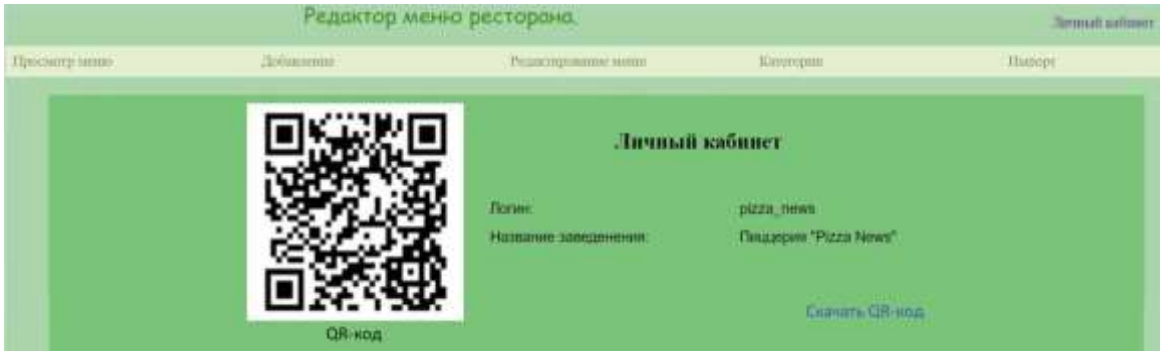

Рис. 5. Форма системы «Личный кабинет»

Использование данной системы облегчает работу сотрудникам ресторана, решает проблему с бумажным меню и предоставляет мгновенный доступ к меню для гостей заведения.

Литература

1. Архитектура «Клиент-Сервер» [Электронный ресурс]. URL: https://itelon.ru/blog/arkhitektura-klient-server/ (дата обращения: 05.04.2022).

А.А. Пашин, М.А. Кудрина

ИССЛЕДОВАНИЕ МЕТОДОВ СТЕГАНОГРАФИИ ИЗОБРАЖЕНИЙ

(Самарский университет)

Введение

Стеганография – это наука, о способе тайной передачи сообщения, т.е. исходный текст остаётся неизменным, а прячется само письмо или его содержимое. Развитие вычислительной техники и новых каналов передачи информации привело к рождению новых методов сокрытия информации, в основе которых лежит особенность представления информации в файлах компьютера, вычислительных сетях и т.п. Целью стеганографии является скрытие факта существования секретного сообщения [1].

Методы стеганографии для изображений

Метод наименьшего значащего бита или Least Significant Bit (LSB). В 24-битном формате RGB изображения на каждый пиксел приходится 3 байта информации (1 байт для красного спектра, 1 для зеленого и 1 для синего соответственно). Младшие биты пикселов не несут в себе значимую информацию, поэтому в основу данного метода входит их замена на биты скрываемого текста.

Популярность данного метода обусловлена его простотой и объемом скрываемых данных (в картинку размером 800x600 пикселов незаметно для человеческого глаза можно записать данные объемом до 360 КБ [2]). Основной недостаток — высокая чувствительность к малейшим искажениям контейнера.

Разность значений пикселов или Pixel Value Difference (PVD). Метод основан на межпиксельной зависимости. В простейшем случае вычисляется разность между значениями соседних пикселов и принимается решение о ее изменении в зависимости от бита встраиваемой информации [3].

Для сокрытия бита сообщения вычисляется разность между интенсивностями цветов соседних пикселов. Если остаток после деления разности на 2 не равен скрываемому биту, то происходит корректировка интенсивности второго пиксела в паре на один пункт.

Извлечение секретного сообщения заключается в нахождении остатка после деления разности значений пикселов на 2.

Данный метод наследует все достоинства и недостатки от предыдущего, однако, позволяет скрывать примерно в 6 раз меньше данных.

Дискретное косинусное преобразование (ДКП). Одна из идей стеганографии состоит в том, что скрытое сообщение маскируют заменой несущественных параметров изображения, но в формате JPEG в процессе сжатия возможно изменение или даже удаление таких параметров, что приводит к частичному или, что более вероятно, к полному уничтожению встроенной в изображение информации. Более стойкими к компрессии, являются методы, основанные на ДКП, алгоритм которого является базовым в стандарте JPEG.

Чтобы зашифровать данные необходимо разложить изображение RGB по составляющим цветам, разделить матрицы интенсивности каждого цвета на блоки 8x8 пикселов, выполнить ДКП для каждого блока с целью получения матриц коэффициентов 8x8.

Математическая формула данного преобразования:

$$\mathrm{p}(x,y) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} C(u)C(v)S(u,v)\cos\left[\frac{(2x+1)\pi u}{2N}\right]\cos\left[\frac{(2y+1)\pi v}{2N}\right],$$

где $p(x,y)$ – текущий пиксел с координатами $[x, y]$;

x, y – координаты пиксела на изображении;

N – размерность преобразуемой матрицы;

u, v – координаты коэффициентов ДКП в матрице;

$C(u)$, $C(v)$ – коэффициенты, зависящие от координат матрицы (формула нахождения показана ниже);

$S(u,v)$ – значение байта пиксела с координатами $[u, v]$.

$$\mathrm{C}(f) = \begin{cases} \frac{1}{\sqrt{2}}, f = 0 \\ 1, f > 0 \end{cases},$$

где f принимает значение u или v [4].

Полученные коэффициенты представляют частотную область изображения, где в левом верхнем углу матрицы находятся низкие частоты (НЧ), отвечающие за наиболее важную информацию, в правом нижнем – высокие (ВЧ), определяющие мелкие детали изображения. Для минимальной заметности рекомендуется встраивать информацию в среднечастотную область (СЧ).

В каждый такой блок (рисунок 1) возможно встроить 1 бит секретной информации для чего необходимо выбрать пару коэффициентов и произвести встраивание. Встраивание информации осуществляется таким образом: для передачи бита «0» необходимо, чтобы разница пары коэффициентов ДКП превышала некоторую положительную величину, а для передачи бита «1» эта разница не должна превышать некоторую отрицательную величину.

После манипуляций с матрицей коэффициентов ДКП необходимо выполнить обратное дискретное косинусное преобразование, после которого сообщение будет считаться встроенным в изображение.

Рис. 1. Пример матрицы 8x8 коэффициентов ДКП

Для извлечения данных из картинки необходимо выполнить все шаги в обратном порядке.

Достоинством данного метода является устойчивость к сжатию. Недостатком – низкий объем скрываемых данных (в картинку размером 800x600 пикселов можно записать данные объемом приблизительно 937 Байт).

Исследования

Визуальный осмотр. Исследование проводилось на картинках, изображенных на рисунках 2а и 3а. Алгоритм LSB при встраивании до 2 бит в каждый байт картинки не дает никаких искажений исходного изображения (рисунок 2б). Однако, если попытаться встроить большее количество данных (например, используя 6 бит), то, вероятно, картинка будет испорчена (рисунок 2в). При встраивании информации методом ДКП в область ВЧ/СЧ можно получить отличный результат (рисунок 3б), что нельзя сказать при встраивании в НЧ изображения (рисунок 3в). Метод PVD не обладает возможностью испортить картинку из-за его принципа работы.

а) исходное изображение (контейнер) б) заполненный контейнер (2 бита на байт) в) заполненный контейнер (6 бит на байт)

Рис. 2. Влияние количества встраиваемой информации на качество изображения-контейнера (метод LSB)

а) исходное изображение (контейнер) б) заполненный контейнер (в ВЧ/СЧ) в) заполненный контейнер (в НЧ)

Рис. 3. Влияние выбора частотной области изображения для встраивания (метод ДКП)

Расслоение изображения. Исследование расслоением основано на получении среза изображения по порядковому номеру бита в значении пиксела. Если срезать изображение по нулевому биту, то получим наименьший значащий слой изображения. Если срезать по седьмому, то получим наиболее значащий слой изображения. На рисунке 4 изображен пример расслоения картинки, заполненной на треть при помощи метода LSB.

На 0 и 1 слое видна высокая плотность данных, что не свойственно обычным картинкам. Аналогичный результат можно получить для метода PVD (рисунок 5), что подтверждает их низкую устойчивость к данному виду воздействия на изображение. Факт наличия зашифрованной информации методом ДКП нельзя раскрыть при помощи расслоения.

Рис. 4. Расслоение контейнера, заполненного методом LSB

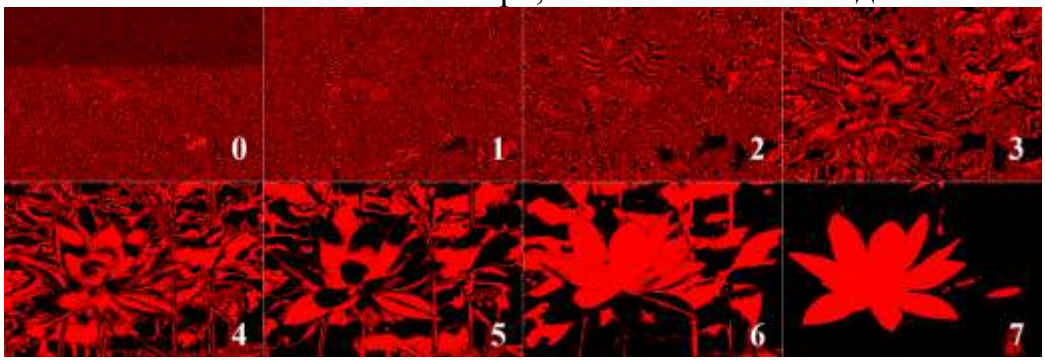

Рис. 5. Расслоение контейнера, заполненного методом PVD

Устойчивость к сжатию. Данное исследование заключается в проверке устойчивости рассмотренных методов стеганографии к компрессии. После сжа-

тия выполнена попытка извлечения данных из картинок. В качестве сообщения использована простая фраза: «Привет».

После попыток извлечения информации из сжатых изображений получились следующие результаты.

Метод LSB: «ѽBp_C$=…».

Метод PVD: «r2;Sf*6æ3…».

Метод ДКП: «Привет».

Итоги исследований

Исходя из полученных результатов наиболее надежным можно считать метод ДКП, так как он обладает устойчивостью к компрессии. Для домашнего использования фаворитом является метод LSB из-за объемов скрываемой информации и простоты реализации.

Литература

1. Методы компьютерной стеганографии [Электронный ресурс]. – URL: http://www.vsavm.by/knigi/kniga3/1740.html.

2. Сейеди, С.А. Сравнение методов стеганографии в изображениях [Текст] / С.А. Сейеди, Р.Х. Садыхов // Информатика. – 2013. – №1. – С. 66-75.

3. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика [Текст] / Г.Ф. Конахович, А.Ю. Пузыренко. – М.: МК-Пресс, 2006. – 288 с.

4. Белим, С.В. Стеганоанализ алгоритма Коха-Жао [Текст] / С.В. Белим, Д.Э. Вильховский // Математические структуры и моделирование. – 2018. – Вып. 4. – С. 113-119.

Р.Ф. Сагитов, И.А. Лёзин

ИССЛЕДОВАНИЕ СПОСОБОВ ОРГАНИЗАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ЗВУКОВОЙ ФИЛЬТРАЦИИ

(Самарский университет)

Задача распознавания

Фильтрация аудиопотока представляет собой отделение в смешанном потоке одних источников звука от других на базе некоторого множества критериев и преобразование в выходной поток тех звуков, сохранение которых требует исходная задача. Иными словами, в основе стоит задача классификации.

Для нейронной сети фактические критерии отображаются уже множеством признаков, именно обучившись определять признаки, сеть сможет выполнить корректную классификацию [1], в конечном итоге – операции по определению требуемых источников звука.

Главными элементами всех форм представления данных выступают признаки, которые являются наблюдаемыми свойствами объекта. Векторы имеют плоскую и простую структуру и обычно, в большинстве приложений для ма-