УДК 004.056.5

СПЕКТРАЛЬНО-КОДОВАЯ СТЕГАНОГРАФИЧЕСКАЯ ЗАЩИТА ИЗОБРАЖЕНИЯ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

С.Б. САЛОМАТИН, Ю.Е. ЯВОРКО

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 13 ноября 2018

Аннотация. Рассмотрены алгоритмы каскадной спектрально-кодовой стеганографической защиты изображения в распределенных системах с использованием дискретного преобразования Фурье на первом этапе и метода разделения секрета (алгоритма Гарнера) – на втором.

Ключевые слова: стеганография, преобразование Фурье, разделение секрета, китайская теорема об остатках.

Введение.

В современных инфокоммуникационных технологиях широко используются распределенные системы передачи и обработки данных. Одна из задач информационной безопасности в таких системах связана со стеганографической защитой мультимедийных данных. При этом алгоритмы стеганографического кодирования, которые отображают структуру изображения в случайную структуру фона, могут изменить фрактальный характер изображения и привести к потерям при применении алгоритмов сжатия [1, 2].

Одним из путей решения такого рода задач является выполнение кодирования источника с помощью стеганографического спектрального преобразования Фурье и распределенного кодирования на основе метода разделения секрета для повышения криптостойкости.

Алгоритм стеганографического пробразования Фурье

1. Изображение определяется как массив данных $d\left(n_1, n_2\right)$, $n_1, n_2 = 0,1,...N-1$

2. Выполняется преобразование Фурье:

$F\{d\left(n_1, n_2\right)\} = \{D\left(m_1, m_2\right),\ m_1, m_2 = 0,1,...N-1$.

3. Выполняется сдвиг фаз компонент спектра на случайную величину $\theta_{rand}\left(0-2\pi\right)$.

4. В спектральной области выделяются области (кластеры), удовлетворяющие условию

$m-0,5 < \sqrt{m_1^2 + m_2^2} < m+0,5.$

Компонентам, попавшим в один и тот же кластер, ставится в соответствие одна и та же частота.

5. Частотные компоненты D_m в выделенных областях (кластерах), удовлетворяющих условию $m-0,5 < \sqrt{m_1^2 + m_2^2} < m+0,5$, заменяются случайными значениями φ_{rand} .

6. Вычисляются значения дисперсий σ_m^2 по формуле:

$$\sigma_m^2 = \left\langle \left(\upsilon_m\right)^2 \right\rangle = \frac{1}{N_m} \sum_{m-0,5<\sqrt{m_1^2+m_2^2}<m+0,5} \upsilon_{m_1,m_2}^2 ,$$

где N_m соответствует количеству компонент в кластере.

7. Выполняется масштабирование:

$$D'_m = D_m \cdot \frac{m^{\frac{\beta_1+1}{2}}}{m^{\frac{\beta_2+1}{2}}} = D_m m^{\Delta\beta/2},$$

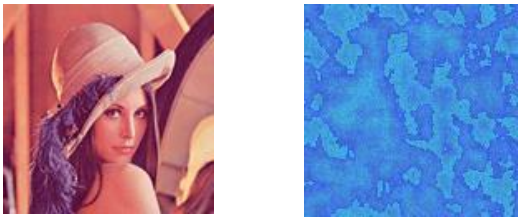
где β_1, β_2 – спектральные экспоненты исходного и преобразованного изображений, $\Delta\beta = \beta_1 - \beta_2$

7. Осуществляется переход в пространственную область с помощью нормированного обратного БПФ.

В результате было получено изображение (рис. 1), которое имеет случайные фазы спектральных составляющих $\theta'_{m_1,m_2} = \theta + \theta_{rand}$, а дисперсии амплитудных составляющих удовлетворяют условию фрактального распределения исходного изображения

$$\left\langle \left(D_m \right)^2 \right\rangle \propto 1/f^{\beta} \propto 1/m^{\beta}.$$

Процедура декодирования использует обратные операторы.



а *б*

Рис. 1. Результат применения стеганографического преобразование Фурье:
а – исходное изображение Lena; *б* – спектр стеганографического преобразования

Алгоритм вычисления отображений на основе метода разделения секрета

1. Выбирается число t, и массив данных преобразуется в новый массив B в виде матрицы из m строк и t столбцов.

2. Для каждой k-й строки матрицы и заданного значения x, вычисляется полином

$$s_k(x) = s_0 + s_1 x + \ldots + s_{t-1} x^{t-1} \pmod p.$$

3. Результаты вычислений образуют m строк массива A_x.

4. Массив A_x преобразуется в матрицу размером $a \times b$, которая является возвращаемым отображением.

5. Изменяя значение x и повторяя шаги 2 и 3 алгоритма, формируется множество n различных отображений.

Предположим, что имеется n различных отображений и используется (t,n)-схема разделения секрета [3]. Любая комбинация из t различных отображений позволяет построить алгоритм восстановления. Определим массив $X = \{x_0, x_1, \ldots, x_{t-1}\}$ для хранения значений x, соответствующих выбранным t отображениям.

Алгоритм восстановления массива данных по отображениям.

1. Все A_x-матрицы t отображений преобразуются в массивы длиной m.

2. Элемент с номером i каждого массива задается как $s_i(x_l)$, где l – индекс соответствующего массива, а x_l представляет собой l-й элемент массива X. В результате формируются t значений. $s_i(x_0), s_i(x_1), \ldots, s_i(x_{t-1})$.

3. Составляется система уравнений следующего вида

$$s_i\left(x_0\right) \equiv s_0^i + s_1^i x_0 + ... + s_{t-1}^i x_0^{t-1} \left(\mathrm{mod}\, p\right),$$

. . .

$$s_i\left(x_{t-1}\right) \equiv s_0^i + s_1^i x_{t-1} + ... + s_{t-1}^i x_{t-1}^{t-1} \left(\mathrm{mod}\, p\right).$$

Решение системы уравнения дает значения $s_0^i, ..., s_{t-1}^i$, являющиеся элементами i-й строки восстанавливаемого массива B.

4. Шаги 2 и 3 алгоритма повторяются, до тех пор, пока все элементы каждого массива не будут вычислены, что дает полный восстановленный массив B.

5. Массив B размером $m \times t$ преобразуется в массив исходного размера $H \times W$, что дает восстановление исходного массива данных.

6. Если выбрана (t, n) - пороговая схема и N – произведение наименьших t их них, а M-произведение $t-1$ наибольших. Тогда при нехватке одной части для восстановления результата недостающий множитель находится среди более, чем $\frac{N-M}{M}$ целых чисел (алгоритм Гарнера).

Из китайской теоремы об остатках следует, что можно заменять операции над числами операциями над кортежами. Каждому числу a ставится в соответствие кортеж $(a_1, ..., a_k)$, где $a_i \equiv a\left(\mathrm{mod}\, n_i\right)$. Решение дается в смешанной системе счисления:

$$a = x_1 + x_2 \cdot n_1 + x_3 \cdot n_1 \cdot n_2 + \ldots + x_k \cdot n_1 \cdot \ldots \cdot n_{k-1}.$$

Обозначим r_{ij} через $(i = 1...k-1, j = i+1...k)$ число, являющееся обратным для n_i по модулю n_j: $r_{ij} = (n_i)^{-1} \,(\mathrm{mod}\, n_j)$.

Подставим выражение a в смешанной системе счисления в первое уравнение системы. В результате получим $a_1 \equiv x_1$. Подставим теперь выражение во второе уравнение: $a_2 \equiv x_1 + x_2 \cdot n_1 \,(\mathrm{mod}\, n_2)$. Преобразуем это выражение, отняв от обеих частей x_1 и разделив на n_1:

$$a_2 - x_1 \equiv x_2 \cdot n_1 \,(\mathrm{mod}\, n_2);\ (a_2 - x_1) \cdot r_{12} \equiv x_2 \,(\mathrm{mod}\, n_2);.\ x_2 \equiv (a_2 - x_1) \cdot r_{12} \,(\mathrm{mod}\, n_2).$$

Подставляя в третье уравнение, аналогичным образом получаем:

$$a_3 \equiv x_1 + x_2 \cdot n_1 + x_3 \cdot n_1 \cdot n_2 \,(\mathrm{mod}\, n_3);$$

$$(a_3 - x_1) \cdot r_{13} \equiv x_2 + x_3 \cdot n_2 \,(\mathrm{mod}\, n_3);$$

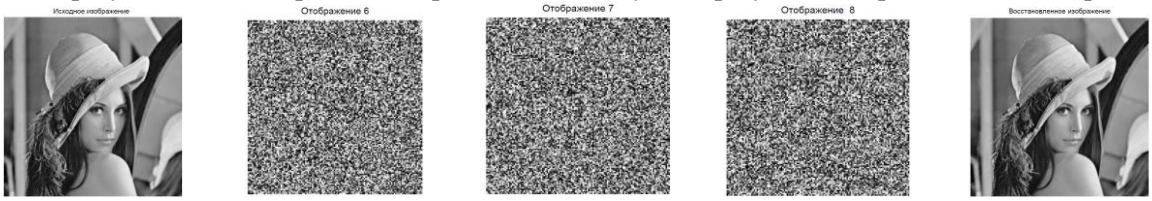
$$((a_3 - x_1) \cdot r_{13} - x_2) \cdot r_{23} \equiv x_3 \,(\mathrm{mod}\, n_3);$$

$$x_3 \equiv ((a_3 - x_1) \cdot r_{13} - x_2) \cdot r_{23} \,(\mathrm{mod}\, n_3).$$

Число a восстанавливается по формуле :

$$a = x_1 + x_2 \cdot n_1 + x_3 \cdot n_1 \cdot n_2 + \ldots + x_k \cdot n_1 \cdot \ldots \cdot n_{k-1}.$$

В результате моделирования в среде MatLab получены результаты, представленые на рис. 2.



а *б* *в* *г* *д*

Рис. 2. Моделирование алгоритма разделения секрета: *а* – исходное изображение; *б, в, г* – кодировка изображения алгоритмом разделения секрета; *д* – восстановленное изображение

Заключение

Применение ДПФ сохраняет фрактальный характер стеганографического изображения. Защита схемы каскадного кодирования обеспечивается ключом сдвига фаз спектрального преобразования и невозможностью вычислить точно t-й корень системы из $(t-1)$ уравнений при криптоанализе алгоритма разделения секрета.

SPECTRAL-CODE STEGANOGRAPHIC PROTECTION OF THE IMAGE IN DISTRIBUTED SYSTEMS

S.B. SALOMATIN, Yu.E. YAVORKO

Abstract. Algorithms of spectral code steganographic protection of the image in a distributed systems using the Fourier transform and the method of secret separation and the Garner algorithm are considered.

Keywords: steganography, Fourier transform, secret separation, Chinese remainder theorem.

Список литературы

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика К., 2006.
2. Д. Ватолин [и др.] Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М., 2002.
3. Wang S., Fang Y., Cheng S. Distributed source coding theory and practice. Wiley, 2017