$$\Delta y \le \frac{Sp}{2},$$

где Sp - длина стороны контактной площадки.

Второй алгоритм предусматривает наличие общего векторного описания только одного из совмещаемых слоев. Для второго слоя этапы совмещения кадров слоя в векторном формате с учетом КТО и растровых кадров не проводятся, и он представлен отдельными векторными описаниями каждого кадра. В этом случае для каждого кадра второго слоя вычисляются его абсолютные координаты положения путем минимизации суммарной функции ошибки положения связывающих контактных площадок этого кадра и контактных площадок соответствующего кадра первого слоя. Такой подход позволяет для каждого кадра второго слоя вычислить координаты положения в слое относительно заданной точки привязки и избежать трудоемкой с вычислительной точки зрения процедуры совмещения растровых кадров. Затем для второго слоя проводится этап совмещения кадров в векторном формате с учетом КТО.

После получения абсолютных координат слоев необходимо произвести уточнение положения контактных площадок с учетом КТО. Изменение положения контактной площадки может потребовать внесение значительных изменений в векторное описание слоев. Поэтому здесь могут применяться специальные алгоритмы обработки векторных представлений слоев, которые контролируют следующие конструкторско-технологические параметры:

- размер контактной площадки;
- размер контактного окна;
- расстояние между контактной площадкой и проводником;
- ширина проводника;
- расстояние между проводниками;
- расстояние от границы контактного окна до внешней границы контактной площадки.

Окончательное положение контактной площадки в каждом слое выбирается как усредненное положение связывающих площадок, если допустимое смещение D меньше или равно заданному порогу. Величина D вычисляется из следующего выражения:

$$D = |Do - Dn|, \qquad (5)$$

где Do - старое положение контактной площадки;

Dn - уточненное положение контактной площадки.

В противном случае окончательное положение контактной площадки выбирается исходя из требования внесения минимальных изменений в векторные описания слоев.

В результате работы алгоритмов формируется: векторное описание слоев и уточненные координаты контактных площадок.

На данном этапе выявляются также отсутствующие контактные площадки. Рассмотрим множество $\{P_i / i = 1,2,\ldots, k\}$ слоев, где слой i расположен над слоем $i + 1$. Множество КП слоя i, соединенных с КП слоев $i - 1$и $i + 1$ обозначим как P_i^{pred} и P_i^{succ} соответственно, $P_i = P_i^{pred} \cup P_i^{succ}$, $i = 1,\ldots, k$. Для слоя 1 имеем $P_1^{pred} = \varnothing$ и для слоя k - $P_k^{succ} = \varnothing$. Нарушение равенства $P_i^{pred} = P_{i-1}^{succ}$ *or* $P_{i+1}^{pred} = P_i^{succ}$ свидетельствует о об отсутствии или наличии лишней КП.

Заключение

Предложен эффективный по точности алгоритм аппроксимации выделенных контуров отрезками различной длины, основанный на преобразовании Хафа. Алгоритм формирует векторное описание топологии одного кадра видеоизображения. Предложен алгоритм объединения векторных описаний каждого кадра в общее векторное описание слоя и алгоритм совмещения этих описаний для формирования многослойного представления топологии ИС.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Ваткин М.Е., Дудкин А.А.* Алгоритм совмещения частично перекрывающихся кадров изображения // Анализ цифровых изображений. Минск: ОИПИ Национальной академии наук Беларуси, 2003. Вып. 2. С. 25-32.
2. *Duda R. O., Hart P. E.* Use of the Hough transformation to detect lines and curves in pictures // Communication of the Association for Computing Machinery. 1972. Vol. 15. №. 1. P. 11-15.
3. *Denzler J.* Texture region Extraction. "http://www.dai.ed.ac.uk/CVonline/LOCAL_ COPIES/DENZLER1/node11.html". In CVonline: On-Line Compendium of Computer Vision [Online]. R. Fisher (ed). Available: "http://www.dai.ed.ac.uk/CVonline/". [9.07.2001].
4. *L. G. Brow.*A survey of image registration techniques // ACM (Assoc. Comput. Mach.) Comput. Surv. 1992. № 24**.** P. 325–376.
5. *Д.А. Вершок, А.А. Дудкин, А.Г. Калюта, А.М. Селиханович.* Система цифровой обработки изображений слоев интегральных микросхем // Идентификация образов. Минск: Ин-т техн. кибернетики НАН Беларуси, 2001. № 2. С. 72-87.
6. *Z. Zhang, R. Deriche, O. Faugeras and Q.-T. Luong.* A Robust Technique for Matching Two Uncalibrated Images Through the Recovery of the Unknown Epipolar Geometry //Artificial Intelligence Journal. 1995.V.78. P. 87-119
7. *William J. Chimitt, Jr., and Laurence G. Hassebrook.* Scene recons ruction from partially overlapping images with use of composite // J. Opt. Soc. Am. 1999. № 16(9), P. 2124-2135.
8. *Прэтт У.* Цифровая обработка изображений: Пер. с англ. М.: Мир, 1982. Кн. 2. 480 с.

УДК 681.3

Горбашко Л.А.

СТЕГАНОГРАФИЧЕСКОЕ СКРЫТИЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ПРЕОБРАЗОВАНИЯ ФУРЬЕ

Введение

Стеганография исследует скрытую передачу данных в маскирующем сигнале. Для скрытия информации могут быть выбраны любые файлы: текстовые, HTML, графические, звуковые, dll- библиотеки, но чаще используются графические и звуковые файлы, т.к. при встраивании сообщения в эти типы файлов не увеличивается размер файла со скрытой информацией.

В стеганографии принята следующая терминология.

Контейнер (изображение- носитель, container, cover image, carrier) – файл для встраивания данных.

Скрытое сообщение – сообщение, встраиваемое в контейнер.

Стего-образ, стего (stego-image) – изображение со скрытой информацией.

Все известные методы цифровой стеганографии можно

***Горбашко Лариса Ашотовна**, ст. преподаватель кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*

Беларусь, БГТУ, 224017, г. Брест, ул. Московская, 267.

разделить на четыре группы [1]:

- прямые методы,
- методы преобразований (встраивание изображений в частотной области),
- фрактальные методы,
- методы, использующие особенности форматов файлов.

Методы цифровой стеганографии должны удовлетворять следующим условиям:

прозрачность (transparency) – отсутствие видимых различий контейнера от стего;

робастность (robust) – устойчивость к пространственным искажениям: шум, фильтрация, сжатие, афинные преобразования (вращение, изменение масштаба), редукция (вырезание части данных), изменение формата данных (сжатие).

Объем информации, которая должна быть встроена в изображение, оценивается относительно к размеру контейнера. Существует противоречие между возможным объемом встроенной информации и прозрачностью и робастностью. При встраивании необходимо найти компромисс между этими характеристиками. Если требуется встроить изображение большого объема, то придется пойти на ухудшение качества и снижение робастности [1].

В данной статье предложен метод стеганографического скрытия информации путем преобразования изображений с использованием преобразования Фурье, который позволяет встраивать информацию в соотношении 1:1 и при этом обладает прозрачностью и достаточной робастностью.

Методы стеганографического встраивания изображений

Предположим, что нужно тайно передать некоторое сообщение. Независимо от его природы, любое сообщение может быть продискретизировано и представлено в виде последовательности чисел (отсчетов), которую и нужно передать незаметно.

Прямые методы встраивают информацию непосредственно в подмножество пикселов изображения. В общем случае встраиваемая информация отображается небольшим изменением значений яркости отдельных пикселов изображения (в случае RGB- формата – в каждом слое). При этом изменение яркости не должно восприниматься человеческим глазом. Как правило, изменение яркости на уровне 3-4 последних бит незаметно для нетренированного глаза. Методы данного класса различаются выбором модифицируемого подмножества пикселов (т. н. стегопути), стратегией изменения значений пикселов [2].

В наиболее простом случае скрываемая информация встраивается в наименее значащие биты изображения, почему их и называют LSB (Least Significant Bit). Если рассмотреть черно- белое растровое изображение, то каждому пикселу соответствует один байт, который хранит цвет пиксела в виде градации серого: 0- черный, 255- белый, остальные – градации серого. Изменение последнего бита приводит к изменению уровня серого на 1 из 256. Человеческий глаз не заметит изменения оттенка. Т.о., сообщение необходимо представить в виде последовательности бит, которая записывается на место младших бит контейнера.

Аналогично можно рассмотреть цветное изображение, только каждому пикселу будет соответствовать 3 байта – яркость цветов RGB. Для встраивания изображения необходимо изменять сразу 3 младших бита в каждом байте.

Размер контейнера не меняется при встраивании, но нельзя встроить изображение, превышающее размер контейнера, уменьшенный в 8 раз (соотношение между размером контейнера и встраиваемым изображением – 1:8). Однако LSB – методы имеют низкую робастность и криптостойкость. Они неустойчивы практически ко всем преобразованиям. Если предположить, что изображение содержит скрытую информацию, то ее легко извлечь.

Более робастными и устойчивыми к атакам являются *преобразования изображения в частотной области*. В этом случае в качестве отсчетов изображения контейнера используются составляющие, полученные путем разложения дискретного сигнала на любые частотные составляющие. Это могут быть преобразования Фурье, дискретное косинусное, Карунена-Лоэва и т.п.

Для встраивания последовательности чисел сообщения в контейнер используются аддитивные алгоритмы [2], которые заключаются в линейной модификации частотных составляющих исходного изображения:

$$f'(m,n) = f(m,n) + \alpha\omega_i, \qquad (1)$$

где $f(m, n)$ и $f'(m, n)$ – значения коэффициентов частотных составляющих изображений контейнера и стего соответственно;

α - весовой коэффициент;

ω_i - последовательность встраиваемых чисел сообщения или отсчетов изображения.

Для извлечения сообщения производится обратное действие:

$$\omega_i = \frac{f'(m,n) - f(m,n)}{\alpha}. \qquad (2)$$

Если вместо последовательности чисел в изображение встраивается другое изображение (например, разложенное на частотные составляющие), то такие алгоритмы внедрения называются алгоритмами слияния. В этом случае можно допустить некоторое искажения скрытого сообщения, т.к. человек все равно сможет его распознать.

Алгоритмы встраивания сообщения

Внедрение информации по аддитивному алгоритму происходит одинаково для всех видов частотного преобразования. Изображение представляется в виде матрицы отсчетов дискретного сигнала. Обычно в языках программирования имеется специальная функция для преобразования графического изображения любого формата в матрицу отсчетов, каждый элемент которой представляет собой закодированный цвет пиксела. Использование стандартной функции избавляет от необходимости обрабатывать заголовок файла отдельно от информации [3]. Затем полученный дискретный сигнал раскладывается на частотные составляющие, сообщение встраивается в частотные составляющие по аддитивной формуле (1), с полученной матрицей проводится обратное частотное преобразование, матрица сохраняется в виде стегоизображения.

Стего передается по цифровому каналу передачи данных, визуально стего ничем не отличается от контейнера.

Для извлечения сообщения необходимо иметь *стего и контейнер*, в который встраивалось сообщение. Это является недостатком данного типа алгоритмов. Контейнер может передаваться вместе со стего, либо в другое время или по другому каналу для снижения вероятности успешной атаки на скрытую информацию, а может использоваться из набора заранее определенных контейнеров с заданными вероятностными характеристиками.

При реализации общего алгоритма была выявлена трудность выполнения условия прозрачности стего. Если сообщение встраивать в произвольные частотные составляющие, то визуально в стего проявляется встроенное сообщение. Поэтому перед встраиванием предварительно производится фильтрация составляющих, которая заключается в отборе гармоник, значение которых выше определенного порога q.

Т.о., в качестве недостатков данного алгоритма можно отметить следующие:

- необходимость подбора порога q для обеспечения прозрачности, что осуществляется путем многократного визуального сравнения стего при использовании разных значений q, при этом величина порога зависит от используемого контейнера;
- значительно меньшие размеры сообщения по сравнению с контейнером (менее 1:4).

Поэтому вышеприведенный алгоритм был модифицирован.

Для встраивания в контейнер используются не отсчеты сигнала сообщения, а гармоники ряда Фурье $\omega(m, n)$ скрываемого сообщения. Последовательность действий выглядит следующим образом:

1) разложить дискретный сигнал контейнера на частотные составляющие, в данном случае, на гармоники ряда Фурье (прямое дискретное преобразование Фурье):

$$f(m,n) = \sum_{m=0}^{N-1} x(k,n) exp\left(-j\frac{2\pi nm}{N}\right), \qquad (3)$$

где $x(k, n)$ – значение отсчетов изображения контейнера k-й строки n-го столбца;

m – номер гармоники при разложении n-го столбца, m=0..N-1;

N – количество гармоник, на которые разлагается исходное изображение.

Т.е. исходной информацией для разложения является столбец (или строка) матрицы пикселов изображения. В результате происходит преобразование матрицы пикселов $x(k, n)$ в матрицу гармонических составляющих $f(m, n)$ по столбцам. Количество гармоник N обычно равно количеству пикселов изображения по вертикали, но не может быть меньше;

2) разложить дискретное сообщение на гармоники ряда Фурье по формуле (3); количество гармоник также равно N, получим матрицу частотных составляющих сообщения $\omega(m, n)$;

3) встроить гармоники сообщения $\omega(m, n)$ в частотные составляющие контейнера $f(m, n)$ по аддитивной формуле:

$$f'(m,n) = f(m,n) + \alpha\omega(m,n). \qquad (4)$$

Коэффициент α служит для обеспечения прозрачности и выбирается визуально. Основная особенность алгоритма в том, что вместо дискретных отсчетов сигнала ω_t внедряются значения коэффициентов разложения $\omega(m, n)$, полученные на шаге 2;

4) провести обратное преобразование Фурье:

$$x(k,n) = \frac{1}{N}\sum_{n=0}^{N-1} f'(m,n) exp\left(j\frac{2\pi mk}{N}\right) \qquad (5)$$

5) затем из векторов $x(n)$ составляется матрица изображения, которая после преобразования в графический формат и является стего.

Последовательность действий при извлечении сообщения из стего, полученного с помощью преобразования Фурье, выглядит следующим образом:

1) представить стего в виде матрицы отсчетов дискретного сигнала;

2) разложить полученный дискретный сигнал на частотные составляющие по формуле (3) с количеством гармоник, равным количеству пикселов изображения по вертикали;

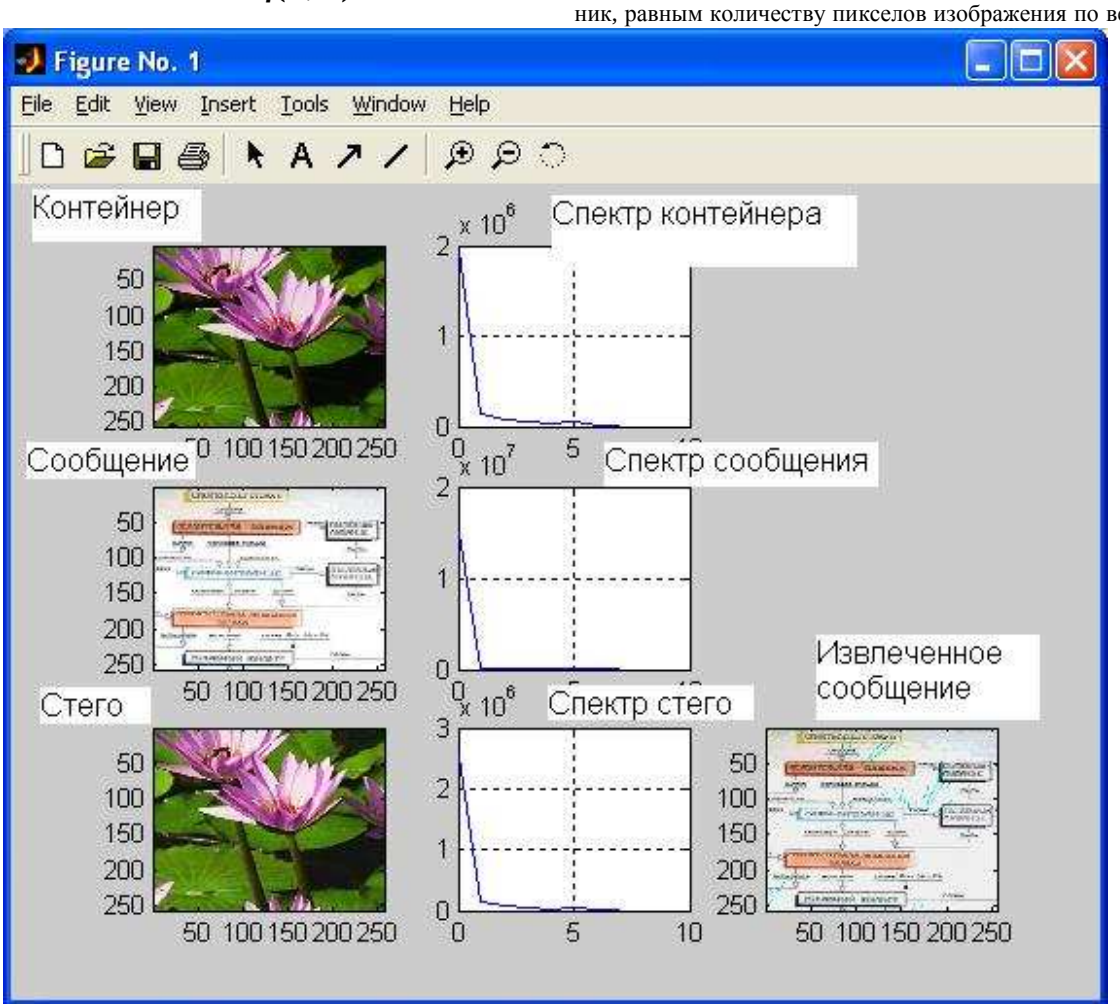
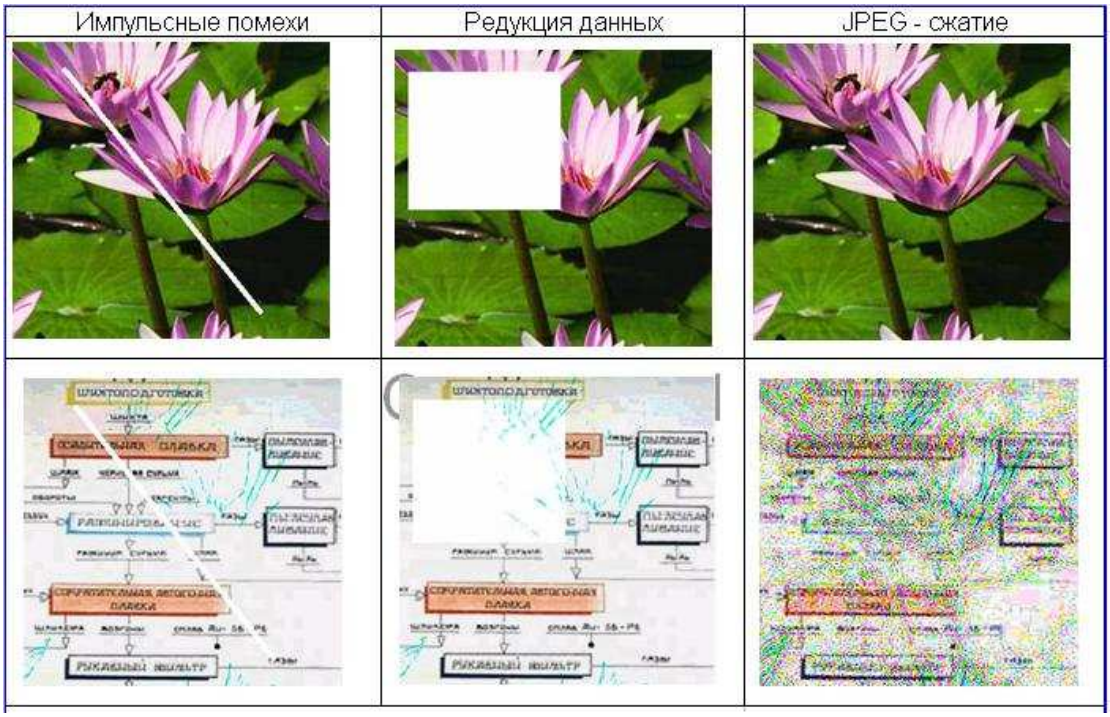


Рис. 1. Визуализация результатов экспериментов



В верхнем ряду - стего с искажениями, в нижнем – извлеченные сообщения

Рис. 2. Тестирование робастности стего.

3) использовать разложение контейнера на частотные составляющие по формуле (3); при этом количество гармоник сообщения выбирается равным количеству гармоник сигнала;

4) извлечь сообщение из частотных составляющих стего по формуле:

$$\omega(m,n) = \frac{f'(m,n) - f(m,n)}{\alpha}$$

5) выполнить обратное преобразование Фурье по формуле (5).

Полученная последовательность отсчетов является принятым сообщением после преобразования в графический формат.

Преимущества модифицированного алгоритма:

- возможность встраивания изображения в соотношении размеров контейнера и сообщения 1:1, в то время как известные методы имеют наилучшее соотношение 1:6,5 [4], в любом случае контейнер должен быть по размерам больше сообщения [5];
- простота реализации, т.к. отсутствует необходимость выбора порога q путем подбора.

Результаты экспериментов

В качестве контейнера и сообщения использовались графические файлы формата .bmp одинакового размера 256x256 с 24-битной градацией цвета. Для встраивания и извлечения сообщений была разработана программа на языке пакета MatLab 6.5. Для выбранного контейнера использовалось значение α=0,05, которое было определено с учетом выполнения условия прозрачности. Визуализация результатов преобразований представлена на рисунке 1.

Затем полученное стегоизображение было протестировано на робастность к шуму, импульсным помехам, редукции данных и Jpeg- сжатию. Для моделирования помех в канале передачи использовался графический редактор Paint. По визуальному сравнению результатов, представленных на рисунках 1 и 2, можно сделать следующие выводы:

1) визуально сообщение не обнаруживается в стего;

2) спектр контейнера и стего визуально совпадают, что затрудняет обнаружение скрытого сообщения;

3) извлеченное изображение при отсутствии помех соответствует исходному;

4) робастность алгоритма:

при воздействии на стего импульсных помех, редукции, изменения яркости извлеченное изображение имеет такие же искажения, как и стего, и является вполне узнаваемым; следовательно, метод может быть признан устойчивым;

5) метод неустойчив к Jpeg-сжатию, что является естественным, т.к. в алгоритме jpeg- сжатия заложено дискретное косинусное преобразование (ДКП) и наиболее робастным к данному виду преобразований будет алгоритм встраивания с использованием ДКП.

Результаты экспериментов показывают, что предложенный алгоритм может применяться для скрытой передачи информации в цифровых каналах связи и для защиты авторских прав цифровых данных. В этом случае скрытое сообщения является цифровым водяным знаком и удалить его без контейнера не представляется возможным.

Достоинством данного метода является возможность встраивания в соотношении размеров контейнера и сообщения 1:1, недостатком – отсутствие робастности сообщения к сжатию изображения. Однако данный недостаток может быть легко устранен, если в качестве контейнера выбирать файл формата .jpeg, который уже является сжатым, следовательно, стего также получим в формате .jpeg.

Полезность алгоритма встраивания информации может быть оценена только в контексте конкретных требований, данный алгоритм целесообразно применять для скрытой передачи больших объемов информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Городецкий В.И., Самойлов В.И. Стеганография на основе цифровых изображений. – Санкт-Петербургский институт информатики и автоматизации РАН, http://space.iias.spb.su/ai/doc/Steganography-01.pdf.
2. Грибунин В.А. Цифровая стеганография. – М.:Эксмо, 2002.
3. Сергиенко А.Б. Цифровая обработка сигналов.- СПб: Питер, 2002.
4. Николаевич В. Тайнопись/ журнал «Компьютерра»/ № 489, 2003.
5. Rosen J., Javidi B. Hidden images in halftone pictures.- Optical Society of America/ Vol. 40, No. 20/ 10 July 2001.