УДК 004.021

ПРИМЕНЕНИЕ ДИСКРЕТНОГО КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ И ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ В АЛГОРИТМАХ ЦИФРОВОЙ СТЕГАНОГРАФИИ

А.С. ТАНАНА
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

В статье рассматривается стеганографический алгоритм встраивания текстовой информации в мультимедийный объект на основе дискретного косинусного преобразования и генератора псевдослучайной последовательности.

В современном мире одной из важнейших задач является защита информации, например, обеспечение безопасности хранения криптографических ключей или передачи конфиденциальных данных. Существует множество криптографических методов для решения этой задачи, однако большинство алгоритмов шифрования данных не обладают нужной стойкостью. К каждому алгоритму можно найти обратный метод, который дешифрует закодированное слово. Рациональным решением задачи обеспечения защиты информации является сокрытие факта передачи данных. Стеганография – специальная наука, изучающая методы сокрытия информации, которая должна оставаться не обнаружимой как статистически, так и для человеческого восприятия. В настоящее время такая задача актуальна для мультимедийных объектов: цифровые изображения, звуковые файлы, видеозаписи.

Современная стеганография разделяется на два направления: компьютерная и цифровая стеганография. Первое направление основано на особенностях компьютерной платформы и широко применяется в файловых системах. Второе направление, цифровая стеганография, основано на встраивании дополнительной информации в цифровые объекты. Алгоритмы цифровой стеганографии могут быть направлены как на полное сокрытие внедренной информации от посторонних глаз, так и на наложение специальных знаков на исходный сигнал. Таким образом, цифровую стеганографию можно разделить на следующие группы [1]:

– встраивание информации в непосредственно цифровой сигнал;
– встраивание цифровых водяных знаков;
– встраивание идентификационных номеров;
– встраивание заголовков.

Наибольший интерес представляют алгоритмы первой группы. Совокупность средств и методов, которые используются для формирования скрытого канала передачи, формируют стеганографическую систему, или стегосистему.

Каждый стеганографический метод должен обладать набором качественных характеристик. К ним можно отнести невидимость, устойчивость и объем встраиваемого сообщения. Невидимость скрытой информации достигается за счет особенностей человеческого восприятия. Например, система человеческого зрения наименее чувствительна к изменениям канала синего цвета в изображениях, а система человеческого слуха практически нечувствительна к изменениям фазы звукового сигнала. Оценка стойкости алгоритма основана на его устойчивости к различного рода модификациям и атакам. Под модификацией понимается применение фильтров, изменение объема контейнера, аналогово-цифровое и цифро-аналоговое преобразование. Под атакой на стегосистему понимается попытка обнаружить, извлечь или повредить стеганографическое сообщение. Объем встраиваемого сообщения является немаловажным параметром оценки стеганографического алгоритма, т.к. наибольший интерес представляют алгоритмы, способные внедрить большое количество информации в контейнер. Таким образом, контейнеры большего размера позволяют внедрить большее количество информации.

На сегодняшний день существует множество различных алгоритмов и методов стеганографического внедрения информации, однако большинство из них уже устарели и имеют большую вероятность обнаружения данных. Безусловно, разработаны методы, обеспечивающие высокую надежность, однако их реализация слишком сложна в вычислительном процессе. Анализ существующих методов встраивания информации показывает, что задача разработки стеганографических методов остается актуальной. На основе существующих стеганографических алгоритмов можно создать усовершенствованный алгоритм, который будет обладать достаточной степенью устойчивости к различным преобразованиям и хорошо противостоять методам стегоанализа.

Один из самых распространенных методов сокрытия информации основан на замене наименее значащих бит (LSB) потока данных на биты встраиваемого сообщения. Однако большинство мультимедий-

ных объектов хранятся в сжатом виде. Алгоритмы сжатия построены так, что на этапе квантования происходит округление спектральных коэффициентов, полученных после косинусного преобразования. Идею метода LSB можно применить и в спектральной области [2].

Для получения спектра используют не только дискретное преобразование Фурье, но и дискретное косинусное преобразование. Известно, что коэффициенты, полученные после применения ДКП, упорядочены от более низкочастотных к более высокочастотным (рис. 1). Низкочастотные коэффициенты содержат самую важную информацию для восстановления исходных данных. Высокочастотные коэффициенты можно занулить без существенных потерь после обратного применения ДКП.

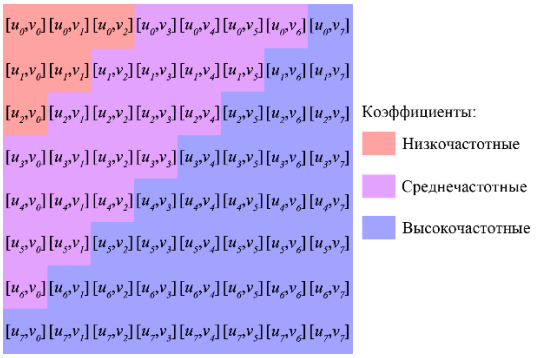

Рисунок 1. – Матрица коэффициентов ДКП размером 8x8

Самый высокочастотный коэффициент массива ДКП выступает в роли наименее значащего бита. Этот коэффициент можно заменить другим значением без риска существенного искажения исходного сигнала. В основе алгоритма будет лежать принцип замены заранее определённого высокочастотного или среднечастотного коэффициента.

Рассмотрим алгоритм внедрения информации. В качестве стегоконтейнера может быть использован как видео-, аудиофайл, так и изображение. Встраиваемое сообщение представляет собой обычное текстовое сообщение, преобразованное в битовую последовательность. Для увеличения стойкости алгоритма полученную битовую последовательность можно закодировать любым помехоустойчивым кодом. Разделим исходный сигнал на блоки размером 8x8 и получаем массив номеров блоков. При этом следует учитывать то факт, что многие контейнеры содержать специальные блоки заголовков, содержащие специальные данные согласно формата контейнера. Встраивание сообщения будем производить не в каждом блоке, а в блоках с номерами, соответствующими номерам из псевдослучайной последовательности чисел (ПСП).

В качестве генератора псевдослучайной последовательности выберем генератор Блюм-Блюма-Шуба (BBS). Это простейший и наиболее эффективный генератор, использующий сложный теоретический подход разложения на множители [3].

Пусть есть два простых числа p и q. Их произведение n является целым числом Блюма. Выберем другое случайное число x, взаимно простое с n. Тогда

$$x_0 = x^2 mod\ n$$

есть стартовое число генератора. Последующие значения последовательности будут вычисляться по формуле:

$$x_i = x_{i-1}^2 mod\ n$$

Безопасность этой схемы основана на сложности разложения n на множители. Более того, генератор BBS непредсказуем как в левом направлении, так и в правом направлении. Это означает, что, получив последовательность, криптоаналитик не сможет предугадать ни следующий, ни предыдущий номер последовательности.

После того, как контейнер и сообщение преобразованы, можно приступать непосредственно к внедрению информации:

1. Для каждого блока, соответствующему номеру из полученной ПСП, применяем дискретное косинусное преобразование.
2. Извлекаем первый бит из битовой последовательности, полученной после кодирования сообщения.
3. Выбираем значение уровня шума ($s > 0$). Чем выше уровень шума, тем выше уровень искажения сигнала.
4. Наиболее высокочастотный коэффициент заменяется значением уровня шума следующим образом:

$$F[N-1] = \begin{cases} -s, & b = 1 \\ s, & b = 0 \end{cases},$$

где F – массив коэффициентов ДКП; N – размерность массива коэффициентов; s – значение уровня шума, b – встраиваемый бит сообщения.

5. К текущему блоку применяется обратное дискретное косинусное преобразование.

Процесс повторяется до тех пор, пока в битовой последовательности есть значения.

Предложенный алгоритм обладает высокой надежностью, а также приемлемой пропускной способностью и сложностью реализации. Заполненный контейнер не будет отличаться от оригинального контейнера в силу человеческого восприятия.

ЛИТЕРАТУРА

1. Садов, В.С. Компьютерная стеганография / В.С. Садов – Минск: БГУ, 2010. – 211 с.
2. Blackledge, J. Resilient Digital Image Watermarking for Document Authentication / J. Blackledge, O. Iakovenko // IAENG International Journal of Computer Science. – 2014. – № 41(1). – С. 1-17.
3. Горелкина Д.А., Дорошенко Н.С., Осипов Д.Л. Применение методов цифровой стеганографии для внедрения конфиденциальной информации в растровые изображения // Вестник Ставропольского государственного университета. – 2011. – №75. – С. 75-76.
4. Грибунин В.Г., Оков И.Н., Туринцев В.И. Цифровая стеганография. – М. : СОЛОН-Пресс 2002. 272 с.