Математические структуры и моделирование 2018. № 4(48). С. 113–119

УДК 004.932.2
DOI: 10.25513/2222-8772.2018.4.113-119

СТЕГАНОАНАЛИЗ АЛГОРИТМА КОХА-ЖАО

С.В. Белим
д.ф.-м.н., профессор, e-mail: sbelim@mail.ru
Д.Э. Вильховский
аспирант, e-mail: vilkhovskiy@gmail.com

Омский государственный университет им. Ф.М. Достоевского

Аннотация. Проведён анализ стеганографического алгоритма Коха–Жао. Рассмотрена возможность атаки на обнаружение сообщения. Предложен алгоритм вычисления границ встроенного сообщения, основанный на анализе коэффициентов дискретного косинусного преобразования. Проведён компьютерный эксперимент. Определены параметры встраивания, позволяющие осуществить атаку.

Ключевые слова: стеганография, стегоанализ, алгоритм Коха–Жао, дискретное косинусное преобразование.

Введение

Основной целью стеганографического анализа (стегоанализа) является исследование стойкости схемы стеганографического встраивания к атакам различного типа. Традиционно формулируются три основные задачи стегоанализа. Первая состоит в обнаружении факта наличия встроенного сообщения. При обнаружении встроенного сообщения ставится задача вычисления его размера и расположения в контейнере. Третьей и самой сложной задачей является извлечение встроенного сообщения и его интерпретация без каких-либо данных о параметрах встраивания.

На сегодняшний день основные успехи стегоанализа связаны с решением первой задачи. Причём применяются преимущественно статистические методы исследования контейнера с встроенным сообщением. Все эти методы основаны на предположении о том, что встраивание сообщения вносит изменения в статистические характеристики контейнера, которые могут быть обнаружены на основе исследования различных распределений. Так в статьях [1, 2] делают предположение о случайном характере распределения младших битов синей компоненты и на его основе применяют критерий χ-квадрат для задачи обнаружения стегановставки. Предложенный метод даёт хорошие результаты при равномерном заполнении контейнера. Для решения второй и третьей задачи статистических методов недостаточно и необходимо применять интеллектуальные алгоритмы. Например, в статьях [3–8] для анализа младшего слоя используется метод анализа иерархий, что позволяет с высокой степенью точности определить размеры и положение встроенной информации.

Целью данной работы является стегоанализ алгоритма Коха–Жао [9].

1. Алгоритм встраивания и постановка задачи

В качестве исходного объекта будем рассматривать изображение, в которое, предположительно, осуществлено встраивание сообщения. Достоверная информация о том, было осуществлено встраивание или нет, отсутствует. Однако известно, что встраивание могло быть осуществлено только методом Коха–Жао [9]. Причём встраивание сообщения могло быть осуществлено только непрерывным блоком. Поставим задачу обнаружения факта встраивания и извлечения встроенного сообщения, если оно присутствует.

Метод стеганографического встраивания Коха–Жао [9] использует двумерное дискретное косинусное преобразование и может быть записан в виде следующего алгоритма:

Шаг 1. Разбить исходное изображение на блоки размером 8×8 пикселей.

Шаг 2. Применить дискретное косинусное преобразование к каждому блоку. Получить набор матриц коэффициентов D_i ($i = 1, ..., N$; N — количество блоков) размером 8×8.

Шаг 3. Выбрать блоки для встраивания. Записать в каждый выбранный блок 1 бит встраиваемой информации.

Шаг 4. В каждом блоке выбрать два коэффициента дискретного косинусного преобразования (ДКП) симметричные относительно главной диагонали. Рекомендуется выбирать коэффициенты в среднечастотной области ($D_i[3,4]$ и $D_i[4,3]$, $D_i[3,5]$ и $D_i[5,3]$, $D_i[4,5]$ и $D_i[5,4]$).

Шаг 5. Если встраиваемый бит равен 0, то разность модулей пары коэффициентов дискретного косинусного преобразования должна превышать пороговое значение M_0, для встраивания единичного бита разность должна быть меньше M_0. Поэтому для встраивания нулевого бита увеличивается модуль первого коэффициента и на ту же величину уменьшается модуль второго. Для встраивания единичного бита, наоборот, уменьшается модуль первого коэффициента и на ту же величину увеличивается модуль второго коэффициента.

Шаг 6. Выполняются пункты 4 и 5 для каждого блока.

Шаг 7. Выполнить обратное дискретное косинусное преобразование для каждого блока.

Изменение среднечастотных компонент дискретного косинусного преобразования позволяет минимизировать визуальные эффекты встраивания. Встраивание в низкочастнотные компоненты приводит к заметному изменению фона изображения. Встраивание в высокочастное компоненты приводит к потере мелких деталей изображения.

При извлечении встроенного сообщения считается, что известны пары изменяемых коэффициентов дискретного косинусного преобразования. Первые четыре пункта алгоритма извлечения совпадают с пунктами алгоритма встраивания. Остальные шаги алгоритма имеют вид:

Шаг 5. Найти модуль разности модулей пар коэффициентов дискретного косинусного преобразования, в которое осуществлялось встраивание.

Шаг 6. Если разность превышает M_0, то был встроен нулевой бит, в противном случае — единичный.

Шаг 7. Последовательно определяем встроенные биты для каждого блока.

Для атаки на алгоритм Коха–Жао необходимо определить используемые пары коэффициентов дискретного косинусного преобразования и пороговое значение M_0. При осуществлении стегоанализа будем исходить из трёх предположений:

1. Встраивание происходит в непрерывную область, то есть используются подряд идущие блоки.

2. Во всех блоках для встраивания используются одни и те же пары коэффициентов.

3. Во всех блоках используется одно и то же пороговое значение.

2. Стеганографический анализ

Для решения задач стегоанализа будем исходить из того, что пороговое значение M_0 должно иметь большое значение. В противном случае особенности изображения, используемого в качестве контейнера, могут приводить к ошибкам при извлечении данных.

На первом этапе необходимо выявить пары коэффициентов дискретного косинусного преобразования, используемые для встраивания информации. По аналогии с алгоритмом извлечения сообщения разобъём изображение-контейнер на блоки B_i $(i = 1, ..., N)$ размером 8×8 пикселей. Выполним дискретное косинусное преобразование для каждого блока B_i $(i = 1, ..., N)$ и найдём матрицы коэффициентов D_i $(i = 1, ..., N)$, которые также имеют размер 8×8. Выполним анализ элементов матриц D_i $(i = 1, ..., N)$. Для этого построим три последовательности:

$$C_i(1) = ||D_i[3,4]| - |D_i[4,3]||, \quad i = 1, ..., N,$$
$$C_i(2) = ||D_i[3,5]| - |D_i[5,3]||, \quad i = 1, ..., N,$$
$$C_i(3) = ||D_i[4,5]| - |D_i[5,4]||, \quad i = 1, ..., N.$$

Если встраивание было осуществлено в среднечастотную компоненту, то одна из этих последовательностей должна значительно измениться. Для каждой из последовательностей $C_i(j)$ $(j = 1, 2, 3;\ i = 1, ..., N)$ проанализируем гистограмму зависимости от номера блока i Встроенное сообщение приводит к появлению изменённого блока в виде ступенчатой зависимости. Причём высота ступени зависит от порогового значения M_0. Пример гистограммы для последовательности без встроенного сообщения приведён на рис. 1, а аналогичная последовательность с встроенным сообщением — на рис. 2.

Таким образом, стегоанализ алгоритма Коха–Жао сводится к анализу зависимости последовательностей $C_i(j)$ $(j = 1, 2, 3;\ i = 1, ..., N)$ и выявлению участка ступенчатых изменений. После обнаружения ступенчатых участков необходимо определить их границы. Для этого выполним численное дифференцирование зависимости $C_i(j)$ $(j = 1, 2, 3;\ i = 1, ..., N)$ по i с использованием

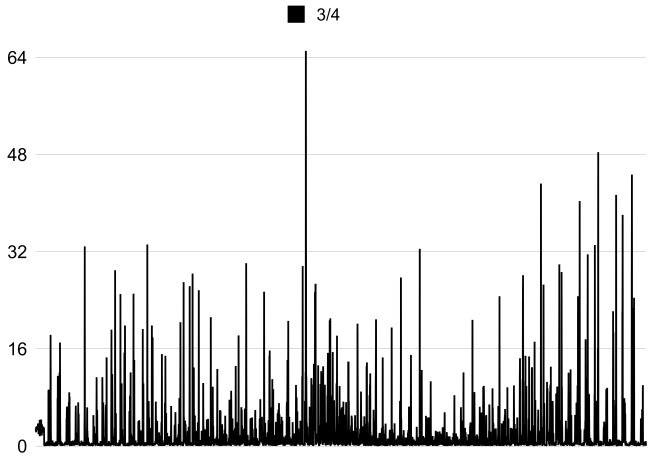

Рис. 1. Гистограмма зависимости $C_i(1)$ без встроенного сообщения

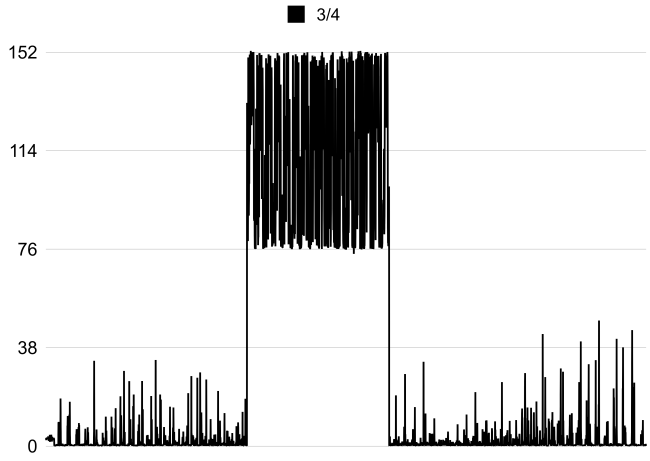

Рис. 2. Гистограмма зависимости $C_i(1)$ с встроенным сообщением

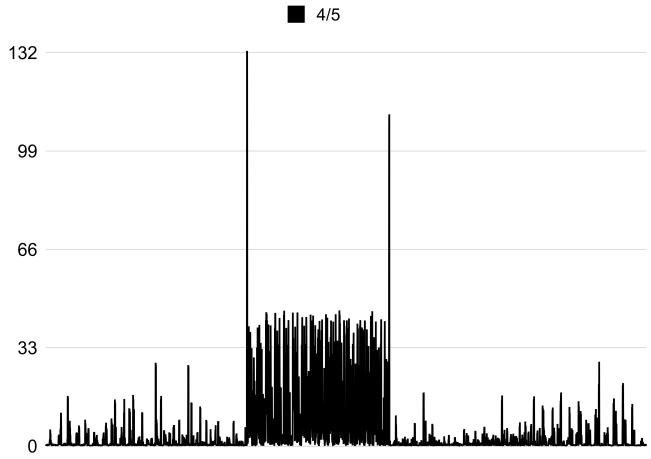

Рис. 3. Гистограмма последовательности $d_i(1)$ с встроенным сообщением

конечных разностей

$$dC_i(j) = C_i(j) - C_{i-1}(j).$$

В точках ступенчатого изменения после дифференцирования будут наблюдаться высокие пики, соответствующие границе встраивания сообщения. Гистограмма $dC_i(j)$ для случая встроенного сообщения представлена на рис. 3.

Поставим задачу автоматического определения границ области встраивания. Для этого для каждой последовательности $d(j)$ определим несколько характеристик: M_j — максимальное значение элементов последовательности $d(j)$, N_j — среднее значение элементов последовательности $d(j)$, O_j — среднеквадратичное отклонение для элементов последовательности $d(j)$. Далее вычислим $R_j = N_j + O_j$. Введём переменную Y_j, принадлежащую интервалу $[R_j,\ M_j]$. Подберём такое значение Y_j, чтобы существовало ровно два элемента последовательности $d(j)$, превышающих его: $C_{i1}(j) > Y_j$ и $C_{i2}(j) > Y_j$. Полученные индексы элементов i_1 и i_2 являются границами встраивания сообщения. Для определения порогового значения M_0 найдём значение минимального элемента последовательности $C_i(j)$ на интервале $[i_1,i_2]$.

Алгоритм выявления встроенного изображения принимает вид:

Шаг 1. Разбить изображение на блоки B_i размером 8×8 пикселей.

Шаг 2. К каждому блоку B_i применить дискретное косинусное преобразование и получить матрицы коэффициентов дискретного косинусного преобразования D_i.

Шаг 3. Вычислить элементы трёх последовательностей величин:

$$C_i(1) = ||D_i[3,4]| - |D_i[4,3]||, \quad i = 1, ..., N,$$
$$C_i(2) = ||D_i[3,5]| - |D_i[5,3]||, \quad i = 1, ..., N,$$
$$C_i(3) = ||D_i[4,5]| - |D_i[5,4]||, \quad i = 1, ..., N.$$

Шаг 4. Выполнить численное дифференцирование каждой из последователь-

ностей $C_i(j)$ по i:

$$dC_i(j) = C_i(j) - C_{i-1}(j) \quad j = 1, 2, 3 \quad i = 1, ..., N.$$

Шаг 5. Вычислить: M_j — максимальное значение элементов массива $d(j)$, N_j — среднее значение элементов массива $d(j)$, O_j — среднеквадратичное отклонение для элементов массива $d(j)$, $R_j = N_j + O_j$.

Шаг 6. Перебрать различные значения величины Y_j в интервале от R_j до M_j с шагом dY. Определить Y_j такое, что существует ровно два значения $C_{i1}(j) > Y_j$ и $C_{i2}(j) > Y_j$. Если такое значение определить невозможно, то уменьшить шаг dY. Определить i_1 и i_2.

Шаг 7. Найти минимальное значение $C_i(j)$ на интервале от i_1 до i_2. Присвоить M_0 найденное значение.

Шаг 8. Извлечь сообщение, используя найденные параметры.

Компьютерный эксперимент показал, что данный алгоритм позволяет безошибочно находить и извлекать встроенное сообщение при значениях $M_0 > 54$.

Заключение

Стегоанализ алгоритма стеганографического встраивания Коха–Жао, проведённый в данной статье, выявил неустойчивость к атаке анализа коэффициентов дискретного косинусного преобразования. Предложенный в статье алгоритм позволяет с высокой точностью определить положение встроенного сообщения и извлечь его. Алгоритм применим при встраивании в непрерывную область.

Литература

1. Provos N., Honeyman P. Detecting steganographic content on the internet // Technical Report CITI 01-1a. University of Michigan, 2001.
2. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems // Lecture Notes in Computer Science. 2000. V. 1768. P. 61–75.
3. Vilkhovskiy D.E., Belim S.V. Detection the Stego-Insertions Like LSB-Substitution in Bitmap Images // Proceedings of the Workshop on Data, Modeling and Security (DMS 2017). CEUR Workshop Proceedings. 2017. V. 1965. URL: `http://ceur-ws.org/Vol-1965/paper11.pdf` (дата обращения: 26.10.2018).
4. Belim S.V., Vilkhovskiy D.E. Usage of analytic hierarchy process for steganographic inserts detection in images // 2016 Dynamics of Systems, Mechanisms and Machines (Dynamics). 2016. URL: `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7818977&isnumber=7818960` (дата обращения: 26.10.2018).
5. Belim S.V., Vilkhovskiy D.E. Steganalysis Algorithm Based on Heirarchy Analysis Method // Proceedings of the Workshop on Data Analysis and Modelling (DAM 2016). CEUR Workshop Proceedings. 2016. V. 1732. URL: `http://ceur-ws.org/Vol-1732/paper7.pdf.` (дата обращения: 26.10.2018).
6. Belim S.V., Vilkhovskiy D.E. Algorithm for detection of steganographic inserts type LSB-substitution on the basis of an analysis of the zero layer // Journal of Physics: Conf. Series. 2017. V. 944. P. 012012(1–6).

7. Белим С.В., Вильховский Д.Э. Алгоритм выявления стеганографических вставок типа LSB-замещения на основе анализа слоя младших битов // Информатика и системы управления. 2017. № 4(54). С. 3–11.
8. Белим С.В., Вильховский Д.Э. Алгоритм выявления стеганографических вставок типа LSB-замещения на основе метода анализа иерархий // Вестник компьютерных и информационных технологий. 2018. № 4. С. 25–33.
9. Koch E., Zhao J. Towards robust and hidden image copyright labeling // IEEE Workshop on Nonlinear Signal and Image Processing. 1995. P. 452–455.

KOCH-ZHAO ALGORITHM STEGANALYSIS

S.V. Belim
Dr.Sc. (Phys.-Math.), Professor, e-mail: sbelim@mail.ru
D.E. Vilkhovskiy
Postgraduate Student, e-mail: vilkhovskiy@gmail.com

Dostoevsky Omsk State University

Abstract. The analysis of the Koch–Zhao steganographic algorithm was carried out. The possibility of an attack on the detection of messages is considered. An algorithm for calculating the boundaries of the embedded message based on the analysis of the discrete cosine transform coefficients is proposed. A computer experiment is conducted. Embedding parameters that allow the attack are defined.

Keywords: steganography, steganalysis, Koch–Zhao algorithm, discrete cosine transform.

Дата поступления в редакцию: 17.11.2018