

# СОКРЫТИЕ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИК СТЕГАНОГРАФИИ И МЕТОДОВ СЖАТИЯ

**Мифтахов Р.Р.**, старший оператор 4 научной роты ФГАУ «Военный инновационный технополис «ЭРА».

## **Аннотация**

В статье производится сравнение двух различных методов сокрытия информации в изображениях. В первом методе использовалась техника под названием «наименьший значащий бит» (НЗБ или LSB) без шифрования и сжатия. Во втором методе секретное сообщение сначала зашифровывается, а затем применяется техника НЗБ. Для сжатия изображения применяется дискретное косинусное преобразование (ДКП или DCT). Эффективность этих двух методов оценивается с помощью средней квадратичной ошибки (СКО) и отношения сигнал/шум (ОСШ).

**Ключевые слова:** стеганография, стегоизображение, сокрытие информации, наименьший значащий бит.

Стеганография - это наука и искусство тайного общения двух сторон, которые пытаются скрыть содержание передаваемых сообщений, это наука о встраивании информации в изображение без каких-либо видимых проявлений, также это искусство и технология написания сообщений таким образом, что никто, кроме отправителя и получателя, не подозревают о сокрытой информации в сообщении. В настоящее время эта наука привлекает огромное внимание, так как она позволяет не просто зашифровать сообщение или закодировать его, а скрыть сам факт его существования [1].

Базовая схема стеганографии показана на рис.1. Она содержит два файла: первый - это изображение, а второй - секретный файл, который будет скрыт закрытым ключом для шифрования. Как показано на рис.1, есть два шага: первый - сокрытие данных (техника встраивания), а другой - сжатие, чтобы уменьшить пространство и размер данных. Конечным результатом системы является стегоизображение, представляющее собой цифровое изображение, в котором есть скрытое сообщение. Затем это изображение отправляется получателю по общедоступному каналу связи (Интернет), где получатель, применяя набор правил для извлечения и секретный пароль, сможет получить сокрытые данные.



Рисунок 1. Базовая схема сокрытия данных

Техника НЗБ является одной из первых полезных техник кодирования в стеганографии [2,3]. Эта техника использует методы пространственного встраивания и внедряет секретные данные в изображение, в котором пиксели подвергаются наименьшим изменениям. Следовательно, человек почти не замечает этих незначительных изменений, поэтому вероятность раскрытия информации мала. Хотя эта техника кодирования и представляет собой простой инструмент, тем не менее, она имеет свои слабости. Шум, фильтрация, ограничение, пространственные преобразования цвета и повторная выборка - самые слабые стороны техники НЗБ (LSB). Кроме того, на этот подход могут влиять алгоритмы сжатия с потерями.

Математические функции ДКП применяются для преобразования данных цифрового изображения из пространственной области в частотную область. В ДКП после преобразования изображения в частотную область данные внедряются в младший бит среднечастотных компонентов и детализируются для сжатия с потерями. Коэффициенты техники ДКП используются для сжатия изображений формата JPEG [4]. ДКП делит изображение на части различной важности, а также может разделить изображение на компоненты высокой, средней и низкой частоты, в низкочастотном поддиапазоне, большая часть энергии сигнала находится на низкой частоте, которая содержит наиболее важные визуальные части изображения, в то время как в высокочастотном поддиапазоне компоненты изображения обычно удаляются с помощью сжатия и шумовых атак. Таким образом, секретное сообщение внедряется путем корректировки коэффициентов поддиапазона средней частоты, чтобы на видимость изображения это не влияло.

Криптография - это искусство кодирования передаваемых сообщений, с целью сделать их нечитаемыми, это процесс безопасной передачи данных через сеть с применением криптографических алгоритмов, так что злоумышленникам будет сложно получить скрытую информацию. В криптографии используются две основные процедуры: шифрование и дешифрование; Процедура шифрования - это процесс преобразования простого текста в зашифрованный текст, а процедура дешифрования - обратный процесс. Простой текст - это текст, который содержит исходное сообщение или данные, которые не зашифрованы, а зашифрованный текст - это текст, который готов к использованию после шифрования сообщения. Ключ необходим как для шифрования, так и для дешифрования данных или сообщений [5-6].

В данной статье применены несколько методов для сокрытия информации. С использованием сжатия ДКП [7-9] и шифрования с помощью криптографических алгоритмов данные встраиваются в изображение, после чего зашифрованное изображение передается через Интернет и с другой стороны выполняется обратный процесс с использованием закрытого ключа для извлечения данных. В предлагаемом алгоритме предполагается, что как отправитель, так и получатель имеют одинаковую систему закрытых ключей. Получатель отправляет открытый ключ отправителю по небезопасному каналу связи, затем отправитель генерирует стегоизображение с обоими ключами и отправляет их через другой незащищенный канал получателю, который может извлечь секретный файл.

Алгоритм встраивания секретной информации, который на вход принимает изображение, секретный файл и ключ, может быть описан следующим образом:

- считать изображение;
- считать секретный ключ;
- считать секретный файл и преобразовать его в двоичный формат;
- разделить изображение на блоки по 8 на 8 пикселей;
- применить технику ДКП для каждого блока;
- выполнить сжатие для каждого блока и квантование коэффициентов ДКП в соответствии таблицей коэффициентов квантования;
- определить НЗБ для каждого коэффициента ДКП и заменить НЗБ данными секретного файла;
- записать стегоизображение;
- рассчитать среднеквадратичную ошибку и отношение сигнал / шум для полученного изображения.

Алгоритм извлечения секретной информации, который на вход принимает зашифрованное изображение, выглядит так:

- считать стегоизображение;
- преобразовать его в двоичный вид;

- получить коэффициенты горизонтальной и вертикальной фильтрации для алгоритма ДКП;
- разбить изображение на блоки по 8 на 8 пикселей;
- применить ДКП для каждого блока и получить стегоизображение до сжатия;
- прочесть секретный ключ;
- вычислить коэффициенты горизонтальной и вертикальной фильтрации изображения и определить НЗБ для каждого из них;
- извлечь секретную информацию.

Цель проведения эксперимента в данной статье состояла в том, чтобы скрыть как можно больше данных с наименьшей заметной разницей в изображении. В качестве методов оценки использовались средняя квадратическая ошибка и отношение сигнал/шум.

Среднеквадратическая ошибка - степень, используемая для количественной оценки изменения между начальным и зашумленным изображениями. Формула, по которой она вычисляется выглядит так:

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{n-1} \sum_{j=0}^{n-1} (o(i, j) - s(i, j))^2 + (2n + m) \quad (1)$$

где  $s$  - стегоизображение;  $o$  - оригинальное изображение;  $m, n$  - размеры изображения.

Отношение сигнал/шум позволяет узнать качество стегоизображения после встраивания в оригинальное секретной информации. Вычисляется так:

$$PSNR = 10 \log_{10} \frac{256^2}{MSE} \quad (2)$$

В рамках проведения эксперимента были использованы некоторые случайно выбранные изображения. С помощью алгоритма встраивания выполнено сокрытие секретной информации и с помощью средств оценки вычислены степень искажения изображения после работы алгоритма.

Согласно результатам проведенных экспериментов (табл.1) можно сделать вывод, что способность встраивания секретной информации в предложенном алгоритме хорошая. Вычисленные отношение сигнал/шум и средняя квадратическая ошибка показывают, что качество изображения остается высоким после встраивания и имеет больший уровень безопасности при использовании техник НЗБ и ДКП вместе, нежели использование техники НЗБ отдельно. Также использование двух техник одновременно позволяет получать наименьшие искажения в изображении и, как следствие, большую безопасность в сокрытии данных.

Таблица 1. СКО и ОСШ для изображений

Изображение	Техника НЗБ		Техника ДКП	
	ОСШ, дБ	СКО, дБ	ОСШ, дБ	СКО, дБ

car.jpg	49,833	1,312	58,786	0,854
tree.jpg	48,985	1,381	55,689	0,867
girl.jpg	48,921	1,411	59,157	0,954
lion.jpg	49,521	1,347	52,263	0,789
desert.jpg	49,563	1,315	54,483	0,823

Таким образом, в данной статье производится сравнение двух разных методов скрытия информации в изображениях. В первом методе используется только техника получения наименьшего значащего бита, а во втором эта же техника, но с предварительным шифрованием и дискретно косинусным преобразованием. Согласно полученным результатам стало ясно, что можно скрыть секретную информацию в изображении, а также сжать его, что позволяет скрыть сам факт присутствия посторонних данных и, как следствие, передавать данные по сети более безопасно. Эффективность двух методик оценивается с помощью средней квадратичной ошибки и отношения сигнал/шум. Использование техник НЗБ и ДКП позволяет эффективно снизить объем файла, что позволяет передавать его быстрее по медленным интернет соединениям или просто занимать меньше места на диске. Проведенное исследование позволяет улучшить стандартный алгоритм сокрытия данных и при этом сохранить его изначальные критерии восприимчивости и устойчивости.

### **Литература**

1. Алаа Вахаб, Романенко Д.М. Методы цифровой стеганографии на основе модификации цветовых параметров изображения // Труды БГТУ. Серия 3: Физико-математические науки и информатика. 2018. №1 (206).
2. Kelash HM, Osama F AbdelWahab, Elshakankiry OA. Hiding Data in Video Sequences Using Steganography Algorithms. ICT International Conference, IEEE. Jeju Island, Korea. 2013: 353-358.
3. Назаренко Ю.Л. Стегоанализ метода сокрытия информации в изображении замены наименьшего значащего бита (LSB) // European science. 2018. №3 (35).
4. M. Iwata, K. Miyake, A. Shiozaki. Digital Steganography Utilizing Features of JPEG Images. IEICE Trans. Fundamentals. 2004; E87-A (4): 929–936.
5. P Venkateswaran, Souvik Roy. Online Payment System using Steganography and Visual Cryptography. Conference on Electrical, Electronics and Computer Science, IEEE. Bhopal, India. 2014: 101-115.
6. AOZCERIT, OCETIIN. A new for Color Images, Proceedings of International Steganography Algorithm Based on Color Histograms for Data Embedding into Raw Video Streams. Elsevier Ltd, Computers & Security.Turkey. 2009; 28: 670-682.

7. Сидякин И. М., Павлов Ю. Н. Исследование сжатия телеметрической информации без потерь на основе дискретного косинусного преобразования // Машиностроение и компьютерные технологии. 2006. №8.

8. Suchitra B, Priya M, Raju J. Image steganography based on DCT algorithm for data hiding. Int J Adv Res Comput Eng Technol. 2013; 2(11): 3003–3006.

9. В.В. Ключеня Структурные решения процессоров дискретного косинусного преобразования для встраиваемых систем мультимедиа реального времени // Доклады БГУИР. 2009. №6 (44).