Результат построения поверхности заданной функцией $y = \sin(x^2+z^2)$ представлен на рис. 2.

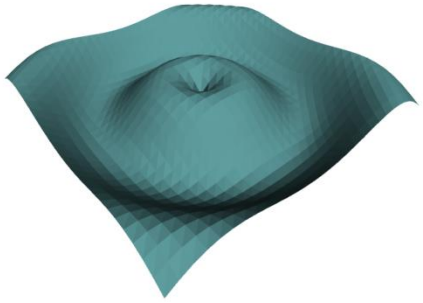

Рис. 2. Результат построения поверхности

Заключение

Данная программа будет полезна для математиков и студентов, так как может наглядно показать любую поверхность. Перспективой развития работы является возможность построения сложных 3D предметов, таких как детали механизмов, роботов, сложных биологических объектов.

Список литературы

1. Мэтью Мак-Дональд. WPF: Windows Presentation Foundation в .NET 3.5 с примерами на C# 2008 для профессионалов = Pro WPF in C# 2008: Windows Presentation Foundation with .NET 3.5. – 2-е изд. – М.: Вильямс, 2008. – С. 25.
2. Ильин В.А., Позняк Э.Г. Аналитическая геометрия. – М.: ФИЗМАТЛИТ, 2002. – 240 с.

УДК 004

АНАЛИЗ И РЕАЛИЗАЦИЯ АЛГОРИТМОВ СКРЫТИЯ ДАННЫХ В ИЗОБРАЖЕНИЯХ ФОРМАТА BMP

Чан ТхюиЗунг
Научный руководитель: Вичугова А.А., к.т.н., доцент кафедры АиКС

Национальный Исследовательский Томский политехнический университет,
634050, Россия, г. Томск, пр. Ленина, 30
E-mail: bluesky25792@gmail.com

The article describes the questions to hide data in image files BMP format. The idea of image processing algorithms and the result of the program implementation are presented

Key words: *BMP, CPTE algorithm, MCPTE algorithm, 24-bit*

Ключевые слова: *BMP, алгоритм CPTE, алгоритм MCPTE, 24-х битовых*

Введение

В современном быстро меняющемся мире эффективность работы с информацией является одним из важнейших факторов успеха. Защита конфиденциальной информации получила

особенную актуальность в связи с большим количеством атак на коммуникативные средства связи и на данные, хранимые на различных видах электронных носителей. Как правило, деятельность предприятия зависит от уровня развития ее информационных систем и технологий, а также методов и средств защиты информации. Именно поэтому вопрос о защите персональных данных имеет не меньшую значимость и актуальность, чем, например, план по стратегическому развитию предприятия. Существует два способа защиты информации: криптографический и стеганографический. Стеганография – это способ скрытой передачи информации путём сохранения в тайне самого факта передачи.[1] В рамках статьи мы будем исследовать способ стеганографии на примересокрытие данных в изображенияхформата BMP.

Теоретическая часть

BMP – это стандартный формат графических файлов Windows.Этот файл состоит из четырех частей:заголовка,информационного заголовка, таблицы цветов и данных изображения.Основной особенностью графических файлов формата BMP, в частности 24-х битовых изображений, является их способность скрывать внутри себя большие объемы дополнительной информации без особых потерь качества.

Для сокрытия информации в изображении BMP, будем использовать алгоритм CPTE. Предоставим бинарное изображение размером: m*n. В алгоритме используются 4 вида исходных данных: бинарная матрица F, бинарная ключевая матрица K, матрица весов W (значение элементов матрицы W принадлежат множеству {1,2,…,2r}, где r= log2(m*n)), и последовательность битов b, которые необходимо скрыть в матрице F. Важно отметить, что алгоритм CPTE нельзя использовать, если все элементы матрицы F одинаковые (равны 1 или 0).

Идея алгоритма:инвертируем значения битов матрицы F (1->0 или 0->1), количество инверсий не более 2 раз. Если S равно bmod 2(r+1) тогда инвертировать биты в матрице Fне нужно. В результате этого действия получим матрицу S’, значение которой увеличивается на α:

$$S' = S + \alpha = b \bmod 2(r+1),$$

где T= F (xor) K и r= [log2(m*n)], $S = \sum_{i=1}^{m} \sum_{j=1}^{n} T * W mod 2^{r+1}$.

В итоге матрица m*n может скрыть максимум [log2(mn)] битов с высокой безопасностью. Но при этом возникает задача улучшения качества изображения. Например, матрица F превратилась в F’ или F’’, как показано на рис. 1.

$$F = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & \boxed{0} & 0 & 0 & 0 \\ 1 & 0 & 0 & \boxed{0} & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad F' = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & \boxed{1} & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad F'' = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & \boxed{1} & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Рис. 1. матрица F превратилась в F’ или F”

Качество матрицы F’ выше, чем F’’, потому что в F’’ белый пиксел, значение которого равно 1, находится в окруженииичерных, равным 0. Для дальнейшего улучшения качества изображения следует использовать алгоритм MCPTE, основанного на вычислении расстояния между матрицами:

$$d(F)ij = \min \{\sqrt{(i-x)^2 + (j-y)^2}\}.$$

Кроме этого, необходимо отметить на вопрос «В каком изображение сохранилась информация?». Для этого, следуетудалить один бит в последовательности битов b. После этого качество изображения повысится.

Алгоритмы CPTE и MCPTE очень эффективны для 24-х битовыхизображений. Каждаяточка изображения содержит 24-бита (8 бит описывают красный цвет, 8 бит – зеленый и 8 бит – синий). Необходимо выбрать последний бит в каждой точке изображения. Для 24-х битового изображения будут выбраны 3 бита и получится битовую матрицу, изменение которой будет незаметно визуально, в отличие от 8-битового изображения.

Практическая часть

Вышеописанные теоретические положения были реализованы на практике в виде программного приложения «Скрытие информации в изображении формата BMP». Приложение разработано в среде MicrosoftVisualStudio 2012 на языке программирования C#. Результат сокрытия данных показан на рис. 2 и 3. Визуально оба изображения выглядят одинаково, однако изображение на рис. 3 содержит новую скрытую информацию.

Рис. 2. Исходное изображение 24-х

Рис. 3. Выходное изображение 24-х

Список литературы

1. Стеганография. Скрытие информации в изображениях [Электронный ресурс]. URL: http://xain.hackerdom.ru/zine/online/issue0/Steganography.html
2. BMP [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/BMP