УДК 681.3.04

О.А. Нистюк, ст. преп. (БГТУ, г. Минск)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ЦИФРОВОЙ СТЕГАНОГРАФИИ НА ОСНОВЕ ИЗМЕНЕНИЯ ПИКСЕЛЕЙ КОНТЕЙНЕРА

Цифровая стеганография, являясь частью классической стеганографии, направлена на скрытие информации внутри цифровых объектов, таких как изображения, аудио, видео и текст. В основе цифровой стеганографии лежит идея, что внутри стандартного цифрового файла можно разместить дополнительные данные, при этом такие изменения не должны быть заметны для обычного пользователя. Данный подход становится особенно актуальным в условиях информационной безопасности и защиты конфиденциальных данных.

Рассмотрены важные особенности методов стеганографии, параметр для сравнения качества изображения отношение сигнала к шуму по методу пикового отношения, а также особенности встраивания информации в контейнер. При сравнении методов необходимо учитывать размер внедряемого сообщения, пропускную способность контейнера и его разрешение.

Существующие на сегодняшний день методы защиты текстовой информации не могут полностью гарантировать полное сокрытие сообщения в носителе. Процесс размещения тайного сообщения подразумевает изменение некоторых параметров контейнера.

При работе с пикселями необходимо владеть таким понятием, как «пропорция». Пропорция – это связь между шириной и высотой изображений. Обычно она выражается в виде двух чисел, таких как 3:2, 4:3 или 16:9. Ширина всегда является первым числом. Например, соотношение 16:9 может быть 1600 пикселей в ширину и 900 пикселей в высоту. Соответственно, получаем 1 440 000 пикселей изображения, что говорит о высокой пропускной способности.

Сравнительный анализ методов проводился по следующим параметрам:

– скорость внедрения тайного сообщения в контейнер;

– скорость извлечения сообщения;

– влияние размера сообщения на качество стегоконтейнера;

– отношение сигнала к шуму;

– оценка визуального качества.

Алгоритмы PM1 и LSB используют изменение битовых значений пикселей для сокрытия информации в изображении. Алгоритм PM1 достигает этого путем увеличения или уменьшения значения каждого

пикселя на единицу, в зависимости от значения соответствующего бита секретного сообщения (если бит равен 1, значение пикселя увеличивается на 1, если бит равен 0, значение пикселя уменьшается на 1).

LSB работает путем изменения наименее значимого бита каждого пикселя в изображении для кодирования секретного сообщения.

В качестве контейнера для сокрытия информации (стегоконтейнера) используются цветные растровые изображения в формате BMP с глубиной цвета 24 бита. Это означает, что каждая точка изображения (пиксель) представлена тремя байтами (24 бита), которые определяют интенсивность красного, зеленого и синего цветов.

Различные разрешения изображений позволяют оценить эффективность и надежность алгоритмов стеганографии при работе с изображениями разного размера. В экспериментах в качестве стегоконтейнеров были использованы цветные растровые изображения формата BMP и разрешением 512x512, 1024x1024 и 2048x2048 пикселей.

В контейнер были встроены сообщения различного размера с использованием методов стеганографии PM1 и LSB.

Для анализа скорости внедрения и извлечения информации из контейнера было проведено 20 измерений на изображение с разрешением 512x512 и объемом сообщения 100 байт (80 символов), 20 – на изображение с разрешением 512x512 и объемом сообщения 1 килобайт (1000 символов). С последующими разрешениями контейнера проведены аналогичные эксперименты.

Были проведены эксперименты скорости внедрения и извлечения информации из контейнера для методов стеганографии PM1 и LSB на изображениях с разрешениями (512x512, 1024x1024 и 2048x2048) и двумя разными объемами тайного сообщения (100 байт и 1 килобайт).

Результаты замеров обработаны и представлены в сводной таблице, которая содержит средние значения времени внедрения и извлечения информации для каждого метода и каждого варианта разрешения и объема сообщения. Это позволяет сравнить производительность методов стеганографии PM1 и LSB и оценить влияние разрешения и объема сообщения на скорость внедрения и извлечения информации.

На основе результатов проведенных исследований можно сделать вывод, что метод PM1 требует больше времени для внедрения и извлечения тайного сообщения из контейнера, чем метод LSB. В среднем, метод PM1 занимает на 10-15% больше времени, чем метод LSB, в зависимости от разрешения изображения и размера внедряемого сообщения. Это означает, что метод LSB является более быстрым и эффективным для внедрения и извлечения тайного сообщения.

Другим важным параметром для сравнения качества изображения является отношение сигнала к шуму по методу пикового отношения (PSNR). Этот параметр позволяет оценить степень искажения изображения после внедрения тайного сообщения и сравнить качество с исходным изображением.

PSNR является мерой отношения между максимально возможной мощностью сигнала и мощностью шума в изображении. Чем выше значение PSNR, тем меньше искажений в изображении и тем лучше его качество. Сравнение значений PSNR для изображений, полученных с помощью методов PM1 и LSB, позволяет оценить, какой из методов лучше сохраняет качество изображения после внедрения тайного сообщения.

Таблица содержит значения PSNR для каждого изображения, что позволяет оценить качество изображений после внедрения информации. Чем выше значение PSNR, тем меньше искажений и лучше качество изображения.

Таблица 1 – Оценка качества изображений

Метод	Разрешение	Размер сообщения	PSNR, дБ
PM1	512x512	100 байт	59.34
PM1	1024x1024	100 байт	58.21
PM1	2048x2048	100 байт	57.54
PM1	512x512	1 КБ	44.01
PM1	1024x1024	1 КБ	43.12
PM1	2048x2048	1 КБ	42.31
LSB	512x512	100 байт	59.34
LSB	1024x1024	100 байт	58.21
LSB	2048x2048	100 байт	57.54
LSB	512x512	1 КБ	44.01
LSB	1024x1024	1 КБ	43.12
LSB	2048x2048	1 КБ	42.31

На основе произведенных замеров можно сделать вывод, что оба метода стеганографии одинаково справляются со своей задачей по внедрению информации в изображение. Результаты показывают, что оба метода имеют примерно одинаковое качество изображения после внедрения информации, о чем свидетельствуют значения PSNR и SSIM.

При выборе метода стеганографии, необходимо учитывать не только эффективность метода, но и объем сообщения, которое необходимо внедрить, чтобы обеспечить оптимальное качество изображения.

Анализ методов стеганографии показал, что оба метода, PM1 и LSB, могут быть эффективными для внедрения информации в изображения. Однако, результаты показали, что метод LSB имеет некоторые

преимущества над методом PM1.

Во-первых, метод LSB показал лучшее качество изображения после внедрения информации, чем метод PM1. Это было подтверждено значениями PSNR и SSIM, которые были выше для метода LSB.

Во-вторых, анализ показал, что метод LSB более устойчив к искажениям изображения, чем метод PM1.

В-третьих, анализ показал, что метод LSB более эффективен для внедрения информации в изображения с высоким уровнем детализации, чем метод PM1.

В целом, результаты показали, что метод LSB является более эффективным и надежным методом стеганографии для внедрения информации в изображения, чем метод PM1. Однако, необходимо отметить, что выбор метода стеганографии зависит от конкретных требований и ограничений приложения.

ЛИТЕРАТУРА

1. Brassil J., Low S., Maxemchuk N.F., O'Gorman L., Electronic Marking and Identification Techniques to Discourage Document Copying, IEEE Journal on Sel. Areas in Commun., 13 (1995), nr. 8, 1495–1504.

2. Shutko, N. The use of aprosh and kerning in text steganography / N. Shutko // PrzeglądElektrotechniczny. – 2016. – № 10. – p. 222-225.

3. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

УДК 003.26

А.Н. Николайчук, асп.; П.П. Урбанович, проф.
(БГТУ, г. Минск)

ИСПОЛЬЗОВАНИЕ ПОЛЕЙ ЗАГОЛОВКА ПРОТОКОЛА IP ДЛЯ СОЗДАНИЯ СКРЫТОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ

Для передачи информации через Internet на хостах используется набор протоколов, соответствующий модели TCP/IP, которая разделена на четыре уровня (прикладной, транспортный, сетевой, канальный). Одним из самых важных протоколов этого стека является IP (Internet Protocol), который выполняет две основные функции – адресацию и фрагментацию/сборку дейтаграмм [1].

Согласно протоколу, сообщение формируется в пакет, наделенный служебной информацией – заголовком (рис. 1). Заголовок разбит на несколько полей: двенадцать обязательных и два необязательных,