УДК 004.056.5

ПРЕОБРАЗОВАНИЕ СПЕКТРА СИММЕТРИЧНОЙ МАТРИЦЫ КАК ВОЗМОЖНАЯ ОСНОВА СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА ДЛЯ ПРОИЗВОЛЬНОГО ЦИФРОВОГО ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА

Д. т. н. А. А. Кобозева, к. т. н. О. В. Николаенко, В. С. Васьковец

Одесский национальный политехнический университет
Украина, г. Одесса
alla_kobozeva@ukr.net

В работе проводится исследование свойств спектра симметричной матрицы с целью их использования в компьютерной стеганографии для контейнера с произвольной матрицей.

Ключевые слова: стеганография, спектральное разложение, цифровое изображение, собственное значение, матрица

Мощное развитие вычислительной техники дало толчок для развития компьютерной стеганографии [1, 2], целью которой является защита информации, представленной в цифровом виде, от несанкционированного доступа. Методы стеганографии позволяют встраивать секретное сообщение или дополнительную информацию (ДИ) в непривлекающее внимания «безобидное» послание или контейнер так, чтобы невозможно было заподозрить сам факт существования тайного послания. Процесс погружения ДИ преобразовывает исходный контейнер, или основное сообщение (ОС), в стеганосообщение (СС), которое затем открыто пересылается адресату по каналу связи. В качестве ОС рассматривается цифровое изображение (ЦИ) в градациях серого, математической моделью которого выступает прямоугольная матрица.

При погружении ДИ в ОС последнее может предварительно преобразовываться, причем вид преобразования зависит от многих факторов, в частности, предполагаемых атак на СС, требования надежности восприятия СС и т. д.

Целью работы является математическое обоснование свойств спектра симметричной матрицы, важных с точки зрения возможности использования спектрального разложения и особенностей собственных значений неотрицательных матриц в компьютерной стеганографии. Предлагаемый теоретический аппарат может быть использован не только для создания стеганометодов, но и для решения некоторых вопросов, остающихся открытыми из-за недостаточной теоретической базы в уже существующих алгоритмах, построенных на основе сингулярного разложения матриц.

Пусть H – произвольная симметричная $n \times n$ матрица, элементы которой $h_{ij} \in R,\ \ i, j = \overline{1, n}$, с собственными значениями $\lambda_i \in R,\ \ i = \overline{1, n}$, и ортонормированными собственными векторами $u_i,\ \ i = \overline{1, n}$, т. е. $H = U \Lambda U^T$ — спектральное разложение матрицы H (здесь $\Lambda = diag(\lambda_1, ..., \lambda_n)$, $U = [u_1, ..., u_n]$) [3]. В силу симметричности H ее спектр, т. е. множество всех собственных значений, всегда действительный. Кроме того, множество собственных значений, являясь корнями характеристического многочлена $\det(H - \lambda E) = 0$, определяется однозначно, в отличие от спектрального разложения.

В работе показано следующее.

— Если погружение ДИ происходит за счет возмущения δ некоторого собственного значения симметричной матрицы ОС, то величина результирующего возмущения матрицы контейнера, вызванного таким стегопреобразованием, определяется лишь абсолютным значением δ, и не зависит от того, какое именно собственное значение было возмущено.

— При погружении ДИ за счет изменения нескольких собственных значений симметричной матрицы ОС, ее возмущение определяется максимальным по модулю возмущением собственных зна-

чений (при использовании спектральной матричной нормы [4]).

— Возмущение матрицы контейнера при погружении секретного сообщения за счет изменения собственных значений не зависит от того, какие именно собственные значения были возмущены, а зависит лишь от величины этих возмущений.

— Если возмущение матрицы исходного изображения H осуществляется путем увеличения хотя бы одного диагонального элемента (что эквивалентно прибавлению к исходной матрице H положительно полуопределенной диагональной матрицы), это приводит к неуменьшению (а на практике, как показывает вычислительный эксперимент, к увеличению) всего спектра, т. е. влиять на весь спектр можно при помощи единственного, наиболее «удобного» для этого диагонального элемента исходной матрицы. Корректировка спектра осуществляется в соответствии с определенными требованиями, например, наличие в спектре элемента, модуль которого больше определенного порогового значения.

Матрица произвольного ЦИ не является в общем случае симметричной. «Виртуальная симметричность» достигается следующим образом. Пусть матрица F размерности $n \times m$, значения элементов которой принадлежат множеству $\{0, 1, ..., 255\}$, отвечает ОС. Разобьем ее на квадратные блоки фиксированного небольшого размера, например 8×8, как это делается в стандарте JPEG. Пусть A — матрица одного из таких блоков. Блоку A исходного изображения поставим в соответствие две матрицы B, C той же размерности в соответствии со следующим правилом:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \dots a_{18} \\ a_{21} & a_{22} & a_{23} \dots a_{28} \\ a_{31} & a_{32} & a_{33} \dots a_{38} \\ \dots & \dots & \dots \\ a_{81} & a_{82} & a_{83} \dots a_{88} \end{pmatrix} \to B = \begin{pmatrix} a_{11} & a_{12} & a_{13} \dots a_{18} \\ a_{12} & a_{22} & a_{23} \dots a_{28} \\ a_{13} & a_{23} & a_{33} \dots a_{38} \\ \dots & \dots & \dots \\ a_{18} & a_{28} & a_{38} \dots a_{88} \end{pmatrix}, \quad C = \begin{pmatrix} a_{11} & a_{21} & a_{31} \dots a_{81} \\ a_{21} & a_{22} & a_{32} \dots a_{82} \\ a_{31} & a_{32} & a_{33} \dots a_{83} \\ \dots & \dots & \dots \\ a_{81} & a_{82} & a_{83} \dots a_{88} \end{pmatrix}$$

Матрицы B, C являются симметричными, они могут использоваться в качестве блоков контейнера для стеганопреобразования, заключающегося в определенной модификации собственных значений с учетом полученных выше свойств, при этом блок СС будет формироваться из подматриц B, C по правилу, определяемому конкретным стеганографическим алгоритмом.

Таким образом, в работе проведено исследование некоторых свойств собственных значений симметричной матрицы, представляющих интерес с точки зрения использования модификаций спектра матрицы в стеганографических алгоритмах. Полученные теоретические результаты открывают широкие возможности для создания новых стеганометодов, результат работы которых окажется математически предсказуемым и обоснованным.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А. Стеганография, цифровые водяные знаки и стеганоанализ.— Москва: Вузовская книга, 2009.

2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика.— Киев: МК – Пресс, 2006.

3. Бахвалов Н. С., Жидков Н. П., Кобельков Г. М. Численные методы.— Москва: БИНОМ. Лаборатория знаний, 2006.

4. Деммель Дж. Вычислительная линейная алгебра.— Москва: Мир, 2001.

A. A. Kobozeva, O. V. Nikolaenko, V. S. Vaskovets

Transformation of the spectrum of a symmetric matrix as a possible basis for steganographic algorithm for arbitrary digital cover-images.

This paper is devoted to the properties of the spectrum of a symmetric matrix to be used in computer steganography for container with an arbitrary matrix.

Keywords: *steganography, spectral decomposition, digital image, eigenvalue, matrix.*