Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
Высшего профессионального образования
«Национальный исследовательский ядерный университет «МИФИ»
Факультет
«Кибернетика и информационная безопасность»
Кафедра № 43
«Стратегические информационные исследования»

Метод защиты кадров (изображений) с помощью обратимых геометрических преобразований.

Исполнитель: аспирант кафедры 43 Абрамов А.А.
Научный руководитель: к.т.н. Мельников Д.А.

Москва 2016

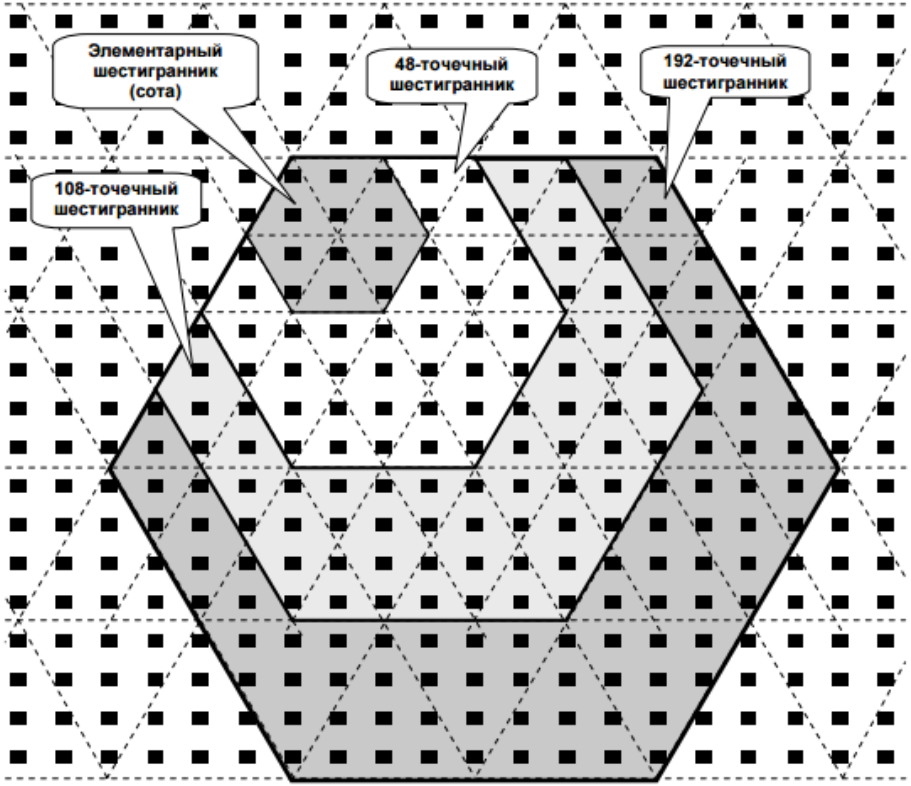
Цель работы

Разработать алгоритм защиты кадров (изображений) с использованием поворота геометрических фигур, определить свойства такого алгоритма, определить область его применимости в практических задачах.

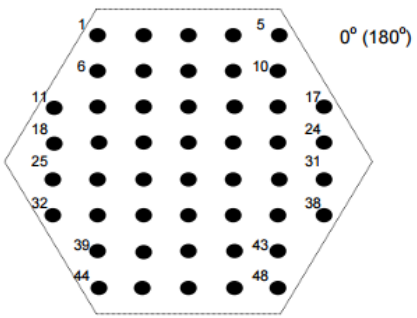
Основные задачи

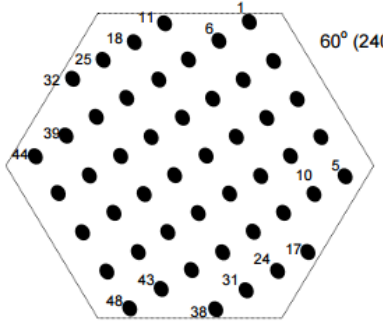
- Изучение метода защиты неподвижных изображений с использованием поворота шестигранника.
- Поиск и описание путей реализации данного метода.
- Определение критериев применимости, граничных условий, условий ослабляющих свойства данного метода.
- Выбор и обоснование наиболее удачной конфигурации рассматриваемого метода.
- Подробное описание полученного метода и сравнение с аналогичными, близкими либо альтернативными методами защиты.
- Создание полноценного криптографического алгоритма.

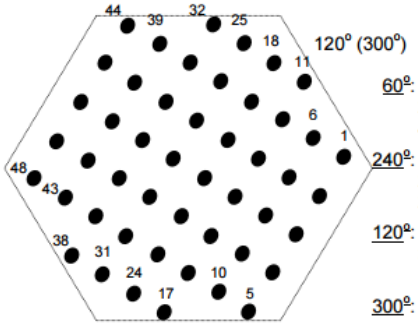
Метод защиты неподвижных изображений с использованием поворота шестигранника



Преобразование: поворот шестигранника







180°: 48 47 46 45 ... 3 2 1

60°: 5 17 10 24 4 16 31 9 23 38 3 15 30 8 22 37 2 14 29 43 7 21 36 48 1 13 28 42 6 20 35 47 12 27 41 19 34 46 11 26 40 18 33 45 25 39 32 44

240°: 44 32 39 25 45 33 18 40 26 11 46 34 19 41 27 12 47 35 20 6 42 28 13 1 48 36 21 7 43 29 14 2 37 22 8 30 15 3 38 23 9 31 16 4 24 10 17 5

120°: 38 48 31 43 24 37 47 17 30 42 23 36 46 16 29 41 10 22 35 45 5 15 28 40 9 21 34 44 4 14 27 39 8 20 33 3 13 26 7 19 32 2 12 25 6 18 1 11

300°: 11 1 18 6 25 12 2 32 19 7 26 13 3 33 20 8 39 27 14 4 44 34 21 9 40 28 15 5 45 35 22 10 41 29 16 46 36 23 42 30 17 47 37 24 43 31 48 38

Преобразование: поворот шестигранника

- Задача поворота шестигранника была заменена на эквивалентную задачу перестановки элементов, решение которой эквивалентно повороту шестигранника

- Предложено несколько решений по реализации перестановки для реальных изображений, выявлены достоинства и недостатки каждого

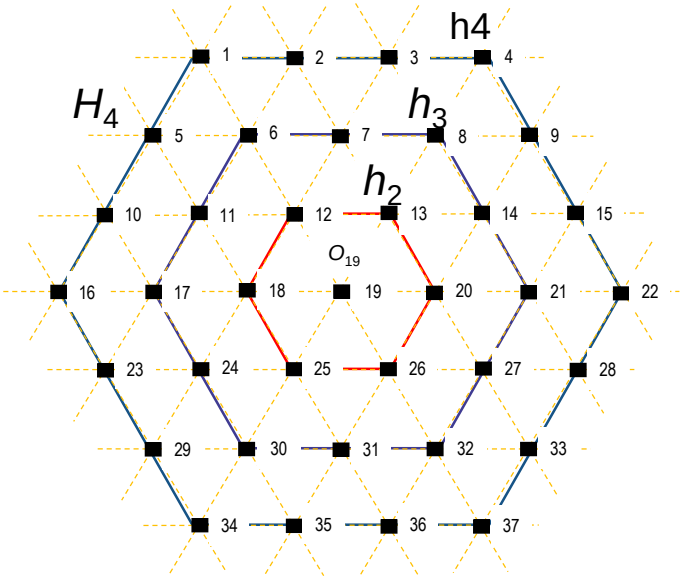
Перестановка эквивалентная повороту шестигранника

Для решения задачи по реализации перестановки эквивалентной повороту шестигранника были выделены 2 подзадачи:

1) выделение элементов из изображения над которыми будет осуществляться перестановка;

2) перестановка выбранных элементов.

Перестановка эквивалентная повороту шестигранника



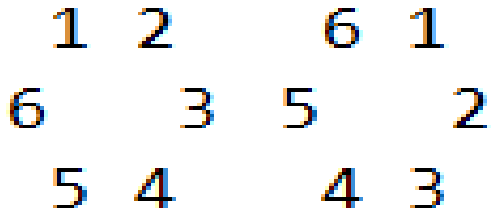
Шестигранник H_4 и контурные шестигранники h_4, h_3 и h_2

Перестановка эквивалентная повороту шестигранника

Количество точек изображения входящих в состав шестигранника сторона которого содержит n точек изображения можно рассчитать по формуле:

$$S_n = 3n^2 - 3n + 1\ .$$

Перестановка эквивалентная повороту шестигранника



Записав элементы шестигранника в строку получаем: 123456, после поворота 612345, видно, что поворот на 60 это сдвиг на n-1 элемент где n – размерность контурного шестигранника (или же количество элементов в его грани).

Таким образом поворот шестигранника размерности N представляет из себя сдвиг на *n*-1 элемент каждого из *N* – 1 контурных шестигранников размерности n, где 1<*n*<*N*+1 *n* – целое. То есть перестановка - поворот шестигранника размерности *N* может быть разложена в композицию перестановок поворота контурных шестигранников, из которых шестигранник размерности *N* состоит.

Верхняя оценка количества перестановок для изображения

Пусть: m – количество точек в изображении,
x – максимальное целое удовлетворяющее условию:
$m \geq 3x^2 - 3x$ и $x \geq 2$.

Для шестигранника состоящего из $k = 3n^2 - 3n$ точек существует *m – k+1 различных позиций в изображении.* В каждой из точек шестигранник может быть повернут на любой из 6 углов.
Число возможных состояний для шестигранников, состоящих из *k* точек:

$$6^{m-k+1}(m-k+1)!$$

т.к. состояние описывается не только углом поворота, но и порядком в котором поворачивалась шестигранники

Верхняя оценка количества перестановок для изображения

Так как *k* может быть различным и можно использовать любую комбинацию неодинаковых шестигранников (даже с одним центром), то всего комбинаций:

$$\prod_{i=2}^{x} 6^{m-3i^2+3i+1}(m-3i^2+3i+1)!\,,$$

где m – количество точек в изображении, x – максимальное целое удовлетворяющее условию: $m \geq 3x^2 - 3x$ и $x \geq 2$.

Нижняя оценка количества перестановок для изображения

Нижняя оценка может быть получена аналогичным образом, нужно сделать предположение, что шестигранник в каждой точке изображения должен быть повернут на угол отличный от 0, тогда количество перестановок:

$$\prod_{i=2}^{x} 5^{m-3i^2+3i+1}(m-3i^2+3i+1)!\,,$$

где m – количество точек в изображении, x – максимальное целое удовлетворяющее условию: $m \geq 3x^2 - 3x$ и $x \geq 2$.

Оценка количества изображений, которые можно получить из исходного

Пусть в битовом представлении изображения длиной ***y*** присутствует ***z*** нулей, тогда число различных изображений, которые можно получить из исходного изображения:

$$\frac{y!}{(y-z)!z!}$$

Подходы к реализации

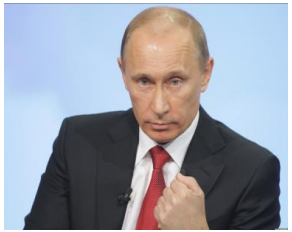
- Прямой, т.е. изображение представляется в виде матрицы, в ней выбираются элементы, образующие шестигранник, и затем осуществляется перестановка этих элементов в виде поворота шестигранника

- Прямой модифицированный. Изображение представляются в виде шестигранника, в котором выбираются элементы, образующие шестигранник, а затем осуществляется перестановка этих элементов в виде поворота шестигранника

- Изображение рассматривается в виде строки и осуществляется перестановка эквивалентная перестановке поворота шестигранника для подряд идущих элементов

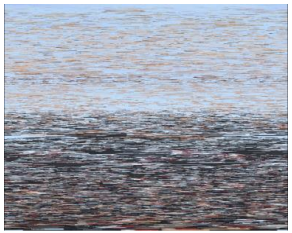
- Изображение рассматриваются в виде кольца и осуществляется перестановка эквивалентная перестановке поворота шестигранника для подряд идущих элементов

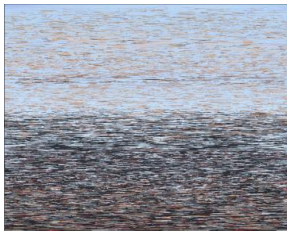
Результаты простейшего метода


а)


б)


в)


г)


д)

Для каждого варианта перемежения использовалось, соответственно, 50 (*б*), 100 (*в*), 200 (*г*) и 300 (*д*), шестигранников. Кроме этого, во всех вариантах перемежения угол поворота, начальная точка и размер шестигранника (из множества [2,199]) выбирались случайным образом.

Проблемы прямого применения описанного алгоритма

Прямое применение описанного алгоритма предполагает 2 этапа:

1) сложение изображения с гаммой;

2) перестановка элементов полученного изображения в соответствии с ключом.

При таком подходе, имея исходное и зашифрованное изображения возможен перебор двух частей ключа независимо.

Решение описанной проблемы

В качестве решения описанной проблемы предлагается использовать перестановку для искажения гаммы, а на основе полученной последовательности осуществить как перестановку исходного изображения так и его гаммирование.

Последовательность работы алгоритма выглядит следующим образом:

1) генерация псевдослучайной последовательности равной длине изображения;

2) перестановка элементов полученной на шаге (1) последовательности с использованием ключа;

3) сложение изображения с гаммой;

4) перестановка элементов полученного изображения с использованием гаммы.

СПАСИБО ЗА ВНИМАНИЕ!