ПРАКТИЧЕСКИЙ АНАЛИЗ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ PATCHWORK И КОХА ДЛЯ РЕАЛИЗАЦИИ СИСТЕМЫ ВОДЯНЫХ ЗНАКОВ

Ждан В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ярмолик В.Н. – д.т.н.,профессор

В работе рассматриваются угрозы интеллектуальной собственности, а также способы защиты от них. Особое внимание уделяется системам цифровых водяных знаков, в частности использованию стеганографических алгоритмов patchwork и коха в рамках их применения для реализации системы водяных знаков.

Для программного обеспечения и других объектов интеллектуальной собственности актуальными являются следующие угрозы: несанкционированное использование, обратное проектирование и несанкционированная модификация.

Одно из направлений для ликвидации данных угроз – системы цифровых водяных знаков. Данное направление использует различные методы: графическая стеганография, текстовая стеганография, обфускация и другие.

Алгоритм Patchwork является одним из базовых алгоритмов графической стеганографии. В его основе лежит статистический подход. Суть этого алгоритма состоит в следующем. При помощи

криптостойкого генератора псевдослучайных чисел, используя заранее известный секретный ключ, выбираются два пикселя изображения. Затем значение яркости одного из них увеличивается или уменьшается на некоторое значечие в зависимости от типа встраиваемой информации. Значение яркости второго – уменьшается или увеличивается на ту же величину соответственно. Процесс повторяется около 10000 раз. Значение приращения варьируется от 1 до 5 [1].

Пусть значения яркостей пикселов, выбираемых на каждом шаге, равны a_i и b_i, а величина приращения – δ. Тогда сумма разностей значений пикселов после преобразований:

$$S_n = \sum_{i=1}^{n}\left[\left(a_i \pm \delta\right) - \left(b_i \quad \delta\right)\right] = \pm 2\delta\, n + \sum_{i=1}^{n}\left(a_i - b_i\right).$$

Математическое ожидание величины $\sum_{i=1}^{n}\left(a_i - b_i\right)$, то есть суммы разности значений пикселов в незаполненном контейнере равно нулю, и его значение в неизмененном изображении будет много меньше чем n. Математическое ожидание величины S_n в заполненном контейнере будет равно $\pm 2\delta\, n$, а вычисленное значение S_n будет иметь большой соответствующий n порядок. В стегодекодере, используя ключ, проверяется значение S_n. Значении встроенного бита выбирается в зависимости от знака S_n. При положительной разности 1, а при отрицательной – 0 [2].

Таким образом, владелец может доказать свои интеллектуальные права, предъявив секретный ключ, который использовался для выборки изменяемых пикселов изображения.

В ходе реализации алгоритма Patchwork был разработан класс PatchworkInjector.

Данный класс реализует алгоритм Patchwork внедрения ЦВЗ в изображение. Для его использования пользователю необходимо ввести секретный ключ и строку, которая служит водяным знаком. Секретный ключ используется как «затравка» для герератора псевдвослучайных чисел. Исходными данными служит путь к файлу, в который необходимо встроить водяной знак. Из данного файла считывается массив байт, представляющий собой цветные компоненты пикселей изображения. Каждый бит водяного знака встраивается в изображение, используя 15 000 пикселов, сгенерированных с помощью псевдослучайного генератора. Таким образом данный класс производит 7 500 Patchwork-итераций, на кадой из которых получает значение двух цветовых компонент изображения. Для первой из них увеличивет значение на δ, для второй – уменьшает на δ. Значение δ выбрано равным 7. Изображение со встроенным водяным знаком отображается на экране.

Для проверки осуществляются те же действия, что и для встраивания. Вводится переменная, которая суммирует общее отклонение разности яркостей двух цветовых компонент. После 7 500 итераций в переменной остается отклонение, вызванное внедрением Patchwork-модификаций. Ошибка распределения принята равной 25 000. И если существует большее отклонение, то водяной знак считается подтвержденным.

Алгоритм Коха реализует внедрение ЦВЗ в области преобразования (служебную информацию) изображения. В качестве стегоконтейнера алгоритм использует коэффициенты дискретного косинусного преобразования (далее по тексту – ДКП), применяемого в широко распространенном формате JPEG.

ДКП производится отдельно для каждого из цветовых каналов. Исходное изображение разбивается на блоки размером 8×8 пикселов. ДКП применяется по отдельности к каждому блоку, по которому вычисляются матрицы коэффициентов ДКП тем же размером 8×8. Коэффициенты обычно обозначаются через $c_b(j,k)$, где b – номер блока, (j, k) – позиция коэффициента внутри блока. Если блок обрабатывается в зигзагообразном порядке, как это имеет место в стандартном JPEG, то коэффициенты обозначаются через $c_{b,j}$. Коэффициент в левом верхнем углу $c_b(0,0)$ называется DC-коэффициентом и хранит информацию о средней яркости всего блока в целом. Остальные коэффициенты называются AC-коэффициентами и содержат информацию о характере распределения яркостей по блоку. В редких случаях может быть выполнено ДКП всего изображения целиком [3].

Алгоритм Коха предполагает внедрение одного бита ЦВЗ в блок размером 8×8 пикселей. Выбирается значение порога встраивания ε. Для передачи бита со значением 0 последовательным изменением двух выбранных псевдослучайно AC-коэффициентов, используя известный ключ, добиваются того, чтобы разность абсолютных значений коэффициентов была больше порога, а для передачи бита со значением 1 эта же разность делается меньше обратного значения порога [4]:

$$\begin{cases} \left|c_b(j_{i,j},k_{i,1})\right| - \left|c_b(j_{i,2},k_{i,2})\right| > \varepsilon, & s_i = 0, \\ \left|c_b(j_{i,j},k_{i,1})\right| - \left|c_b(j_{i,2},k_{i,2})\right| < -\varepsilon, & s_i = 1. \end{cases}$$

Для чтения ЦВЗ в декодере выполняется аналогичная процедура выбора коэффициентов по известному ключу, а значение переданного бита выбирается по следующей формуле [4]:

$$\begin{cases} s_i = 0, & \left|c_b(j_{i,j},k_{i,1})\right| > \left|c_b(j_{i,2},k_{i,2})\right|, \\ s_i = 1, & \left|c_b(j_{i,j},k_{i,1})\right| < \left|c_b(j_{i,2},k_{i,2})\right|. \end{cases}$$

В ходе использования алгоритмов Patchwork и Коха были получены следующие экспериментальные оценки, которые указаны в таблице 1:

Таблица 1 – Экспериментальные оценки использования алгоритмов Patchwork и Коха

№п/п	Алгоритм	Размер изображения	Количество байт водяного знака	Время встраивания водяного знака	Время извлечения водяного знака
1	Patchwork	1920x1080	4	18.9 с.	18.5 с.
2	Коха	1920x1080	4	25.3 с.	12.3 с.
3	Patchwork	1920x1080	8	37.8 с.	37.8 с.
4	Коха	1920x1080	8	25.6 с.	11.1 с.

В ходе сравнения эффективности алгоритмов удалось установить, что алгоритм Patchwork является достаточно стойким к операциям усечения, сжатия, изменения гистограммы изображения. Основной недостаток алгоритма – это неустойчивость к геометрическим преобразованиям: сдвигу, повороту, масштабированию. Другим недостатком является малая пропускная способность, что не дает возможности встраивания значительных по размеру цифровых водяных знаков.

Алгоритм Коха, в свою очередь, является легко реализуемым, достаточно простым и весьма эффективным. Однако до внедрения ЦВЗ нельзя оценить и повлиять на степень искажения изображения.

В ходе анализа экспериментальных оценок использования алгоритмов удалось установить, что при встраивании достаточно малых водяных знаков эффективнее алгоритм Patchwork. Алгоритм Коха в свою очередь одинаково эффективен при встраивании как малых, так и больших водяных знаков, следовательно, он является более универсальным.

Список использованных источников:

1. Семёнов К. П. Алгоритмы встраивания цифровых водяных знаков в растровые изображения / К. П. Семёнов, П. В. Зайцев // Информационная безопастность регионов : научно-практический журнал. – 2011. – №1. – С. 46–50.

2. Bender W. Techniques for Data Hiding / W. Bender, D. Gruhl, N. Morimoto, A. Lu // IBM Systems Journal. – 1996. – Vol. 35.

3. Демидчук А.И., Чернявский Ю.А. Алгоритм поиска в изображениях скрытых данных, встроенных методов Коха – Жао. Информатика. 2012;(1(33)):39-46.

4. Koch E. Towards Robust and Hidden Image Copyright Labeling / E. Koch, J. Zhao // IEEE Workshop on Nonlinear Signal and Image Processing. – 1995.