УДК 004.056.5:518

А.А. Кобозева, канд. физ.-мат. наук, доц., Одес. нац. политехн. ун-т

ИСПОЛЬЗОВАНИЕ НОРМАЛЬНОГО СПЕКТРАЛЬНОГО РАЗЛОЖЕНИЯ СИММЕТРИЧНОЙ МАТРИЦЫ В КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

А.А. Кобозєва. **Використання нормального спектрального розкладання симетричної матриці в комп'ютерній стеганографії.** Обгрунтовуються деякі властивості спектрального розкладання матриці, на основі яких будується новий стегоалгоритм, застосовний до будь-якого контейнера, приводяться результати обчислювального експерименту.

A.A. Kobozeva. **Use of symmetric matrix normal spectral decomposition in computer steganography.** Some features of matrix spectral decomposition are grounded, serving as the basis for constructing a new stegoalgorithm applicable for any container. The results of a calculation experiment are presented.

Интенсивное развитие и распространение компьютерных технологий сделало недопустимо простым получение доступа к одному из ценнейших предметов современной жизни — информации. Поэтому во всем мире назрел вопрос разработки методов защиты информации, представленной в цифровом виде, среди которых важнейшее место занимают методы стеганографии [1, 2].

Общей чертой всех стегометодов является то, что секретное сообщение, или дополнительная информация (ДИ), погружается в некоторый объект, или основное сообщение (ОС), не привлекающий внимания, который затем открыто пересылается по каналу связи адресату или хранится в таком виде.

Не ограничивая общности рассуждений, для простоты изложения далее в качестве ОС, или контейнера, рассматривается монохромное изображение.

Многие известные стеганографические алгоритмы производят погружение секретной информации с использованием различных трансформаций контейнера, например, дискретного преобразования Фурье, сингулярного разложения матрицы (SVD) [3, 4] и т.д. Не найдено работ, посвященных использованию спектрального разложения (СР) симметричной матрицы применительно к стеганографическим методам, что, очевидно, объясняется тем, что матрица контейнера, как правило, не удовлетворяет свойству симметричности, а СР определяется неоднозначно. Однако, построение СР для симметричной матрицы является более предпочтительным в вычислительном смысле, чем SVD для матрицы общего вида [5, 6]. Это явилось побуждающим мотивом к исследованию возможностей использования СР в цифровой стеганографии.

Математически обосновываются свойства СР матрицы, важные с точки зрения применения этого разложения для целей компьютерной стеганографии, что никогда не делалось ранее, а также предлагается новый стегоалгоритм, применимый для любого ОС, основанный на нормальном СР симметричной матрицы, использующий в качестве преобразования, предваряющего погружение ДИ, сжатие ОС при помощи малоранговой аппроксимации.

Матрица контейнера, как правило, симметричной не является. Пусть **A** — произвольная $n \times n$ матрица ОС, элементы которой $a_{ij} \in R, \quad i, j = \overline{1,n}$. Поставим в соответствие матрице **A** две симметричные матрицы по следующему правилу:

$$\mathbf{A}=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix} \to \mathbf{AV}=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{12} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{13} & a_{23} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{nn} \end{pmatrix}, \ \mathbf{AN}=\begin{pmatrix} a_{11} & a_{21} & a_{31} & \dots & a_{n1} \\ a_{21} & a_{22} & a_{32} & \dots & a_{n2} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}. \quad (1)$$

Формула (1) дает принципиальную возможность рассматривать в дальнейшем в качестве матрицы ОС симметричную матрицу (**AV**, **AN**).

Пусть $\mathbf{A}=\mathbf{A}^T$, $\lambda_i \in R$, $i=\overline{1,n}$, — собственные значения (СЗ), u_i, $i=\overline{1,n}$, — ортонормированные собственные векторы (СВ) **A**,

$$\mathbf{A}=\mathbf{U}\mathbf{\Lambda}\mathbf{U}^T \quad (2)$$

— спектральное разложение **A** [7] (здесь $\mathbf{\Lambda}=\mathrm{diag}(\lambda_1,...,\lambda_n)$, $\mathbf{U}=[u_1,...,u_n]$).

Будем называть СР (2) *нормальным*, если элементы матрицы $\mathbf{\Lambda}$ удовлетворяют соотношению: $|\lambda_1| \ge ... \ge |\lambda_n|$, а СВ u_i, $i=\overline{1,n}$, лексикографически положительны, т.е. первая ненулевая компонента каждого столбца **U** положительна.

Теорема. Пусть **A** — невырожденная симметричная $n \times n$-матрица, модули собственных значений которой попарно различны. Тогда для нее существует единственное нормальное спектральное разложение (НСР).

Доказательство. Модули СЗ **A** попарно различны, каждое СЗ имеет кратность, равную единице, которая определяет и размерность любого собственного подпространства матрицы **A**. Тогда для каждого λ_i нормированный базис такого подпространства может определяться двумя способами: это вектора единичной длины противоположных направлений, единственный из них является лексикографически положительным. Таким образом, столбец матрицы **U**, отвечающий СЗ λ_i, определится однозначно. Порядок столбцов соответствует порядку элементов диагонали $\mathbf{\Lambda}$.

Утверждение. Пусть $\mathbf{A}=\mathbf{A}^T$. Для матрицы **A** построено НСР (2). Ближайшей к **A** в смысле спектральной нормы $\|\bullet\|_2$ [6] матрицей ранга $k < n$ является

$$\mathbf{A}_k = \sum_{i=1}^{k} \lambda_i u_i u_i^T, \quad (3)$$

причем $\|\mathbf{A}-\mathbf{A}_k\|_2 = |\lambda_{k+1}|$. Для матрицы $\mathbf{A}_k$, малоранговой аппроксимации **A**, справедливо также представление $\mathbf{A}_k = \mathbf{U}\mathbf{\Lambda}_k\mathbf{U}^T$, где $\mathbf{\Lambda}_k = \mathrm{diag}(\lambda_1,...,\lambda_k,0,...,0)$.

Доказательство. Приведем одно из возможных доказательств утверждения. По построению матрица $\mathbf{A}_k$ имеет ранг k, а $\|\mathbf{A}-\mathbf{A}_k\|_2 = \left\| \sum_{i=k+1}^{n} \lambda_i u_i u_i^T \right\|_2 = |\lambda_{k+1}|$. Пусть **B** — произвольная $n \times n$-матрица ранга k, ее ядро [8] имеет размерность $n-k$, а подпространство, являющееся линейной оболочкой векторов $u_1,...,u_{k+1}$, имеет размерность $k+1$. Поскольку $(n-k)+(k+1) > n$, пересечение указанных подпространств непусто. Пусть нормированный вектор h принадлежит этому пересечению. Тогда **B** $h=0$ и $h=c_1u_1+...+c_{k+1}u_{k+1}$, $\|h\|_E=1$ ($\|\bullet\|_E$ — евклидова векторная норма [6]), т.е. $c_1^2+...+c_{k+1}{}^2=1$. В силу согласованности [6] спектральной матричной и евклидовой векторной норм, имеем

$$\|(\mathbf{A}-\mathbf{B})h\|_g \le \|\mathbf{A}-\mathbf{B}\|_2 \|h\|_E = \|\mathbf{A}-\mathbf{B}\|_2.$$

Если **U** — ортогональная матрица, то для любого вектора x имеет место равенство: $\|x\|_E = \|\mathbf{U}_x\|_E$

Действительно, т.к. $\|\mathbf{U}\|_2 = \sqrt{\lambda_{\max}(\mathbf{U}^T\mathbf{U})} = 1$, то

$$\|x\|_E = \|\mathbf{U}^T\mathbf{U}_x\|_E \le \|\mathbf{U}^T\|_2 \|\mathbf{U}_x\|_E = \|\mathbf{U}_x\|_E \le \|\mathbf{U}\|_2 \|x\|_E = \|x\|_E .$$

Таким образом $\|x\|_E = \|\mathbf{U}_x\|_E \le \|x\|_E$, а значит, $\|x\|_E = \|\mathbf{U}_x\|_E$. Тогда

$$\|\mathbf{A} - \mathbf{B}\|_2^2 \ge \|\mathbf{A}h\|_E^2 = \|\mathbf{U}\Lambda\mathbf{U}^T h\|_E^2 = \|\Lambda\mathbf{U}^T h\|_E^2 ,$$

$$\mathbf{U}^T h = (u_1^T,...,u_{k+1}^T,u_{k+2}^T,...,u_n^T)^T (c_1u_1 + ... + c_{k+1}u_{k+1}) = c_1\ (u_1^T,...,u_{k+1}^T,u_{k+2}^T,...,u_n^T)^T u_1 + ... +$$

$$+c_{k+1}(u_1^T,...,u_{k+1}^T,u_{k+2}^T,...,u_n^T)^T u_{k+1} = c_1(1,0,...,0)^T + ... + c_{k+1}(0,0,...,0,\underset{k+1}{1},0,...,0)^T .$$

В результате $\mathbf{U}^T h = (c_1,...,c_{k+1},0,...,0)^T$, а $\Lambda\mathbf{U}^T h = (c_1\lambda_1,...,c_{k+1}\lambda_{k+1},0,...,0)^T$.

$$\|\Lambda\mathbf{U}^T h\|_2^2 = c_1^2\lambda_1^2 + \ldots + c_{k+1}^2\lambda_{k+1}^2 \ge \lambda_{k+1}^2(c_1^2 + \ldots + c_{k+1}^2) = \lambda_{k+1}^2$$

Таким образом, для произвольной матрицы $\mathbf{B}\|\mathbf{A} - \mathbf{B}\|_2 \ge |\lambda_{k+1}|$

Определим *матрицу разности* (MR) между двумя произвольными матрицами **G** и **H** одинаковой размерности естественным образом: **C**=MR(**G,H**)=**G – H**.

Пусть **AV**(**AN**) — симметричная квадратная матрица ОС. В качестве предваряющей погружение трансформации контейнера рассмотрим его сжатие при помощи ближайшей аппроксимации ранга k —**AV**$_k$ (**AN**$_k$). Обозначим $\mathbf{C}_k^{(V)}$=MR(**AV,AV**$_k$), $\mathbf{C}_k^{(V)}$= MR(**AN,AN**$_k$). Пусть ДИ — это бинарная последовательность $p_1, p_2, ...,$ где $p_i \in \{0,1\}$.

Основные этапы при погружении ДИ предлагаемого нового стегоалгоритма заключаются в следующем:

— для матрицы **A** ОС в соответствии с (6) получаем симметричные матрицы **AV** и **AN**;

— для матрицы **AV** ОС строится НСР (2);

— используя НСР (2), строится **AV**$_k$ в соответствии с (3);

— по матрицам **AV** и **AV**$_k$ вычисляется $\mathbf{C}_k^{(V)}$;

— пусть p_l — очередной элемент секретного сообщения, подлежащий встраиванию, а элементы, следующие за ним в ДИ — это p_{l+1}, p_{l+2}, p_{l+3} и т.д. Процедура погружения будет определяться значением p_l:

а) если $p_l = 1$, то для погружения используется очередной по порядку пиксель верхнего треугольника **AV**$_k$, для которого соответствующий элемент $\mathbf{C}_k^{(V)}$ больше нуля. Пусть такой элемент — $c_{m,j}^{(k)} = t > 0$. Встраивание информации производится в соответствии со следующим правилом: в бинарной последовательности p_l, p_{l+1}, p_{l+2},... выделяется такая ее часть максимальной длины, начиная с p_l, что при рассмотрении ее в виде двоичного представления десятичного числа, это число будет меньше t. Пусть это число w. Тогда погружение выделенной части ДИ осуществляется в соответствии с формулой: $a_{m,j}^{(S)} = a_{m,j}^{(k)} + w$, где $a_{m,j}^{(S)}$ — соответствующий элемент стегосообщения **AV**$^{(S)}$, сформированного на основе **AV**$_k$, $a_{m,j}^{(k)}$ — элемент матрицы **AV**$_k$. Например, пусть $c_{m,j}^{(k)} = 9$, а очередная часть секретного сообщения, которая еще не подверглась погружению, — 1,0,1,1,1,0,1,0,0,... Определим погружаемую подпоследовательность и w:

$$1_{(2)} = 1_{(10)} < 9\ ;\ 10_{(2)} = 2_{(10)} < 9\ ;\ 101_{(2)} = 5_{(10)} < 9\ ;\ 1011_{(2)} = 11_{(10)} > 9 .$$

Таким образом, цепочка ДИ, погружаемая в текущий пиксель — 101, $w = 5$.

б) Если $p_l = 0$, то в цепочке p_l, p_{l+1}, p_{l+2},... ищется первый по порядку ненулевой элемент p_{l+q}. Для погружения используется очередной по порядку пиксель верхнего треугольника $\mathbf{AV}_k$, для которого соответствующий элемент $\mathbf{C}_k^{(V)}$ меньше нуля. Пусть это $c_{i,r}^{(k)}$. Количество нулей, которое можно погрузить в рассматриваемый пиксель, должно быть меньше $\left|c_{i,r}^{(k)}\right|$. Погружение осуществляется в соответствии с формулой: $a_{i,r}^{(S)} = a_{i,r}^{(k)} - q$. Если $q \geq \left|c_{i,r}^{(k)}\right|$, то для погружения оставшейся части подряд стоящих нулей берется следующий по порядку пиксель, для которого соответствующий элемент $\mathbf{C}_k^{(V)}$ меньше нуля;

— для матрицы **AN** повторяем предыдущие этапы, используя $\mathbf{C}_k^{(V)}$, погружая ДИ лишь в нижний треугольник **AN**, формируя на основе **AN** стегосообщение $\mathbf{AN}^{(S)}$;

— стегосообщение $\mathbf{A}^{(S)}$ формируется как объединение двух треугольных матриц, непосредственно участвовавших в погружении ДИ на предыдущих этапах: верхнего треугольника $\mathbf{AV}^{(S)}$ и нижнего треугольника $\mathbf{AN}^{(S)}$.

В качестве секретного ключа в процессе декодирования используется матрица исходного изображения **A** и ранг аппроксимации k. Процесс декодирования ДИ состоит из следующих основных этапов:

— по стегосообщению $\mathbf{A}^{(S)}$ в соответствии с (6) получаем $\mathbf{AV}^{(S)}$, $\mathbf{AN}^{(S)}$;

— находим $\mathbf{C}_k^{(V^{(S)})} = \mathrm{MR}(\mathbf{AV}^{(S)}, \mathbf{AV}_k)$, $\mathbf{C}_k^{(V^{(S)})} = \mathrm{MR}(\mathbf{AN}^{(S)}, \mathbf{AN}_k)$;

— просматриваем по порядку элементы верхнего треугольника матрицы $\mathbf{C}_k^{(V^{(S)})}$. Пусть c_{ij} — очередной элемент:

а) если $c_{ij} > 0$, то десятичное значение c_{ij} представляется в двоичном виде, давая часть секретного сообщения;

б) если $c_{ij} < 0$, то значение $\left|c_{ij}\right|$ определяет количество встроенных в рассматриваемый пиксель нулей;

— аналогичные предыдущему этапу действия повторяем для нижнего треугольника матрицы $\mathbf{C}_k^{(V^{(S)})}$.

Вычислительный эксперимент, целью которого являлась апробация свойств нового алгоритма, проводился в среде MATLAB в условиях идеального канала связи. В качестве ОС брались произвольные монохромные изображения. Эффективность декодирования нового метода составила 100 %, в то время, как алгоритм, основанный на SVD матрицы ОС в аналогичных условиях дает лишь 75 % правильно восстановленной информации [3].

Одним из ключевых вопросов реализации нового алгоритма является выбор параметра k — ранга аппроксимации матрицы ОС. Этот выбор осуществляется на основании компромисса между требованиями, находящимися друг по отношению к другу в обратной зависимости [2]: обеспечения надежности восприятия стегосообщения после погружения и достаточной пропускной способности. В результате установлено, что значение параметра k, удовлетворяющее в достаточной мере обоим требованиям, зависит от конкретного ОС. Так для изображения CAMERAMAN.TIF уже при $k \leq 70$ происходит нарушение надежности восприятия стегосообщения (рис. 1), тогда как для ОС MOON.TIF такое нарушение происходит только для $k \leq 40$ (рис. 2).

Основным преимуществом предложенного метода является его сравнительно большая максимальная пропускная способность, достигаемая при минимальном ранге аппроксимации, обеспечивающем надежность восприятия стегосообщения (см. таблицу). Сравнение проводилось не только с методом, основанным на сингулярном разложении матрицы ОС [3], но и с методом LSB (стегометод замены наименее значащего бита [2]), пропускная способность которого, как известно, достаточно велика. Реальная пропускная способность, конечно, будет зависеть от конкретного ОС и ДИ (рис. 3).

а *б* *в*

Рис. 1.Стегопреобразования изображения CAMERAMAN.TIF: основное сообщение (а); стегосообщение, полученное при ранге аппроксимации k=70 (б); стегосообщение, полученное при k=80 (в)

а *б* *в*

Рис. 2. Стегопреобразования изображения MOON.TIF : основное сообщение (а); стегосообщение, полученное при ранге аппроксимации k=40 (б); стегосообщение, полученное при k=50 (в)

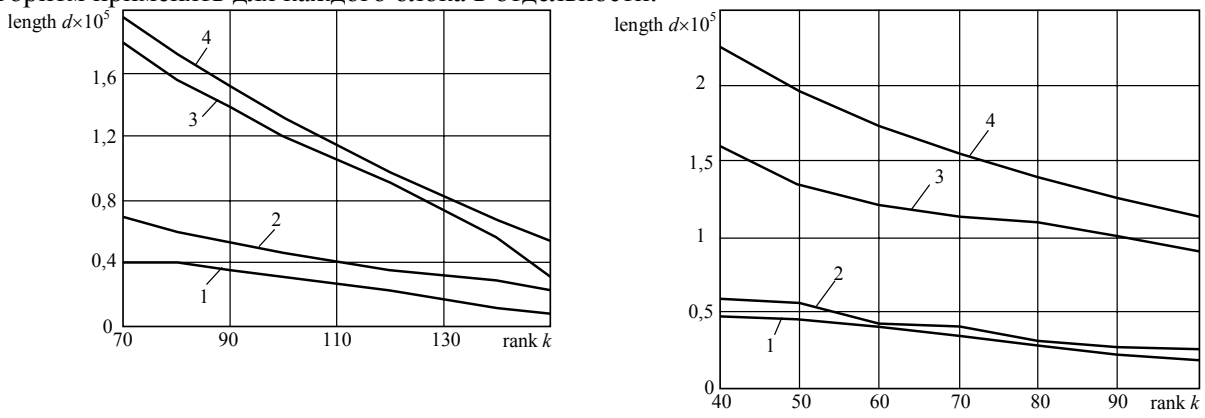
На основании эксперимента можно утверждать, что предложенный алгоритм ведет себя по основным показателям [2] гораздо лучше, чем стегоалгоритм, основанный на сингулярном разложении матрицы ОС [3]. Использование же вместо сингулярного разложения НСР матрицы ОС делает предлагаемый алгоритм более предпочтительным по сравнению с [3] даже при всех равных показателях.

Сравнение пропускной способности различных стегометодов для различных ОС

Основное сообщение	Ранг аппрок-симации	Длина секретного сообщения для метода LSB	Длина сообщения для метода, основанного на сингулярном разложении матрицы ОС	Максимальная длина сообщения для нового метода
CAMERAMAN.TIF	80	65536	15360	172881
POUT.TIF	50	57600	13500	63967
MOON.TIF	50	128164	29040	196422
TIRE.TIF	45	42025	9375	111423
MRI.TIF	25	16384	3840	31655
CELL.TIF	30	25281	5415	39498

Проведенное обоснование некоторых математических особенностей спектрального разложения симметричной матрицы, проведенное в данной работе, дало возможность для создания нового стегоалгоритма, применимого для любого ОС, предпочтительного по эффективности декодирования ДИ и пропускной способности по сравнению с алгоритмом, основанным на сингулярном разложении матрицы ОС [3].

Вычислительная сложность алгоритма сравнима с количеством арифметических операций для построения спектрального разложения матрицы и составляет $\underline{O}(n^3)$, где n — размерность матрицы ОС. Это количество можно уменьшить до $\underline{O}(n^2)$, если предварительно подвергнуть матрицу контейнера операции разбиения на блоки фиксированной малой размерности [9], а алгоритм применять для каждого блока в отдельности.



а *б*

Рис. 3.Графики зависимости длины погружаемого сообщения от ранга аппроксимации k: ОС CAMERAMAN.TIF (а); ОС- MOON.TIF (б): 1, 2, 3 — сообщения, сформированы случайным образом, 4 — сообщение соответствует максимальной пропускной способности

Аналогично [3], нерешенной пока остается проблема обеспечения достаточной эффективности алгоритма в условиях различных атак. Очевидно, что в своем первоначальном предлагаемом виде этот алгоритм формирует стегосообщение, которое будет чувствительным к возмущениям в канале связи, и устранение этой чувствительности может быть проведено только за счет модификации базового алгоритма, над которой ведется работа.

Литература

1. Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. — К.: Юниор, 2003. — 501с.
2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. — К.: МК-Пресс, 2006. — 288 с.
3. Bergman C. Unitary embedding for data hiding with the SVD / Bergman C., Davidson J. // Security, steganography, and watermarking of multimedia contents VII, SPIE. — 2005. — Vol. 5681. — P. 45 — 57.
4. Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах // Вісн. Східноукр. нац. ун-ту ім. В. Даля. — 2006. — № 9(103), ч. 1. — С. 74 — 83.
5. Каханер Д. Численные методы и программное обеспечение / Каханер Д., Моулер К., Нэш С. — М.: Мир, 2001. — 575 с.
6. Деммель Дж. Вычислительная линейная алгебра. — М.: Мир, 2001. — 430 с.
7. Парлетт Б. Симметричная проблема собственных значений. Численные методы. — М.: Мир, 1983. — 384 с.
8. Хорн Р. Матричный анализ / Хорн Р., Джонсон Ч. — М.: Мир, 1989. — 656 с.
9. Гонсалес Р. Цифровая обработка изображений / Гонсалес Р., Вудс Р. — М.: Техносфера, 2005. — 1072 с.

Поступила в редакцию 12 февраля 2007 г.