УДК 004.056

ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ АЛГОРИТМА КОЧА ДЛЯ СОКРЫТИЯ ДАННЫХ В QR-КОД

Ковынёв Н.В.

Московский Государственный Технический Университет имени Н.Э. Баумана
Москва, Российская Федерация

Одна из сложных задач, которую приходится решать в современном цифровом обществе: размещение большого количества информации на ограниченной площади. С применением QR-кода данная задача перестала быть неразрешимой. Используя данный инструмент, можно донести до пользователя требуемую ему информацию или же скрыть в QR-коде информацию, которая сможет защитить от подделки какое-либо изделие или продукт [1]. В данной статье будет рассмотрено применение стегозаписи в контейнер QR-кода с применением алгоритма Коча.

В качестве проверки устойчивости записи будут проделаны следующие действия: пересылка стегосообщения по интернету и попытка его восстановления; фотография и распознования стего при помощи смартфона.

В алгоритме Коча[2] в блок размером NxN осуществляется встраивание 1 бита ЦВЗ (цифровых водяных знаков). Псевдослучайно выбираются два коэффициента ДКП (дискретное косинусное преобразование). Встраивание информации осуществляется следующим образом: для передачи бита 0 добиваются того, чтобы разность абсолютных значений коэффициентов была бы больше некоторой положительной величины, а для передачи бита 1 эта разность делается меньше некоторой отрицательной величины:

$$|c_b(j_{i,j},k_{i,1})| - |c_b(j_{i,2},k_{i,2})| > \varepsilon, if\ s_i = 0$$
$$|c_b(j_{i,j},k_{i,1})| - |c_b(j_{i,2},k_{i,2})| < -\varepsilon, if\ s_i = 1.$$

Рисунок 1 – Коэффициенты

В QR-код помещено сообщение: «Обнаружение и распознавание сигналов». Загрузим созданный QR-код формата bmp в среду MathCAD.

Рисунок 2 – QR-код

Далее формируется матрица (число строк X и число столбцов Y) и разбивается на блоки размерности N, общее количество блоков обозначается N_total:

X:=rows (qr_code) = 297, Y:=cols (qr_code) = 297

Далее вычисляются коэффициенты ДКП Фурье для каждого блока и пременяется прямое

$$\xi(\chi) := \begin{cases} \frac{1}{\sqrt{2}} & \text{if } \chi = 0 \\ 1 & \text{if } \chi > 0 \end{cases}$$

$$\text{Right\_DCT(Blocks)} := \left| \begin{array}{l} \text{for } b \in 0..N\_total-1 \\ \quad \text{for } \upsilon \in 0..N-1 \\ \quad \text{for } \nu \in 0..N-1 \\ \quad \Omega r_{\upsilon,\nu} \leftarrow \frac{\xi(\nu)\cdot\xi(\upsilon)}{\sqrt{2\cdot N}} \cdot \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\left[(Blocks_b)_{x,y} \cdot \cos\left[\frac{\pi\cdot\upsilon\cdot(2\cdot x+1)}{2\cdot N}\right] \cdot \cos\left[\frac{\pi\cdot\nu\cdot(2\cdot y+1)}{2\cdot N}\right]\right] \\ \quad \Omega_b \leftarrow \Omega r \\ \Omega \end{array} \right.$$

Рисунок 3 – ДКП

Зададим параметры стегозаписи в контейнер. Наше стегосообщение:

Message := "Hometask. Koch algorithm"

В качестве ключа в выбранном алгоритме используются две позиции коэффициентов в матрице ДКП, которые будут использоваться при встраивании и извлечении сообщения:

$$\upsilon_1 := 4 \quad \upsilon_2 := 5 \quad \nu_1 := 3 \quad \nu_2 := 4$$

Для выбранного алгоритма также необходимо задать значение порога, с которым будут сравниваться результаты разности модулей коэффициентов ДКП, выбранных в качестве ключа.

Встраивание стего:

$$\text{D2B(x)} := \left| \begin{array}{l} \text{for } i \in 0..N-1 \\ \quad v_i \leftarrow \text{mod}(x,2) \\ \quad x \leftarrow \text{floor}\left(\frac{x}{2}\right) \\ v \end{array} \right.$$

Рисунок 4 – Встраивание стего

Выполнение обратного ДКП:

$$\text{Inverse\_DCT(Blocks)} := \left| \begin{array}{l} \text{for } b \in 0..N\_total-1 \\ \quad \text{for } x \in 0..N-1 \\ \quad \text{for } y \in 0..N-1 \\ \quad \Omega r_{x,y} \leftarrow \frac{1}{\sqrt{2\cdot N}} \cdot \sum_{\upsilon=0}^{N-1}\sum_{\nu=0}^{N-1}\left[\xi(\nu)\cdot\xi(\upsilon)\cdot(Blocks_b)_{\upsilon,\nu} \cdot \cos\left[\frac{\pi\cdot\upsilon\cdot(2\cdot x+1)}{2\cdot N}\right] \cdot \cos\left[\frac{\pi\cdot\nu\cdot(2\cdot y+1)}{2\cdot N}\right]\right] \\ \quad \Omega_b \leftarrow \Omega r \\ \Omega \end{array} \right.$$

Рисунок 5 – Обратное ДКП

Восстанавливаем исходную матрицу:

```
qr_stego := | QR ← Ω_Stego_0
            | for b ∈ 1..X÷N − 1
            |   QR ← stack(QR, Ω_Stego_b)
            | QR_r ← 0
            | for b ∈ (X÷N)..N_total − 1
            |   QR_r ← Ω_Stego_b  if QR_r = 0
            |   QR_r ← stack(QR_r, Ω_Stego_b)  otherwise
            |   QR ← augment(QR, QR_r)  if mod(b + 1, X/N) = 0
            |   QR_r ← 0  if mod(b + 1, X/N) = 0
            | QR ← (QR + |min(QR)|)·255 / max(QR + |min(QR)|)
```

Рисунок 6 – Восстановление матрицы

Сохраняем в файл с названием «stego.bmp»:

WRITEBMP("stego.bmp") := qr_stego

qr_stego

Рисунок 7 – QR-код со стего

Попробуем считать QR-код с помощью приложения на смартфоне:

Рисунок 8 – Сообщение

Как мы видим, стегосообщение никак не повлияло на содержание записанного в QR-код сообщения и успешно скрыто.

Восстановим стего: разбиваем матрицу на блоки размерности N:

Blocks2 := fragmentation(qr_stego)

Применяем прямое ДКП и определяем ключ:

Ω2 := Right_DCT(Blocks2)

$$B2D(x) := \sum_{i=0}^{N-1} \left(x_i \cdot 2^i\right)$$

Восстанавливаем стего:

```
stego := | j ← 0
         | for k ∈ 0..strlen(Message) − 1
         |   for i ∈ 0..N − 1
         |     Ωr ← Ω2_j
         |     ω_1 ← |Ωr(υ_1, ν_1)|
         |     ω_2 ← |Ωr(υ_2, ν_2)|
         |     m_i ← 0  if ω_1 > ω_2
         |     m_i ← 1  if ω_1 < ω_2
         |     j ← j + 1
         |   stego_k ← B2D(m)
         |   m ← 0
         | stego
```

Рисунок 9 – Стего восстановление

Как мы видим, стегосообщение удачно восстановлено.

В данной статье были изучены возможности применения стегозаписи в контейнер в виде QR-кода для хранения ключей, либо персональных данных и написана программа, реализующая занесение текстового стего в QR-код.

В ходе экспериментов стегосообщение было успешно скрыто от расшифровки сканером QR-кода и успешно восстановлено по ключу.

Литература

1. Ковалёв А.И. QR-коды, их свойства и применение // Молодой ученый. – 2016. – № 10. – С. 56–59. – URL https://moluch.ru/archive/114/ 29398/ (дата обращения: 20.09.2018).

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. Москва, СОЛОН-Пресс, 2002, 272 с.

УДК 539.3

ИЗГИБ УПРУГОПЛАСТИЧЕСКОЙ КРУГОВОЙ ТРЁХСЛОЙНОЙ ПЛАСТИНЫ НА СЛОЖНОМ ОСНОВАНИИ

Козел А.Г.

Белорусский государственный университет транспорта, Гомель, Беларусь

В настоящее время использование трёхслойных конструкций в машино- и приборостроении повлекло за собой интенсивную разработку теорий и методов их расчёта. Деформирование круговых трехслойных пластин в настоящее время изучено, в основном, при опирании на однопараметрическое основание Винклера.

Модель упругого основания с использованием двух коэффициентов постели, учитывающая его сжимаемость и связность, была впервые ис-