УДК 621.391.7

Н. В. Лысенко, Г. М. Лабков
Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В. И. Ульянова (Ленина)

Применение стеганографического алгоритма Куттера–Джордана–Боссена в видеопоследовательностях

Рассмотрена возможность работы алгоритма Куттера–Джордана–Боссена в видеопоследовательностях в режиме реального времени. Оценено влияние различных видов шумов на устойчивость работы алгоритма. Показано, что устойчивость к шумовым помехам можно улучшить, увеличив число встраиваний одного бита, однако при этом увеличивается вероятность обнаружения скрытой информации неавторизованным пользователем.

Стеганография, видеопоследовательность, скрытая передача, защита информации

Развитие информационных сетей, в первую очередь сети Интернет, облегчило доступ к различной информации. В связи с этим становится актуальным вопрос защиты информации от несанкционированного доступа. Существует два направления решения указанной задачи: криптография и стеганография. Основная задача криптографии – шифрование сообщений с целью сокрытия их содержания. Методы криптографии позволяют зашифровать информационное сообщение, однако сам факт передачи такого сообщения криптографией не скрывается и может заинтересовать потенциального перехватчика. Стеганография же направлена на сокрытие самого факта передачи зашифрованных данных [1].

В целом стеганография применима к множеству объектов, относящихся не только к компьютерным информационным сетям. Однако такие сети открывают наиболее широкие горизонты возможностей перед стеганографией. По этой причине остро стоит вопрос обеспечения информационной безопасности с точки зрения как обнаружения негативной информации, так и сокрытия секретной информации от злоумышленников. К примеру, на сегодняшний день стеганографические методы применяются для сокрытия сообщений в изображениях, текстовых файлах, аудиофайлах и т. д. [1].

Большой интерес представляют системы, использующие в качестве стеганоконтейнеров изображения. Назовем это направление видеостеганографией. Интерес к видеостеганографическим системам обусловлен рядом причин. Среди них хотелось бы выделить наличие многочисленных и разнообразных методов обработки изображений, поскольку это определяет разнообразие возможных методов и алгоритмов, которые можно применить с целью передачи скрытой информации. Также немаловажной причиной является слабая чувствительность человеческого глаза к незначительному изменению яркости в изображении [2].

Среди систем, использующих в качестве стеганоконтейнеров изображения, важную роль играют видеопоследовательности. Особенностью создания стеганоконтейнера в видеопоследовательности является встраивание информации в реальном времени. В связи с этим методы встраивания информации должны обладать важным качеством – небольшой вычислительной сложностью. В настоящее время существует достаточно много методов для сокрытия данных в видеофайлах [1]. Методы, работающие на этапе преобразований, предполагают частичное преобразование исходных данных. Например, может использоваться замена высокочастотных коэффициентов дискретного косинусного преобразования на информационные биты. Методы, работающие на этапе сжатия, направлены на работу со сжатыми форматами файлов. Такие методы встраивают информацию в контейнер и извлекают информацию из контейнера в процессе компрессии и де-

компрессии, оперируя промежуточными данными, что дает значительную скорость указанных операций. Методы, работающие непосредственно с исходным изображением, позволяют достичь высокого уровня сокрытия информации, поскольку их алгоритмы направлены на максимальную визуальную незаметность вносимой информации.

Существует большое количество методов встраивания стеганоконтейнера в изображение [3]. Авторами настоящей статьи проведено исследование метода Куттера–Джордана–Боссена, обладающего высокой пропускной способностью[1], а также обеспечивающего устойчивость к несанкционированному доступу. Алгоритм основан на одном из свойств зрительной системы человека: ее восприимчивость к перепадам яркости синего цвета значительно меньше, чем зеленого и красного [3]. Исследование данного алгоритма проводилось в программном пакете MATLAB версии "for student use".

Указанный алгоритм предполагает встраивание одного бита данных в один пиксел изображения. В результате на отдельном изображении изменению яркости подвергается некое число пикселов, зависящее от объема изображения.

Для встраивания отдельного бита сообщения в изображении псевдослучайным образом выбирается пиксел с координатами x и y[2], обладающий яркостью

$$L_{x,y} = \overline{r}R_{x,y} + \overline{g}G_{x,y} + \overline{b}B_{x,y},$$

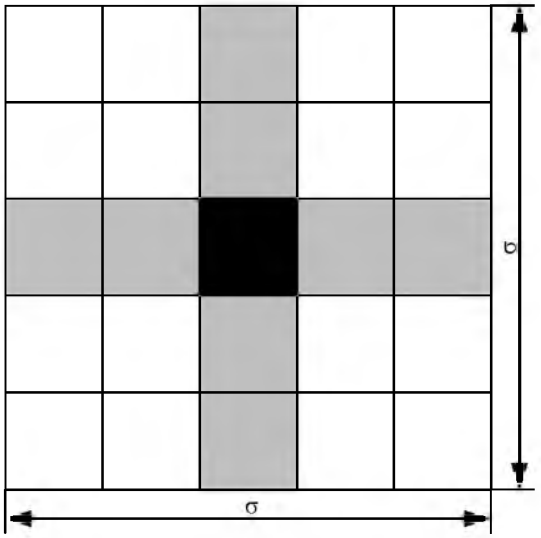
где $\overline{r}$, $\overline{g}$, $\overline{b}$ – удельные цветовые коэффициенты в каналах красного, зеленого и синего соответственно; $R_{x,y}$, $G_{x,y}$, $B_{x,y}$ – цветовые координаты пиксела в указанных каналах.

Секретная информация встраивается в канал синего цвета по формуле

$$B'_{x,y} = \begin{cases} B_{x,y} + uL_{x,y}, & m_i = 1; \\ B_{x,y} - uL_{x,y}, & m_i = 0, \end{cases}$$

где u – константа, определяющая энергию встраиваемого сигнала; m_i – i-й бит встраиваемого сообщения. Энергия встраиваемого сигнала выбирается исходя из назначения системы как компромисс между устойчивостью системы к искажениям (возрастает при увеличении u) и заметностью встраиваемых символов [4].

Извлечение секретного бита происходит на основании сравнения цветовой координаты синего пиксела со значением этой величины, предсказанным на основе соседних пикселов по вертикали и по горизонтали (рисунок, где предсказание происходит по "кресту" из 5×5 пикселей).



Оценка интересующего пиксела находится по формуле

$$B^*_{x,y} = \frac{1}{2(\sigma-1)} \times \left[\sum_{\substack{j=-(\sigma-1)/2, \\ j\neq 0}}^{j=(\sigma-1)/2} B^*_{x+j,y} + \sum_{\substack{j=-(\sigma-1)/2, \\ j\neq 0}}^{j=(\sigma-1)/2} B^*_{x,y+j} \right],$$

где символы "*" указывают на значения цветовой координаты в принятом сигнале; σ – количество пикселов (размер апертуры), на основании которых выполняется предсказание, по одной из координат (как правило, размеры апертуры по горизонтали и вертикали выбираются равными). Для корректности предсказания σ должно быть нечетным. На рисунке $\sigma = 5$.

Чтобы извлечь встроенный бит, определяется разница между текущим и предсказанным значениями пиксела в синем канале:

$$\delta = B^*_{x,y} - \hat{B}^*_{x,y}.$$

Авторами настоящей статьи описанный алгоритм исследован применительно к видеопоследовательности. С целью внесения информации каждый кадр видеопоследовательности был преобразован в изображение формата jpeg, а после встраивания информации последовательность кадров вновь преобразовывалась в видеопоследовательность. Ввиду относительно большого количества изображений появилась возможность вносить информацию не в один кадр, а встраивать каждый бит сообщения в

[1] Количество информации, которую с заданным качеством может передать стегосистема за единицу времени.

[2] Информация о выбранных пикселах или принципе их выбора передается получателю по отдельному каналу.

последовательные изображения. Для выполнения процедуры из видеоряда выбирались кадры (изображения), характеризующиеся максимальными яркостными переходами, поскольку на таких переходах визуально заметить изменения сложнее.

Указанный принцип выбора контейнеров позволяет повысить устойчивость алгоритма к несанкционированному доступу, поскольку максимально на одном изображении изменяется лишь один пиксел. Необходимо отметить, что использование алгоритма в видеопоследовательности также улучшает устойчивость алгоритма, так как визуально заметить изменение пиксела на изображении в последовательности кадров гораздо сложнее.

Для исследования быстродействия алгоритма использовалась видеопоследовательность с частотой 25 кадров в секунду. В видеопоследовательность встраивался символ "А". Данный символ был представлен в двоичной системе счисления как 10000010000. С целью повышения вероятности обнаружения каждый из исходных 11 бит встраивался 5 раз, таким образом, производилось изменение 55 пикселов. На считывание и преобразование символа в двоичную систему программа затратила 5 мс, а на встраивание 55 битов в изображения – 10 мс. Поскольку длительность одного кадра составляет 40 мс, вносимая в видеопоток задержка оказалась меньше времени кадра, т. е. алгоритм может работать в реальном времени. На распознавание символа программой было затрачено 22 мс, что также меньше длительности кадра. На основании полученных данных можно сказать, что алгоритм Куттера–Джордана–Боссена способен работать в режиме реального времени как для внесения скрытой информации в видеопоток, так и для ее извлечения.

Для изучения помехоустойчивости алгоритма изображение с уже встроенной информацией подвергалось воздействию гауссовского "белого" шума с нулевым математическим ожиданием и дисперсией 0.01; импульсного шума с плотностью 0.05; мультипликативного шума с нулевым математическим ожиданием и дисперсией 0.04. В качестве вносимой информации использовалось слово "Телевидение". Одним из результатов распознавания был набор символов "Т л > |е", в остальных случаях также распозналось меньше половины символов. Многократное встраивание информации позволило незначительно улучшить результат распознавания. Однако во многих случаях часть символов распознались неправильно.

Таким образом, исследованный алгоритм Куттера–Джордана–Боссена способен работать в режиме реального времени как для внесения скрытой информации в видеопоток, так и для ее извлечения, однако он слабо устойчив к шумовым искажениям. Устойчивость к шумовым помехам можно улучшить, увеличив число встраиваний одного бита, однако при этом увеличивается вероятность обнаружения скрытой информации неавторизованным пользователем.

СПИСОК ЛИТЕРАТУРЫ

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: СОЛОН-ПРЕСС, 2009. 272 с.

2. Стеганография, цифровые водяные знаки и стеганоанализ / А. В. Аграновский, А. В. Балакин, В. Г. Грибунин, С. А. Сапожников. М.: Вузовская кн., 2009. 220 с.

3. Коханович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. 288 с.

4. Kutter M., Jordan F., Bossen F. Digital signature of color images using amplitude modulation // Storage and retrieval for image and video databases. 1997. Proc. SPIE. Vol. 3022. P. 518–526.

N. V. Lysenko, G. M. Labkov
Saint Petersburg Electrotechnical University "LETI"

Applying of Kutter–Jordan–Bossen steganography algorithm to video sequences

The possibility of operating of the algorithm of Kutter–Jordan–Bossen in video sequences in real time is considered. The influence of different types of noise on the algorithm stability is evaluated. It is shown that the resistance to noise interferences can be improved by increasing the number of embedding one bit, however, this increases the probability of detection of hidden information is not an authorized user.

Steganography, video sequences, hidden communication, information protection

Статья поступила в редакцию 8 сентября 2015 г.