

УДК 003.26

## ИСПОЛЬЗОВАНИЕ ДИСКРЕТНОГО ТРИГОНОМЕТРИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ДЛЯ СТЕГАНОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ

Д. т. н. А. А. Шумейко, А. И. Пасько

Днепродзержинский государственный технический университет  
Украина, г. Днепродзержинск  
Shumeiko\_A@ukr.net

*Предложен метод стеганографической защиты данных, использующий вложение информации в изображение, сжатое методом JPEG, на основе искажения коэффициентов Фурье дискретного тригонометрического преобразования, адаптированного под конкретное изображение или под заданный класс изображений.*

*Ключевые слова: стеганография, JPEG, коэффициенты Фурье.*

Проблема информационной безопасности не уходит из заголовков информационных агентств, откровения Эдварда Сноудена только подлили «масла в огонь», что делает проблему защиты информации более актуальной. С другой стороны, информация о квантовых компьютерах ставит под вопрос будущее современных криптографических методов и протоколов (исключая квантовую криптографию). Выходом из сложившейся ситуации может быть использование методов стеганографической защиты данных. Методы компьютерной стеганографии достаточно эффективны при использовании в качестве контейнеров мультимедийных файлов, что связано, прежде всего, с их избыточностью. Искажения, вносимые в такой файл при внедрении достаточно малой порции информации, не приводят к существенной порче контейнера. Наиболее часто для такой роли используются статические изображения. Наиболее подходящим, можно сказать, удобным форматом для использования в качестве контейнера, является формат BMP, наиболее неудобным – JPEG [1]. К сожалению, популярность этих графических форматов диаметрально противоположна.

Среди методов внедрения информации в мультимедийные файлы самым распространенным является замена младших или менее значимых битов (LSB — Least Significant Bit). Его использование для внедрения информации в JPEG-файл возможно лишь при отсутствии сжатия, что делает в этом случае LSB-метод абсолютно неэффективным. Следовательно, информацию можно внедрять лишь в коэффициенты Фурье (если не считать использования областей, предназначенных для служебной информации). Изменение абсолютных значений коэффициентов дискретного косинус-преобразования (DCT) эффективно только при использовании низкочастотных коэффициентов, что скажется на качестве изображения, а высокочастотные коэффициенты подвержены разрушению на этапе квантования. Поэтому основным направлением исследования методов стеганографической защиты с использованием JPEG является поиск скрытых закономерностей, таких как сравнение коэффициентов DCT на соседних блоках [2] или их абсолютных значений [3].

Предлагается для внедрения информации использовать на тех же блоках  $8 \times 8$  пикселей коэффициенты ортогонального преобразования, отличного от DCT, используемого JPEG. Простейшим примером может быть дискретное преобразование Хартли (см., например, [4])

$$H_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} h_k \operatorname{cas} \left( \frac{2ik\pi}{N} \right),$$

где  $\operatorname{cas}\phi = \cos\phi + \sin\phi$ .

Для случая двух переменных дискретное преобразование Хартли можно записать в виде

$$H_{i,j} = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{n=0}^{N-1} h_{k,n} \operatorname{cas} \left( \frac{2ik\pi}{N} \right) \operatorname{cas} \left( \frac{2jn\pi}{N} \right).$$

Целью работы является улучшение качества использования стеганографической защиты данных с контейнером \*.JPEG путем использования одной модификации ДПФ, допускающей построение адаптивных фильтров. В основе полученных результатов лежит следующее утверждение.

Пусть  $\phi \in \left(0, \frac{\pi}{2}\right)$ , тогда для любых  $\{h_m\}_{m=0}^{N-1}$  таких, что  $-\infty < h_m < \infty, m = 0, 1, \dots, N-1$ , имеет место равенство

$$h_n = \frac{2}{N \sin(2\phi)} \sum_{k=0}^{N-1} H_k \sin\left(\frac{2\pi nk}{N} + \phi\right),$$

где

$$H_k = \sum_{m=0}^{N-1} h_m \cos\left(\frac{2\pi mk}{N} - \phi\right).$$

В случае  $\phi = \frac{\pi}{4}$ , получаем дискретное преобразование Хартли.

При обработке изображений (двумерных сигналов) используется двумерное дискретное тригонометрическое преобразование, так же как и DCT в JPEG, определенное на квадратах  $N \times N$  пикселей, где  $N=8$ . Двумерное дискретное тригонометрическое преобразование имеет вид –

— прямой ход

$$h_{i,j} = \frac{2}{N \sin(2\phi)} \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} p_{n,m} \cos\left(\frac{2\pi in}{N} - \phi\right) \cos\left(\frac{2\pi jm}{N} - \psi\right),$$

— обратный ход

$$p_{n,m} = \frac{2}{N \sin(2\psi)} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j} \sin\left(\frac{2\pi in}{N} + \psi\right) \sin\left(\frac{2\pi jm}{N} + \phi\right).$$

Использование (см. [3]) вместо коэффициентов DCT, коэффициентов дискретного тригонометрического преобразования  $h_{i,j}$ , позволяет подобрать углы  $\phi$  и  $\psi$  адаптивно под конкретное изображение или под некоторый класс изображений и построить достаточно эффективные методы стеганографической защиты информации.

#### ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Лигун А. А., Шумейко А. А. Комп'ютерна графіка /обробка та стиск зображень. — Днепропетровск: Біла К. О., 2010.
2. <http://www.guillermi2.net/stegano/jsteg/index.html>
3. Шумейко А. А., Пасько А. И., Тищенко Т. Н. Использование полиномиального прогноза для внедрения в изображение цифровых водяных знаков // Сучасний захист інформації.— 2010.— № 3.
4. Р. Брейсуэлл. Преобразование Хартли. — Москва: Мир, 1990.

A. A. Shumeiko, A. I. Pasko

#### Using discrete trigonometric transformation for steganographic data protection.

Steganographic method is proposed for data protection using inserts in the image compressed by JPEG - based distortion of the Fourier coefficients of the adaptive discrete trigonometric transformation for a specific image or for a given class of images.

Keywords: *steganography, JPEG, Fourier coefficients.*