АЛГОРИТМЫ ВСТРАИВАНИЯ И ИЗВЛЕЧЕНИЯ ИНФОРМАЦИИ ИЗ ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ВЕЙВЛЕТ-АНАЛИЗА

Лобач В. И.
Кафедра математического моделирования и анализа данных, Белорусский государственный университет
Минск, Республика Беларусь
E-mail: lobach@bsu.by

Предлагается и исследуется алгоритм встраивания и извлечения информации на основе дискретного вейвлет-преобразования матрицы пикселей исходного изображения.

Введение

Развитие средств вычислительной техники дало мощный толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Большинство исследований так или иначе связаны с цифровой обработкой сигналов. Сообщения встраиваются в цифровые данные, имеющие аналоговую природу и речь, аудиозаписи, изображения, видео [1, 2]. Известны также работы по встраиванию информации в текстовые файлы и в исполняемые файлы программ. В данной работе рассматривается один из возможных алгоритмов встраивания информации с использованием целочисленного вейвлет-преобразования.

I. Целочисленное вейвлет-преобразование цифрового изображения

Дискретное изображение I представляет собой $M \times N$ матрицу действительных чисел

$$\mathrm{I} = \begin{pmatrix} \mathrm{I}_{11} & \mathrm{I}_{12} & \dots & \mathrm{I}_{1N} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{I}_{M1} & \mathrm{I}_{M2} & \dots & \mathrm{I}_{MN} \end{pmatrix}. \quad (1)$$

Вейвлет-преобразование матрицы I получается следующим образом:
1) дискретное вейвлет-преобразование применяется к каждой строке матрицы (1), в результате чего генерируется новая матрица;
2) дискретное вейвлет-преобразование применяется к сгенерированной на предыдущем шаге матрице, но теперь ко всем столбцам.

Получаются четыре матрицы, каждая из которых имеет размерность $M/2 \times N/2$:

$$\begin{pmatrix} \mathrm{D}^1 & \mathrm{C}^1 \\ \mathrm{B}^1 & \mathrm{A}^1 \end{pmatrix}. \quad (2)$$

Подматрица A^1 матрицы (2) представляет собой сжатое (огрубленное) исходное изображение (с так называемыми низкочастотными компонентами). Подматрица B^1 сохраняет горизонтальные детали изображения, подматрица C^1 аналогична подматрице B^1 за исключением того, что она сохраняет вертикальные детали изображения (уточняющие коэффициенты). Подматрица D^1 содержит диагональные детали изображения.

На втором шаге проводим те же операции с подматрицей A^1, полученной на первом шаге, в результате чего получаются матрицы второго уровня A^2, B^2, C^2, D^2 и т. д.

Приведем формулы, определяющие элементы матриц A, B, C, D, если в качестве базового вейвлета выбран вейвлет Хаара [3]:

$$\mathrm{A}_{ij} = (\mathrm{I}_{2i,2j} + \mathrm{I}_{2i+1,2j})/2, \quad (3)$$

$$\mathrm{B}_{ij} = \mathrm{I}_{2i,2j+1} - \mathrm{I}_{2i,2j}, \quad (4)$$

$$\mathrm{C}_{ij} = \mathrm{I}_{2i+1,2j} - \mathrm{I}_{2i,2j}, \quad (5)$$

$$\mathrm{D}_{ij} = \mathrm{I}_{2i+1,2j+1} + \mathrm{I}_{2i,2j}, \quad (6)$$

где $1 \le i \le M/2$, $1 \le j \le N/2$.

Очевидно, что формулы (3)–(6) обратимы, и мы можем однозначно восстановить исходное изображение по вычисленным коэффициентам вейвлет-преобразования. Обратное вейвлет-преобразование задается следующими формулами:

$$\mathrm{I}_{2i,2j} = \mathrm{A}_{ij} - \mathrm{B}_{ij}/2, \quad (7)$$

$$\mathrm{I}_{2i,2j+1} = \mathrm{A}_{ij} + \mathrm{B}_{ij}/2, \quad (8)$$

$$\mathrm{I}_{2i+1,2j} = \mathrm{I}_{2i,2j+1} + \mathrm{C}_{ij} - \mathrm{B}_{ij}, \quad (9)$$

$$\mathrm{I}_{2i+1,2j+1} = \mathrm{I}_{2i,2j+1} + \mathrm{D}_{ij} - \mathrm{C}_{ij}, \quad (10)$$

где $1 \le i \le M/2$, $1 \le j \le N/2$.

II. Алгоритмы встраивания сообщения в изображение

На вход алгоритма встраивания поступает контейнер $\mathrm{I} = (\mathrm{I}_{ij})$, $i = \overline{1, M}$, $j = \overline{1, N}$, представляющий собой цветное изображение $M \times N$ пикселей, и скрываемое сообщение $m = (m_1, \dots, m_T)$, $m_i \in \{0, 1\}$, длины T бит. Алгоритм встраивания состоит из следующих шагов:
1) к изображению I согласно формулам (3)–(6) применяется дискретное вейвлет-преобразование, глубина разложения d дается пользователем, рекомендуется брать не более 3-4-х уровней декомпозиции;

Библиотека БГУИР

2) выбирается подматрица коэффициентов, в которую будет встраиваться сообщение. По завершении декомпозиции на уровне глубины d возможно 4^d различных подматриц вейвлет-коэффициентов;
3) на основании полученных данных генерируется стегоключ $Key = (Y, T, K)$, где $Y \in R^3$ – параметры генератора случайных чисел, $T \in N$ – длина встраиваемого сообщения, $K \in N^3$ – число уровней декомпозиции, номер подматрицы для встраивания и размер блока коэффициентов;
4) на основании длины сообщения T задается число блоков изменяемых вейвлет-коэффициентов. Используя сгенерированный ранее параметр ключа Y, случайным образом выбираются номера блоков и их порядок, согласно которому будет производиться встраивание. Далее генерируется двоичный случайный образ, согласно которому каждый блок E_i коэффициентов делится на два субблока E_{i0} и E_{i1}. Для каждого субблока вычисляются средние значения l_{i0} и l_{i1}, выбирается некоторый порог α, и бит сообщения встраивается следующим образом:

$$\begin{array}{ll} l_{i0} - l_{i1} \geq \alpha, & \text{если} \quad m_i = 1, \\ l_{i0} - l_{i1} < -\alpha, & \text{если} \quad m_i = 0. \end{array}$$

Если эти условия не выполняются, то значения субблока B_{i1} изменяются до тех пор, пока одно из условий не будет выполнено;
5) по формулам (7)–(10) обратного вейвлет-преобразования вычисляется стеганограмма $\mathrm{I}^* = (\mathrm{I}^*_{ij})$, $i = \overline{1, M}, j = \overline{1, N}$.

III. Алгоритмы извлечения сообщения из графического изображения

На вход алгоритма извлечения поступает стеганограмма $\mathrm{I}^* = (\mathrm{I}^*_{ij})$, $i = \overline{1, M}, j = \overline{1, N}$, и стегоключ $Key = (Y, T, K)$, сформированный в процессе сокрытия данных. Алгоритм извлечения состоит в следующем:
1) к последовательности I^* согласно формулам (3)–(6) применяется целочисленное вейвлет-преобразование. Глубина декомпозиции определяется на основе параметра ключа $K \in N^3$;
2) на основании параметров ключа $K \in N^3$ определяется подматрицы, в коэффициенты которых производилось встраивание информации, размер блока, содержащего бит сообщения; используя параметры T и Y, восстанавливается количество и порядок субблоков B^*_i коээфициентов, в которых выбрано сообщение.
3) для извлечения бита сообщения из блока B^*_i вейвлет-коэффициентов вычисляются средние значения его субблоков l^*_{i0} и l^*_{i1}, разность между этими значениями позволяет определить искомый бит: $m^*_i = 1$, если $l^*_{i0} - l^*_{i1} > 0$, $m^*_i = 0$, если $l^*_{i0} - l^*_{i1} < 0$;
4) формируется последовательность $m^* = (m^*_1, \ldots < m^*_T)$, $m^*_i \in \{0, 1\}$, состоящая из битов извлеченного сообщения. Извлеченная из стеганограммы последовательность $m^* = (m^*_1, \ldots < m^*_T)$ подается на выход алгоритма.

Проводилась компьютерная реализация указанных алгоритмов, в качестве контейнера использовались графические черно-белые изображения формата bmp. В качестве скрываемых данных использовались файлы формата txt размером от 0.5% до 5% от размеров контейнера – восстановление сообщения было без искажений; при объеме скрываемого сообщения более 5% имелись искажения в извлеченном сообщении.

IV. Список литературы

1. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков – М.: Солон-Пресс, 2002. – 272 с.
2. Хорошко, В. А. Введение в компьютерную стеганографию / В. А. Хорошко, М. Е. Шелест – Киев: МиПресс, 2006. – 178 с.
3. Малла, С. Вейвлеты в обработке сигналов / С. Малла – М.: Мир, 2005. – 671 с.

Библиотека БГУИР