УДК 004.91

Студ. Д. С. Ничипорчик
Науч. рук. доц. Д. В. Шиман
(кафедра информационных систем и технологий, БГТУ)

ОСАЖДЕНИЕ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ

Одной из важнейших задач современности является обеспечение надежности хранения и передачи данных. С каждым днем ответственность за передачу некорректной информации растет, при этом увеличивается количество способов несанкционированного доступа к информации. Данная работа ставит своей целью изучение современных методов шифрования данных.

Основная часть. Шифрование данных широко применяется для различных целей, главные из которых – обеспечение конфиденциальности, защищенности данных, передаваемых компаниями и частными пользователями. Данная научная работа является демонстрационной смесью шифрования и стеганографии. Для шифрования использовался RSA. [1] RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Весь алгоритм можно разбить на два блока действий: преобразования над текстом и преобразования над изображением.

В данном примере взято изображение размера 27 x 12 пикселей. Для большей наглядности будет использоваться строка “дом” и одно-тонное изображение (рисунок 1).

Преобразования над текстом: преобразования над текстом условно можно разбить на несколько последовательных действий: шифрование с использованием RSA и преобразование с использованием таблицы ASCII.

Шифрование с использованием RSA: после зашифровки мы получим следующую строку – 4d61340690daa130f08825ae42984eff, размер которой 32 символа.

Преобразование с использованием таблицы ASCII: на данном этапе мы уже имеем зашифрованную строку, размером 32 символа, наша задача перевести данный набор в символы, а после в шестнадцатеричное систему счисления, (для чего будет рассмотрено в преобразовании изображения). Рассмотрим на примере первого символа: 4 в таблице ASCII 52, в шестнадцатеричной системе счисления это 34, таким образом мы получили первое значение, которое будем использовать в «осаждении».

Конечным результат будем являться 34, 64, 36, 31, 33, 34, 30, 36, 39, 30, 64, 61, 61, 31, 33, 30, 66, 30, 38, 38, 32, 35, 61, 65, 34, 32, 39, 38, 34, 32, 39, 38, 34, 65, 66, 66.

Преобразования над изображением: Преобразования над текстом представляют собой несколько последовательных действий: разбиение изображение на условные квадраты 3x3 пикселя, разбиение этих квадратов на квадраты 1x1 пикселя, “осаждение” (помещение информации) пикселя в центре квадрата 3x3 пикселя, формирование финального изображения. Рассмотрим каждый шаг более подробно.

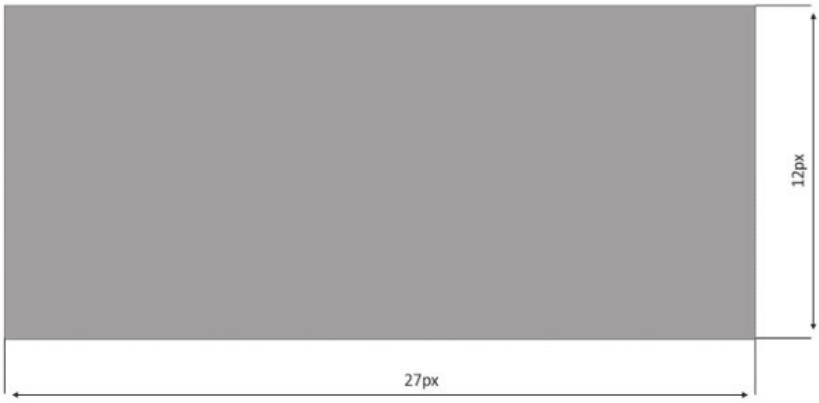

Рисунок 1 - Исходное изображение

В таблице 1 приведены соотношения популярных размеров и количество символов, которые можно поместить.

Таблица 1 - Соотношения размеров и количества символов

Разрешение	Количество символов
1366x768	116480
1600x900	159900
1920x1080	230400

Для произвольного размера количество символов, которые мы можем поместить в изображение мы рассчитываем по формуле (1).

$$l = (w mod\ 3) * (h\ mod\ 3) - 1, \quad (1)$$

где w – ширина изображения; h – высота изображения.

Разбиение изображения на условные квадраты размера 3x3 пикселя: Наш цикл проходит по всему изображению разбивая его на квадраты размером 3x3 пикселя, в данном примере их 36. Размер нашего ввода 32 символа, а это значит, что коллизия, связанная с нехваткой мест для “осаждения”, не возникнет (см. рис.2).

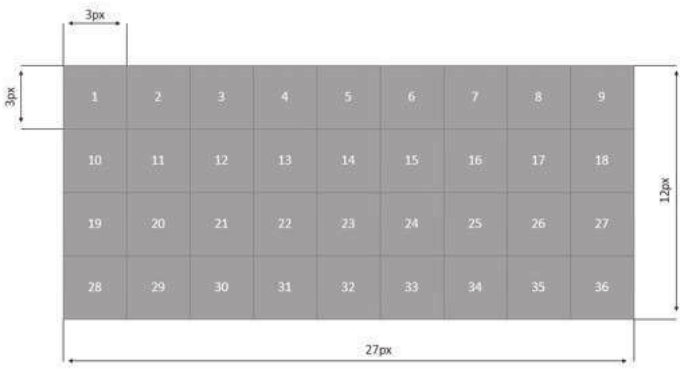

Рисунок 2 - Изображения, разбитое на квадраты 3x3

Разбиение каждого квадрата на квадраты размерами 1x1 пикселя: в данном шаге уже сформированные ячейки разбиваются на более маленькие, размерами 1x1пикселя, для будущего осаждения. Разбиение происходит слева направо. “Осаждение” пикселя в центре квадрата 3x3 пикселя: на данном этапе первым действием является проверка каждой ячейки на коллизию. Если ее размер не равен 9, то она пропускается, а если равен 9, то алгоритм действий следующий: вычисляется значения цвета каждой ячейки в HEX, а также среднее значения всех ячеек без центральной (пятой) ячейки. В данном примере значение цвета равно #5B9BD5, соответственно и среднее равно #5B9BD5. Теперь мы должны сложить первое среднее значение с 1 символом 34. Мы получим следующее значение: 5B9C09. Далее применим этот цвет к 1 ячейке.

Формирование финального изображения: на данном этапе мы имеем уже сформированное изображения, но встает вопрос, как же отличить модифицированные ячейки от исходных? Для этого используется следующий алгоритм: при проверке мы используем преобразованный в шестнадцатеричную систему счисления ключ, а именно сумму всех элементов.

Формирование стоп-символа: для формирования стоп-символа используется следующий алгоритм: мы берем закрытый ключ, производим те же преобразования, что над текстом, а после складываем сумму всех элементов. Рассмотрим формирование стоп-символа для данного примера: 5ad17cbe5d90df75c45e4ba1f16bfe69.

При преобразовании каждого символа с использованием таблицы ASII мы получим следующие значения: 53, 97, 100, 49, 55, 99, 98, 101, 53, 100, 57, 48, 100, 102, 55, 53, 99, 52, 53, 101, 52, 98, 97, 49, 102, 49, 54, 98, 102, 101, 54, 57. После этого требуется получить сумму всех чисел, в данном случае мы получим 2438. Это слишком много, поэтому мы должны поделить нацело на 256. Получим 134, после этого прибавим 256 для того, чтобы ключ не совпадал с текстом. Мы получим 390 и переведем число в шестнадцатеричную систему счисления,

получим 186. Цвет исходной ячейки 5B9BD5, прибавив 186 получим 5B9D5B (см. рис. 3).

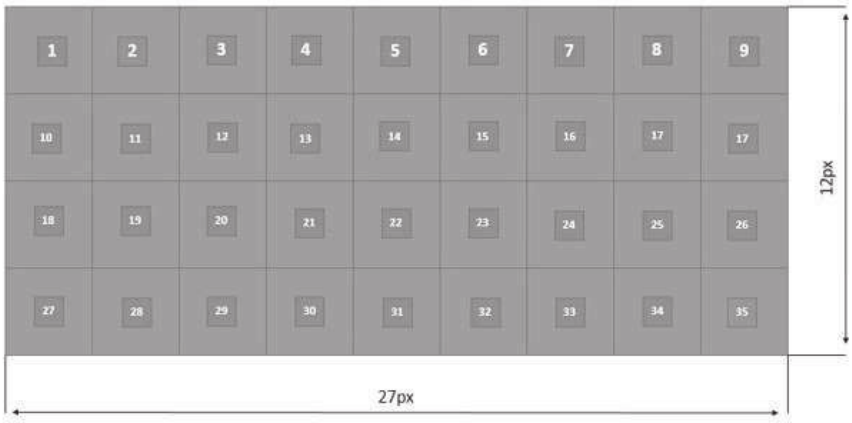

Рисунок 3 - Финальное изображение

Вывод: в данной научной работе рассмотрены варианты совместного использования “осаждения” и шифрования. Данный способ является очень полезным из-за своей универсальности, так как изображения присутствуют во всех сферах реальной жизни, что в свою очередь поможет скрыть факт шифрования данных в изображении.

ЛИТЕРАТУРА

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с

2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с, ил.

УДК 004.042

Студ. Э. В. Ральцевич
Науч. рук. канд. техн. наук Н. А. Жиляк
(кафедра информационных технологий БГТУ)

РАЗРАБОТКА ВЕБ-РЕСУРСА «RESOURCE PLAINNING SYSTEM»

Сегодня большинство компаний занимается предоставлением аутсорсинговых услуг. Продуктом, который продает такая компания, является человеческий ресурс. По этой причине руководители данных компаний нуждаются в программном средстве, которое позволяло бы отобразить информацию о сотрудниках, их занятости и времени, когда сотрудник освобождается. Проводя небольшое исследование, было обнаружено, что существующие приложения не расчитаны на то,