в контейнере, это методы статистической обработки данных, которые можно применять как во временной, так и в частотной области. Многие методы стеганографии обладают сигнатурой, которую легко выявить статистическим анализом. Стеганограмма не должна оставлять в контейнере сигнатуру [17, 18];

• *робастность для защиты от целенаправленного повреждения стеганограммы (РПЦП).* Этот вид робастности обусловлен тем, насколько скрытое сообщение зависит от контейнера. Такие простые операции, как кадрирование, вращение и др., могут повредить сообщение;

– *способность к обнаружению или скрытность (СОС).* Этот критерий определяет успешность метода скрытия, при распознавании наличия сообщения он обусловливает сложность алгоритма распознавания [4–9];

– *вид области (ВО).* Этот параметр указывает на область, в которой применялась стеганография – временная (В) или частотная (Ч). Во временной области методы работают быстро, в частотной гораздо медленнее, но частотная область более надежна для скрытия сообщения;

– *независимость от формата (НФ).* Следует использовать различные форматы файлов. Если партнеры постоянно используют один формат, то это может навести на мысль о тайной переписке [17, 18].

В табл. 2 дается сравнение методов стеганографии по указанным критериям. Высокий уровень (*H*) говорит о полном соответствии требованиям, низкий (*L*) – о несоответствии, средний уровень (*M*) указывает, что требование зависит от конкретного параметра. В одних случаях может быть высокий уровень соответствия, в других – низкий. Например, скрытность алгоритма LSB с цветовой гаммой зависит от формата файла.

Таблица 2

Сравнение стеганографических методов

Алгоритмы	Критерии						
	Нез.	Вмест.	РПСА	РПЦП	СОС	ВО	НФ
LSB(BMP)	*H*	*H*	*L*	*L*	*L*	*L*	В
LSB(JPEG)	*H*	*H*	*L*	*L*	*H*	*L*	В
LSB(палитра)	*M*	*M*	*M*	*L*	*M*	*L*	В
ПП	*M*	*L*	*M*	*L*	*H*	*H*	В
ИП	*H*	*L*	*H*	*H*	*H*	*H*	В /Ч
РС	*H*	*L*	*H*	*M*	*H*	*H*	В / Ч
ДКП	*H*	*L*	*M*	*M*	*H*	*L*	Ч
ДВП	*H*	*H*	*M*	*M*	*H*	*L*	Ч

В идеальном случае стеганографический алгоритм должен удовлетворять высоким уровням всех критериев. Среди множества рассмотренных методов авторы не смогли найти такого алгоритма. Необходим взвешенный выбор стеганографического метода, который зависит от используемого пользователем приложения. Рассмотрим пригодность различных алгоритмов для форматов файлов:

LSB для BMP. Растровый формат BMP не использует сжатия, поэтому файлы этого формата имеют большой объем. К сожалению, для сокрытия сообщения в этих файлах необходим очень большой контейнер. В наше время этот формат используется в глобальной сети нечасто и его многократное применение может вызвать подозрение. Таким образом, этот формат не удовлетворяет условиям робастности. Обычно для сокрытия сообщения используется глубина 1, 4, 8, 16, 24, 48 и 64 бита на пиксел, поэтому BMP может вместить достаточно большое сообщение. Очевидно, что чем больше битов цвета заменяется, тем больше вероятность того, что невооруженный глаз заметит повреждение контейнера.

LSB для JPEG. Распространенный формат JPEG использует 8 битов на каждый цвет RGB, всего 24 бита на пиксел. JPEG может скрыть сообщение большого объема. Обычно стеганограмму в данном формате трудно распознать, это зависит от применяемого метода. Формат JPEG использует сжатие с потерями, и в процессе сжатия сообщение может быть повреждено. В таком случае JPEG не удовлетворяет критерию робастности.

LSB для цветовой палитры. Формат GIF кодирует пиксел 8 битами, изображение записывается в 256 цветах. Алгоритм LSB скрывает информацию с различными степенями успеха в зависимости от доли изменяемых бит. Необходимо искать равновесие между безопасностью и распознаваемостью. В разд. 4.2 указано, что изменение цвета в изображении зависит от структуры цветовой палитры, в этом случае тип изображения (полутоновое или цветное) играет важную роль. Распознаваемость и РПСА зависят от типа изображения.

Псевдослучайные перестановки. Метод вставляет биты сообщения с изменением порядка их появления в сообщении, что затрудняет работу по обнаружению и расшифровке сообщения. Как и в методе LSB, сообщения, биты которых вставлены случайным образом в младший бит, могут быть повреждены. Если же вставлять сообщения в другие, не последние биты, это может внести дополнительный шум в изображение. Формат изображения для этого метода не имеет большого значения.

Метод с использованием патчей. Недостаток этого метода состоит в том, что в один патч инкапсулируется только один бит. Разбиение изображения на более мелкие фрагменты позволяет вставить больше битов [7]. Преимущество этого метода состоит в том, что сообщение распределено по всему изображению, и если один из патчей будет поврежден, то это не принесет больших потерь и сообщение можно восстановить из других патчей [4]. Однако это зависит от других обстоятельств, в частности от размера сообщения. Короткое сообщение можно дублировать. Этот метод имеет большую робастность, так как скрытое сообщение может сохраниться даже при сжатии с потерями.

Метод расширения спектра. Этот метод распределяет сообщение по всему изображению. Такую стеганограмму трудно распознать. Частотная характеристика сообщения обладает гораздо меньшей энергией, чем энергия контейнера. Поэтому распознавание присутствия скрытого сообщения в контейнере очень затруднительно. Этот метод имеет большую робастность против атак.

Дискретное косинус-преобразование. Методы области преобразования (частотной области) скрывают сообщение в значительной области изображения, что делает их более робастными по сравнению с методами во временной области, включая сжатие, обрезку и некоторые алгоритмы обработки изображений. Однако существует компромисс между количеством информации и робастностью. Встраивание информации в область ДКП проще выполнить заменой коэффициентов ДКП. Коэффициенты равны нулю и замена многих нулей ненулевыми значениями будет иметь эффект коэффициента сжатия, поэтому мощность ДКП меньше, чем у LSB.

Дискретное вейвлет-преобразование. Инкапсуляция сообщения с помощью ДВП дает хорошие результаты, которые превосходят методы ДКП. Многомасштабный вейвлетный анализ разлагает сигнал в узкие частотные области, что позволяет скрыть сообщение в мелких деталях изображения.

Заключение

В статье были рассмотрены некоторые из основных методов стеганографии изображений, однако существует множество методов сокрытия информации в изображениях. Все основные форматы графических файлов имеют различные методы сокрытия сообщений со своими сильными и слабыми сторонами. Выбор метода с большой надежностью противостоит методу с высокой скоростью обработки. Например, патч-подход имеет очень высокую устойчивость по отношению к большинству видов атак, но он может скрыть лишь очень небольшое количество информации. Поэтому более разумно скрывать информацию в дополнительных преобразованиях, а не в исходных файлах. Преобразование дискретными вейвлетами более надежно, потому что позволяет скрыть сообщение в области частот. Данная область менее подвержена зрению человека.

Авторы предлагают использовать новые методы стеганографии, т. е. алгоритмы вставки скрытого сообщения в изображение с использованием ДВП. Эти методы могут учитывать многосторонние требования пользователя, предъявляемые к качеству изображения со скрытым сообщением большого объема.

Список литературы

1. Currie, D.L. Surmounting the effects of lossy compression on Steganography / D.L. Currie, C.E. Irvine // 19th National Information Systems Security Conference. – Baltimore, 1996.

2. Ahsan, K. Practical Data hiding in TCP/IP / K. Ahsan, D. Kundur // Proceedings of the Workshop on Multimedia Security at ACM Multimedia. – Canada, 2002.

3. Johnson, N.F. Exploring Steganography: Seeing the Unseen / N.F. Johnson, S. Jajodia // Computer Journal. – 1998. – Vol. 31, № 2. – P. 26–34.

4. Katzenbeisser, S. Information Hiding Techniques for Steganography and Digital Watermarking / S. Katzenbeisser, F.A.P. Petitcolas. – Norwood, MA : Artech House, 2000.

5. Niimi, M. High Capacity and Secure Digital Steganography to Palette-Based Images / M. Niimi // IEEE International conference on image processing. – Japan, 2002. – Vol. 2. – P. 917–920.

6. Al-Sadoon, B. On the Development of Steganographic Tools / B. Al-Sadoon, H. Mathkour, Gh. Assassa // Proceedings of the 1st National Information Technology Symposium, NITS. – Riyadh, Saudi Arabia, 2006.

7. Morkel, T. An Overview of Image Steganography / T. Morkel, J.H.P. Eloff, M.S. Olivier. – South Africa : University of Pretoria, 2002.

8. Bender W. Techniques for data hiding / W. Bender, D.Gruhl // IBM Systems Journal. – 1996. – Vol. 35, № 3–4.

9. Krenn, R. Steganography and steganalysis, Internet Publication, March 2004 [Electronic resource] / R. Krenn. – Mode of access : http://www.krenn.nl/univ/cry/steg/article.pdf. – Date of access : 24.12.2012.

10. Steganography Software [Electronic resource]. – Mode of access : http://www.jjtc.com/Steganography/tools.html. – Date of access : 23.12.2012.

11. Brundick, F. Implementation of Spread Spectrum Image Steganography / F. Brundick, L. Marvel [Electronic resource]. – 2001. – Mode of access : http://permanent.access.gpo.gov/gpo2618/ARL-TR-2433.pdf. – Date of access : 24.12.2012.

12. Chang, C.C. Introduction to the Visual Cryptography / C.C. Chang, L.Z. Chuang // Communication of the Chinese Cryptology and Information Security Association (CCISA). – 2004. – Vol. 10, № 2. – P. 1–14.

13. Meenu Kumari, A. JPEG Compression Steganography & Crypography Using Image-Adaptation Technique / A. Meenu Kumari, P. Khare // Journal of Advances in Information Technology. – 2010. – Vol. 1, № 3.

14. Bushra Kassim Al-Abudi. Colour Image Data Compression Using Multilevel Block Trunsaction Coding Technique / Bushra Kassim Al-Abudi // Phd Thesis. – Baghdad : College of Science, 2002.

15. Sua'd Kakil, A. Image in Image Hiding System using Iterated Function System (IFS) / A. Sua'd Kakil // Msc Thises. – Iraq : University of Sulaimani, 2009.

16. Khosravi, S. A new steganography method based HIOP (Higher Intensity Of Pixel) algorithm and Strassen's matrix multiplication / S. Khosravi, M.A. Dezfoli, M.H. Yektaie // Journal of Global Research in Computer Science. – 2011. – Vol. 2, № 1.

17. Mathkour, H. A New Image Steganography Technique / H. Mathkour, B. Al-Sadoon, A. Touir // Wireless Communications, Networking and Mobile Computing (WiCOM) : 4th International Conference on IEEE. – Dalian, China, 2008. – P. 1–4.

18. Babu, S. Authentication of Secret Information in Image Steganography / S. Babu, K.B. Raja // IEEE. – India : University of Heydarabad, 2008. – P. 1–6.

Поступила 27.06.12

Белорусский государственный университет
информатики и радиоэлектроники,
Минск, ул. П. Бровки, 6
e-mail: amseyyedi@gmail.com
rsadykhov@bsuir.by

S.A. Seyyedi, R.Kh. Sadykhov

COMPARISON OF DIGITAL IMAGE STEGANOGRAPHY METHODS

Steganography is a method of hiding information in other information of different format (container). There are many steganography techniques with various types of container. In the Internet, digital images are the most popular and frequently used containers. We consider main image steganography techniques and their advantages and disadvantages. We also identify the requirements of a good steganography algorithm and compare various such algorithms.