**УДК 004.021**

# РАЗРАБОТКА СИСТЕМЫ ДЛЯ СКРЫТИЯ ИНФОРМАЦИИ НА ОСНОВЕ ДИСКРЕТНЫХ ПРЕОБРАЗОВАНИЙ С ПОМОЩЬЮ АЛГОРИТМА КОХА И ЖАО

***К.В. СТАНКЕВИЧ***
***(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)***

*Рассматриваются алгоритм скрытия данных в изображении на основе дискретных преобразований, описание работы основной программы и основные функции разрабатываемого программного продукта.*

**Введение.** Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Выделилось два основных направления решения этой задачи криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения. Скрытие информации возможно лишь благодаря тому, что противнику неизвестен метод скрытия. Система защиты информации должна обеспечивать свои функции даже при полной информированности противника о её структуре и алгоритмах функционирования

**Основная часть.** В статье будет рассмотрен стеганографический метод скрытия информации в изображениях, как с точки зрения устойчивости к различным видам атак, так и с точки зрения сохранения приемлимого качества изображения.

Алгоритм Коха-Жао для встраивания информации использует частотную область контейнера и заключается в относительной замене величин коэффициентов дискретного косинусного преобразования (ДКП).

Основными функциями разрабатываемого программного продукта являются:

– шифрование информации;
– дешифрование информации;
– вывод промежуточной информации о выполненных операциях.

Рассматриваемая методика ляжет в основу разрабатываемого программного продукта «Скрытие информации на основе дискретных преобразований методом Коха и Жао», который реализует все задачи, в частности, главную – скрыть факт передачи информации.

При проектировании приложения были выделены следующие классы (рис.):

– Koch – класс, реализующий алгоритм;
– Converter – класс для работы с двоичным представлением чисел;
– Form1 – пользовательский интерфейс.

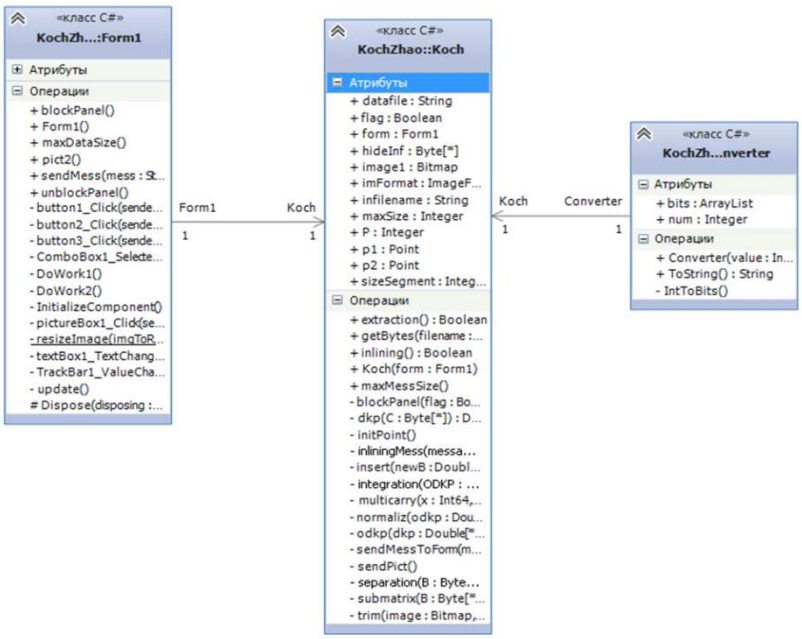


**Рисунок. – Диаграмма классов**

Для скрытия информации методом Коха и Жао необходимо выполнить следующие пункты:

1. Изображение-контейнер разбивается на блоки 8 на 8, 4 на 4 или 2 на 2 пикселей.
2. К каждому блоку применяется дискретное косинусное преобразование. В результате получаем матрицы 8 на 8 коэффициентов ДКП.
3. Выбирается любой блок (в каждый блок записывается 1 бит информации).
4. Выбираются два коэффициента ДКП в каждом блоке из высокочастотных коэффициентов.
5. Для передачи бита 0 необходимо, чтобы разница модулей коэффициентов ДКП превышала некоторую положительную величину (задается вручную); для передачи бита 1 разница должна быть меньшей по сравнению с некоторой отрицательной величиной. Таким образом, при передаче 0 увеличиваем модуль первого коэффициента и уменьшаем модуль второго. При передаче 1 уменьшаем модуль первого коэффициента и увеличиваем модуль второго.
6. Выполняем пункты 3-5 до окончательной записи всего сообщения.
7. Для каждого блока выполняем обратное ДКП.
8. Блоки собираются обратно в изображение.

Извлечение:

1. Изображение-контейнер разбивается на блоки 8 на 8, 4 на 4 или 2 на 2 пикселей.
2. К каждому блоку применяется дискретное косинусное преобразование. В результате получаем матрицы 8 на 8 коэффициентов ДКП.
3. Выбирается любой блок (в каждый блок записывается 1 бит информации).
4. Считаем разность модулей двух коэффициентов ДКП.
5. В результате проверки разности модулей извлекаемому биту присваивается 0 или 1.

При обработке изображения будет использоваться двумерная версия дискретного косинусного преобразования:

$$\Omega(u,v) = \frac{\zeta(u)\cdot\zeta(v)}{\sqrt{2N}} \cdot \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(x,y) \cdot \cos\left[\frac{\pi\cdot u\cdot(2x+1)}{2N}\right] \cdot \cos\left[\frac{\pi\cdot v\cdot(2y+1)}{2N}\right], \quad (1)$$

$$S(x,y) = \frac{1}{\sqrt{2N}} \cdot \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \zeta(u) \cdot \zeta(v) \cdot \Omega(u,v) \cdot \cos\left[\frac{\pi\cdot u\cdot(2x+1)}{2N}\right] \cdot \cos\left[\frac{\pi\cdot v\cdot(2y+1)}{2N}\right], \quad (2)$$

где $C(x,y)$ и $S(x,y)$ – соответственно, элементы исходного и восстановленного по коэффициентам ДКП изображения размерностью $N \times N$;

$x, y$ – пространственные координаты пикселей изображения;

$\Omega(u,v)$ – массив коэффициентов ДКП;

$u, v$ – координаты в частотной области;

$\zeta(u) = \frac{1}{\sqrt{2}}$, если $u = 0$, и $\zeta(u) = 1$, если $u > 0$; $\zeta(v) = \frac{1}{\sqrt{2}}$, если $v = 0$, и $\zeta(v) = 1$, если $v > 0$.

Программа прямого дискретного косинусного преобразования, соответствующая формуле (1) реализована так:

**Листинг 1** – Прямое ДКП

```
1:  private double[,] dkp(byte[,] C){
2:  int n = C.GetLength(0);
3:  double[,] result = new double[n, n];
4:  double U, V, temp = 0;
5:  for (int v = 0; v < n; v++){
6:  for (int u = 0; u < n; u++) {
7:  if (v == 0) V = 1.0 / Math.Sqrt(2);
8:  else V = 1;
9:  if (u == 0) U = 1.0 / Math.Sqrt(2);
10: else U = 1;
11: temp = 0;
12: for (int i = 0; i < n; i++){
13: for (int j = 0; j < n; j++){temp += C[i, j] * Math.Cos(Math.PI *
14: v * (2 * i +1) / (2 * n)) * Math.Cos(Math.PI * u * (2 * j + 1) /
15: (2 * n));}}
16: result[v, u] = U * V * temp / (Math.Sqrt(2 * n));}}
17: return result;
18: }
```

Программа обратного дискретного косинусного преобразования, соответствующая формуле (2) была реализована так:

**Листинг 2** – Обратное ДКП

```
1:  private double[,] odkp(double[,] dkp) {
2:  int n = dkp.GetLength(0);
3:  double[,] result = new double[n, n];
4:  double U, V, temp = 0;
5:  for (int v = 0; v < n; v++){
6:  for (int u = 0; u < n; u++){
7:  temp = 0;
8:  for (int i = 0; i < n; i++){
9:  for (int j = 0; j < n; j++){
10: if (i == 0) V = 1.0 / Math.Sqrt(2);
11: else V = 1;
12: if (j == 0) U = 1.0 / Math.Sqrt(2);
13: else U = 1;
14: temp += U * V * dkp[i, j] * Math.Cos(Math.PI * i * (2 * v + 1) /
15: (2 * n)) * Math.Cos(Math.PI * j * (2 * u + 1) / (2 * n));}}
16: result[v, u] = temp / (Math.Sqrt(2 * n));}}
17: return result;
18: }
```

В результате получаются матрицы 8×8 коэффициентов ДКП, которые зачастую обозначают $\Omega b(u, v)$, где $b$ – номер блока контейнера $C$, а $(u, v)$ – позиция коэффициента в этом блоке. Каждый блок при этом предназначен для скрытия одного бита данных.

Для выбора каждого следующего блока для скрытия одного бита сообщения будет использоваться генератор ПСП «Marsaglia-Multicarry» основанный на методе умножения с переносом.

На следующем этапе выбираются два конкретных коэффициента ДКП из каждого блока, которые будут использоваться для скрытия данных. Для скрытия данных будут использоваться блоки из области высоких частот, что приведет к наименьшим искажениям контейнера. Данные коэффициенты задаются их координатами в массивах коэффициентов ДКП: (u1,v1) и (u2,v2).

Во время организации секретного канала абоненты должны предварительно договориться о двух конкретных коэффициентах ДКП из каждого блока.

**Заключение.** В данной статье был рассмотрен алгоритм скрытия данных в изображении на основе дискретных преобразований, описание работы основной программы и основные функции разрабатываемого программного продукта.

ЛИТЕРАТУРА

1. Садов, В.С. Компьютерная стеганография (конспект лекций) / В.С. Садов. – Минск : Белорус. гос. ун-т, 2010.
2. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев – М. : Солон-Пресс, 2002.