ВЫЯВЛЕНИЕ ПРИЗНАКОВ СТЕНОГРАФИЧЕСКОГО ВЛОЖЕНИЯ МЕТОДОМ БИНАРНОЙ ВЕРСТКИ

В.С. Толмачев, А.В.Пятков

Научный руководитель И.В. Горбунов, с.н.с. каф. КИБЭВС

г. Томск, ТУСУР

Проект ГПО КИБЭВС- 1519 – Моделирование системы защиты информации

Постановка задачи

Задача защиты информации от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени проблем [1]. С появлением интернета и широким применением цифровых средств массовой информации эти темы стали особенно актуальны для людей, заинтересованных в тайном общении, а также для защиты своих цифровых произведений от несанкционированного копирования. Значительных успехов в этой области удалось добиться, применяя современные криптографические методы. Однако, такие методы не позволяют скрыть сам факт наличия или передачи информации. Решить эти проблемы позволяют стеганографические методы защиты информации.

Средства стеганографии могут использоваться как в законных, так и в уголовных целях, поэтому активно развиваются соответствующие методы противодействия, например, стеганоанализ. Он предназначен для обнаружения факта сокрытия информации внутри цифровых файлов. Это есть пассивная атака на стеганографические системы, не изменяющая содержание сообщения. Стеганоанализ выделяют как самостоятельное научное направление, цель которого выявление в носителе (контейнере) факта наличия скрытых данных и оценка объема этих данных [2].

Цель данной работы заключается в описании модификации алгоритма атака хи-квадрат [3], который позволяет обнаружить признаки наличия стеганографического вложения в изображении.

Модифицированный алгоритм, называемый в дальнейшем алгоритм бинарной верстки, основан на вероятностных методах стеганоанализа. Его идея заключается в сравнении теоретического распределения наименее значимых бит изображения с фактическим распределением этих же бит. Распределение младших бит изображения не является случайным. Для незаполненных BMP и JPEG изображений не характерно, чтобы значения частот всех компонентов находились достаточно близко. При встраивании информации данные частоты сближаются или становятся равными. Мера сходства теоретического и

фактического распределения является мерой достоверности встраивания скрытой информации.

Описание алгоритма

В данной работе будет описан общий принцип работы алгоритма бинарной верстки, основанного на статистическом критерии Хи-квадрат. Он является универсальным, то есть подходит для анализа изображений, созданных различными методами скрытия. Автором оригинального алгоритма является И.В. Швидченко [3]. В работе [5] автор предложил «блочный» вариант алгоритма, который позволяет выявлять наличие информации, скрытой псевдослучайным образом. Ниже представлен модифицированная версия алгоритма.

Подробное описание алгоритма:

1) Разбиение изображения на цветовые компоненты (RGB).

2) Разбиение каждой цветовой компоненты изображения на блоки достаточной длины, которые могут как пересекаться, так и не пересекаться.

3) Для каждого блока находится значение эмпирического распределения.

4) Для каждого блока находится теоретическое значение распределения на основе эмпирического. Для этого необходимо найти среднее арифметическое количества пикселей с соседними яркостями. Согласно определению, данному в [4], под соседними яркостями понимают два цвета (R1, G1, B1) и (R2, G2, B2), если для них справедливо следующее соотношение:

$$\begin{cases} R_1 - R_2| \le 1 \\ G_1 - G_2| \le 1 \\ B_1 - B_2| \le 1 \end{cases} \leftrightarrow (R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2 \le 3$$

5) Для каждого блока необходимо оценить схожесть значений теоретического и эмпирического распределения с помощью статистики Хи квадрат применяя критерий Пирсона. Если теоретическое и эмпирическое распределение различаются несущественно, то вероятно, что в пиксель цветовой компоненты исследуемого блока встроена скрытая информация. Вычисляем значение статистики для проверяемого блока цветовой компоненты:

$$\chi^2_{emp} = \sum_{i=1}^{N} \frac{(a_i - A_i)^2}{A_i},$$

где A_i – Значение теоретического распределение для проверяемого блока;

a_i – Значение эмпирического распределение для проверяемого блока.

Если полученное эмпирическое значение статистики Хи-квадрат меньше теоретического значения статистики Хи-квадрат при заданном уровне значимости γ и количестве степеней свободы $k - 1$, то обнаружено встраивание в проверяемый блок.

$$\chi^2_{emp} < \chi^2_\gamma(k-1)$$

Второй шаг алгоритма необходим для того, чтобы наиболее точно определить наличие вложений. При последовательной записи в наименее значимые биты изображения метод обеспечивает хорошие результаты, а при псевдослучайном выборе младших бит и рассеивании сообщения по всей длине контейнера алгоритм срабатывает не всегда.

Заключение

Рассмотренный в данной статье метод дает возможность аналитику с определенной вероятностью судить о том, встроено ли в изображение стеговложение.

На результат работы алгоритма влияет несколько факторов: размер изображения, степень заполнения изображения, алгоритм стеганографического преобразования. Если выбирается изображение сравнительно небольшого размера, то вероятность ложного обнаружения возрастает, и наоборот, при увеличении размера изображения вероятность ложных обнаружений падает. Данный метод позволяет делать выводы о наличии скрытой информации при значительном заполнении изображения. При скрытии небольшого объема информации, этот алгоритм низко эффективен.

Литература

1. Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века/ Барсуков В. С., Романцов А. П. // Специальная техника. 1998. N.4–5. URL: http://st.ess.ru/.

2. Исследование методов интеллектуального стеганографического сокрытия данных в изображениях до и после их изменения / В. В. Полиновский, В. Ю. Королев, В. М. Малкина, М. И. Огурцов, В. А. Герасименко // Управляющие системы и машины. - 2014. - № 4. - С. 84-92.

3. Методы стеганоанализа для графических файлов / И. В. Швидченко // Искусств. интеллект. - 2010. - № 4. - С. 697-705.

4. Johnson, N.F. Exploring Steganography: Seeing the Unseen / N.F. Johnson, S.Jajodia // IEEE Computer. — 1998. — Vol. 31, No. 2. — PP. 26−34.

5. Дрюченко М.А. Алгоритмы выявления стеганографического скрытия информации в jpeg-файлах / М.А. Дрюченко // Вест. Воронеж. гос. ун. Системный анализ и информационные технологии. – 2007. – № 1. – С. 21-30.