УДК 004.056.5:621.396

Чечельницкий В.Я. (ОНПУ)

ПОРОЖДАЮЩИЙ КЛАСС СОВЕРШЕННЫХ ДВОИЧНЫХ РЕШЕТОК РАЗМЕРА 12x12 ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

Квадратные совершенные двоичные решетки — СДР (Perfect Binary Array — PBA) существуют следующих порядков $N = 2^k$ и $N = 3 \cdot 2^k$ для произвольных натуральных k [1]. Понятие порождающего ($\Pi(N)$-класса) и эквивалентного классов СДР впервые введено в [2].

Каждая СДР порядка N путем операций циклического сдвига ее строк и столбцов порождает класс эквивалентных СДР ($E(N)$-класс) мощности

$$\Psi_{E(N)} = N^2. \qquad (1)$$

Таким образом, если каким-либо способом найдена квадратная СДР порядка N, то, по сути, задан класс эквивалентных СДР мощности (1).

Полный класс СДР можно представить в виде объединения классов эквивалентных СДР. Если произвольно выбрать из каждого $E(N)$-класса одну в качестве порождающей, из которой можно построить $E(N)$-класс СДР, то сформируется класс порождающих СДР — $\Pi(N)$-класс.

Впервые порождающий $\Pi(N)$-класс СДР был использован в методе защиты информации [3] при описании блок-схемы криптографической передачи информации и в модифицированном методе криптографической передачи информации [4].

Метод криптографической передачи информации, приведенный в [3, 4] заключается в том, что генератор порождающего класса СДР, управляемый генератором случайных чисел, генерирует очередную СДР $\Pi(N)$-класса, которая используется как опорная для передачи информации. Кодирование очередного символа из некоторого конечного множества — алфавита осуществляется с помощью одной СДР из эквивалентного $E(N)$-класса, построенного из опорной СДР. Количество сдвигов строк и столбцов СДР соответствует коду очередного символа. В канале связи совершенные двоичные решетки никогда не должны повторяться и таким образом максимально возможное сообщение, которое можно передать с помощью данного криптографического метода без смены ключа, определяется мощностью порождающего класса СДР.

К сожалению, известные методы синтеза СДР не позволяют синтезировать порождающие классы СДР многих порядков $N = 3 \cdot 2^k$. Более того, в настоящее время неизвестна мощность таких классов СДР. Так только в [5] приведен алгоритм построения порождающего класса СДР порядка $N = 3 \cdot 2^1 = 6$ и определена его мощность.

Постановка задачи

Целью данной работы является разработка конструктивного метода построения порождающего класса совершенных двоичных решеток квадратной формы порядка $N = 12$ для криптографической передачи информации, который основан на учете структурных и корреляционных свойств СДР и их прореженных матриц, а также нахождение оценки мощности порождающего класса СДР данного порядка.

Решение задачи

Известно, что произвольная СДР квадратной формы $\mathbf{H}(N) = \|h_{i,j}\|$, где $h_{i,j} \in \{\pm 1\}$ — элементы СДР, может быть прорежена по пространственным координатам [2, 5] для получения матриц размерности $N/2 \times N/2$

$$\left.\begin{aligned}
&\mathbf{A}(N/2)=\left\|a_{m,n}\right\|=\left\|h_{2i,2j}\right\|,\\
&\mathbf{B}(N/2)=\left\|b_{m,n}\right\|=\left\|h_{2i,2j+1}\right\|,\\
&\mathbf{C}(N/2)=\left\|c_{m,n}\right\|=\left\|h_{2i+1,2j}\right\|,\\
&\mathbf{D}(N/2)=\left\|d_{m,n}\right\|=\left\|h_{2i+1,2j+1}\right\|,
\end{aligned}\right\},\quad \left.\begin{aligned}
&i=\overline{0,N/2-1},\ m=\overline{0,N/2-1},\\
&j=\overline{0,N/2-1},\ n=\overline{0,N/2-1}
\end{aligned}\right\}, \tag{2}$$

которые будут называться прореженными. Они могут быть как прямыми, так и инверсными. Черта над именем прореженной матрицы будет обозначать ее инверсию, т.е. замену элементов матрицы "+1" на "–1" и наоборот.

Метод построения порождающего класса СДР порядка $N=3\cdot 2^2=12$ основан на использовании прореженных матриц (2) порядка $N/2=6$. Поэтому, вначале рассмотрим алгоритм формирования прореженных матриц порядка $N/2=6$, а затем метод создания СДР порождающего класса порядка $N=12$ на основе построенных прореженных матриц.

Алгоритм формирования прореженных матриц СДР порядка $N/2=6$ основан на использовании прореженных матриц $\mathbf{A}(N/4)$, $\mathbf{B}(N/4)$, $\mathbf{C}(N/4)$ и $\mathbf{D}(N/4)$ порядка $N/4=3$.

Исходными данными для построения прореженных матриц порядка $N/2=6$ являются прореженные матрицы порядка $N/4=3$ [5]

$$\mathbf{A}(3)=\begin{bmatrix}-&-&-\\+&+&+\\+&+&+\end{bmatrix},\ \mathbf{B}(3)=\begin{bmatrix}-&+&+\\-&+&+\\-&+&+\end{bmatrix},\ \mathbf{C}(3)=\begin{bmatrix}-&+&+\\+&-&+\\+&+&-\end{bmatrix},\ \mathbf{D}(3)=\begin{bmatrix}+&+&-\\+&-&+\\-&+&+\end{bmatrix}, \tag{3}$$

где символом "+" обозначено значение элемента СДР "+1", а символом "–" — значение элемента "–1" (для краткости). В дальнейшем в примерах, будут использоваться аналогичные обозначения.

Прореженные матрицы порядка $N/2=6$ необходимо создать по трем алгоритмам, получив 3 группы прореженных матриц $\mathbf{A}(6)$, $\mathbf{B}(6)$, $\mathbf{C}(6)$ и $\mathbf{D}(6)$. Для указания принадлежности определенной прореженной матрицы к конкретной группе введены обозначения: номер группы — верхний индекс, номер прореженной матрицы в группе — нижний. Индексы изменяются от нуля, поэтому $\mathbf{A}_1^0(6)$ — вторая прореженная матрица $\mathbf{A}(6)$ первой группы размера 6×6. Если не указан нижний индекс, соответствующее утверждение относится к любой прореженной матрице в группе, а если верхний — к матрице любой группы.

Прореженные матрицы $\mathbf{A}(6)$, $\mathbf{B}(6)$, $\mathbf{C}(6)$ и $\mathbf{D}(6)$ строятся по следующим шести выражениям, которые разбиты на два столбца

$$\left.\begin{array}{ll}
\mathbf{A}(3),\mathbf{B}(3) & \mathbf{C}(3),\overline{\mathbf{D}}(3)\\
\mathbf{A}(3),\mathbf{C}(3) & \mathbf{B}(3),\overline{\mathbf{D}}(3)\\
\mathbf{A}(3),\mathbf{D}(3) & \mathbf{B}(3),\overline{\mathbf{C}}(3)\\
\mathbf{B}(3),\mathbf{C}(3) & \mathbf{A}(3),\overline{\mathbf{D}}(3)\\
\mathbf{B}(3),\mathbf{D}(3) & \mathbf{A}(3),\overline{\mathbf{C}}(3)\\
\mathbf{C}(3),\mathbf{D}(3) & \mathbf{A}(3),\overline{\mathbf{B}}(3)
\end{array}\right\}. \tag{4}$$

Рассмотрим построение прореженных матриц $\mathbf{A}(6)$, $\mathbf{B}(6)$, $\mathbf{C}(6)$ и $\mathbf{D}(6)$ отдельно по каждому алгоритму.

Алгоритм первый. Каждая прореженная матрица первой группы $\mathbf{A}_0^0(6)$, $\mathbf{A}_1^0(6)$, $\mathbf{A}_2^0(6)$, $\mathbf{A}_3^0(6)$, $\mathbf{A}_4^0(6)$, $\mathbf{A}_5^0(6)$ формируется одним и тем же способом для соответствующей комбинации прореженных матриц первого столбца из (4)

$$\left.\begin{matrix}\mathbf{A}(3)\mathbf{B}(3)\\ \mathbf{A}(3)\mathbf{C}(3)\\ \mathbf{A}(3)\mathbf{D}(3)\\ \mathbf{B}(3)\mathbf{C}(3)\\ \mathbf{B}(3)\mathbf{D}(3)\\ \mathbf{C}(3)\mathbf{D}(3)\end{matrix}\right\}. \qquad (5)$$

Для первой комбинации $\mathbf{A}(3)\mathbf{B}(3)$ из исходных прореженных матриц (3)

$$\mathbf{A}(3)=\left\|a_{i,j}\right\|=\begin{bmatrix}-&-&-\\+&+&+\\+&+&+\end{bmatrix} \text{ и } \mathbf{B}(3)=\left\|b_{i,j}\right\|=\begin{bmatrix}-&+&+\\-&+&+\\-&+&+\end{bmatrix} \qquad (6)$$

с использованием операции перемежения столбцов формируется вспомогательная прямоугольная матрица размерности 3×6

$$\mathbf{X}_0^0(3,6)=\left\|x_{m,n}\right\|=\begin{bmatrix}-&-&-&+&-&+\\+&-&+&+&+&+\\+&-&+&+&+&+\end{bmatrix},$$

где $m=\overline{0,3}$ — номера строк;

$n=\overline{0,6}$ — номера столбцов.

Элементы вспомогательной матрицы $\mathbf{X}_0^0(3,6)$ определяются по правилу

$$\left.\begin{matrix}x_{i,2j}=a_{i,j}\\ x_{i,2j+1}=b_{i,j}\end{matrix}\right\},\ i=\overline{0,3-1},\ j=\overline{0,3-1}.$$

Затем путем применения операции циклического сдвига вниз на одну строку вспомогательной матрицы $\mathbf{X}_0^0(3,6)$ строится вспомогательная матрица $\mathbf{Y}_0^0(3,6)$

$$\mathbf{Y}_0^0(3,6)=\begin{bmatrix}+&-&+&+&+&+\\-&-&-&+&-&+\\+&-&+&+&+&+\end{bmatrix}.$$

Используя операцию перемежения строк вспомогательных матриц $\mathbf{X}_0^0(3,6)$ и $\mathbf{Y}_0^0(3,6)$

$$\left.\begin{matrix}a_{2i,j}=x_{i,j}\\ a_{2i+1,j}=y_{i,j}\end{matrix}\right\},\ i=\overline{0,3-1},\ j=\overline{0,6-1}$$

получаем прореженную матрицу $\mathbf{A}_0^0(6)$.

По первому правилу можно построить шесть прореженных матриц $\mathbf{A}^0(3)$ – по одной матрице для каждой комбинации матриц из (5). Представим построенную прореженную матрицу $\mathbf{A}_0^0(6)$ и остальные, полученные по остальным пяти комбинациям матриц из (5)

$$\mathbf{A}_0^0(6)=\begin{bmatrix}-&-&-&+&-&+\\+&-&+&+&+&+\\+&-&+&+&+&+\\-&-&-&+&-&+\\+&-&+&+&+&+\\+&-&+&+&+&+\end{bmatrix},\ \mathbf{A}_1^0(6)=\begin{bmatrix}-&-&-&+&-&+\\+&+&+&+&+&-\\+&+&+&-&+&+\\-&-&-&+&-&+\\+&+&+&+&+&-\\+&+&+&-&+&+\end{bmatrix},\ \mathbf{A}_2^0(6)=\begin{bmatrix}-&+&-&+&-&-\\+&-&+&+&+&+\\+&+&+&-&+&+\\-&+&-&+&-&-\\+&-&+&+&+&+\\+&+&+&-&+&+\end{bmatrix},$$

$$\mathbf{A}_3^0(6)=\begin{bmatrix}-&-&+&+&+&+\\-&+&+&+&+&-\\-&+&+&-&+&+\\-&-&+&+&+&+\\-&+&+&+&+&-\\-&+&+&-&+&+\end{bmatrix},\ \mathbf{A}_4^0(6)=\begin{bmatrix}-&+&+&+&+&-\\-&-&+&+&+&+\\-&+&+&-&+&+\\-&+&+&+&+&-\\-&-&+&+&+&+\\-&+&+&-&+&+\end{bmatrix},\ \mathbf{A}_5^0(6)=\begin{bmatrix}-&+&+&+&+&-\\+&-&+&+&-&+\\+&+&-&-&+&+\\-&+&+&+&+&-\\+&-&+&+&-&+\\+&+&-&-&+&+\end{bmatrix}.$$

Прореженные матрицы $\mathbf{C}^0(6)$ формируются так же, как и прореженные матрицы $\mathbf{A}^0(6)$, но вспомогательная матрица $\mathbf{Y}^0(3,6)$ в операции перемежения строк используется

инверсная.

Прореженные матрицы $\mathbf{B}^0(6)$ формируются так же, как и прореженные матрицы $\mathbf{A}^0(6)$, но в качестве исходных прореженных матриц выбираются матрицы из второго столбца (4)

$$\left.\begin{array}{l}\mathbf{C}(3)\overline{\mathbf{D}}(3)\\ \mathbf{B}(3)\overline{\mathbf{D}}(3)\\ \mathbf{B}(3)\overline{\mathbf{C}}(3)\\ \mathbf{A}(3)\overline{\mathbf{D}}(3)\\ \mathbf{A}(3)\overline{\mathbf{C}}(3)\\ \mathbf{A}(3)\mathbf{B}(3)\end{array}\right\}. \qquad (7)$$

Заметим, что в каждом выражении из (7) одна матрица всегда используется инверсная.

Прореженные матрицы $\mathbf{D}^0(6)$ строятся так же, как и прореженные матрицы $\mathbf{C}^0(6)$, в качестве исходных прореженных матриц выбираются прореженные матрицы из (7), а вспомогательная матрица $\mathbf{Y}^0(3,6)$ используется инверсная.

Алгоритм второй. Прореженные матрицы $\mathbf{A}^1(6)$ формируются отдельно для каждой из шести комбинаций прореженных матриц из (5).

Для первой комбинации из исходных прореженных матриц (3)

$$\mathbf{A}(3)=\left\|a_{i,j}\right\|=\begin{bmatrix}- & - & -\\ + & + & +\\ + & + & +\end{bmatrix} \text{ и } \mathbf{B}(3)=\left\|b_{i,j}\right\|=\begin{bmatrix}- & + & +\\ - & + & +\\ - & + & +\end{bmatrix},$$

с использованием операции перемежения строк

$$\left.\begin{array}{l}x_{2i,j}=a_{i,j}\\ x_{2i+1,j}=b_{i,j}\end{array}\right\},\ i=\overline{0,3-1},\ j=\overline{0,3-1},$$

формируем вспомогательную прямоугольную матрицу $\mathbf{X}_0^1(6,3)$

$$\mathbf{X}_0^1(6,3)=\left\|x_{m,n}\right\|=\begin{bmatrix}- & - & -\\ - & + & +\\ + & + & +\\ - & + & +\\ + & + & +\\ - & + & +\end{bmatrix}$$

размерности 6×3.

После этого путем применения операции циклического сдвига вправо на один столбец вспомогательной матрицы $\mathbf{X}_0^1(6,3)$ формируется вспомогательная матрицу $\mathbf{Y}_0^1(6,3)$

$$\mathbf{Y}_0^1(6,3)=\begin{bmatrix}- & - & -\\ + & - & +\\ + & + & +\\ + & - & +\\ + & + & +\\ + & - & +\end{bmatrix}.$$

С использованием операции перемежения столбцов

$$\left.\begin{array}{l}a_{2i,j}=x_{i,j}\\ a_{2i+1,j}=y_{i,j}\end{array}\right\},\ i=\overline{0,3-1},\ j=\overline{0,6-1}$$

для вспомогательных матриц $\mathbf{X}_0^1(6,3)$ и $\mathbf{Y}_0^1(6,3)$, формируется прореженная матрица $\mathbf{A}_0^1(6)$.

Для остальных выражений из (5) процесс построения прореженных матриц $\mathbf{A}_1^1(6)$, $\mathbf{A}_2^1(6)$, $\mathbf{A}_3^1(6)$, $\mathbf{A}_4^1(6)$, $\mathbf{A}_5^1(6)$ аналогичный. Представим все построенные матрицы

$$\mathbf{A}_0^1(6)=\begin{bmatrix}-&-&-&-&-&-\\-&+&+&-&+&+\\+&+&+&+&+&+\\-&+&+&-&+&+\\+&+&+&+&+&+\\-&+&+&-&+&+\end{bmatrix},\ \mathbf{A}_1^1(6)=\begin{bmatrix}-&-&-&-&-&-\\-&+&+&-&+&+\\+&+&+&+&+&+\\+&+&-&+&+&-\\+&+&+&+&+&+\\+&-&+&+&-&+\end{bmatrix},\ \mathbf{A}_2^1(6)=\begin{bmatrix}-&-&-&-&-&-\\+&-&+&+&-&+\\+&+&+&+&+&+\\+&+&-&+&+&-\\+&+&+&+&+&+\\-&+&+&-&+&+\end{bmatrix},$$

$$\mathbf{A}_3^1(6)=\begin{bmatrix}-&+&+&-&+&+\\-&+&+&-&+&+\\-&+&+&-&+&+\\+&+&-&+&+&-\\-&+&+&-&+&+\\+&-&+&+&-&+\end{bmatrix},\ \mathbf{A}_4^1(6)=\begin{bmatrix}-&+&+&-&+&+\\+&-&+&+&-&+\\-&+&+&-&+&+\\+&+&-&+&+&-\\-&+&+&-&+&+\\-&+&+&-&+&+\end{bmatrix},\ \mathbf{A}_5^1(6)=\begin{bmatrix}-&+&+&-&+&+\\+&-&+&+&-&+\\+&+&-&+&+&-\\+&+&-&+&+&-\\+&-&+&+&-&+\\-&+&+&-&+&+\end{bmatrix}.$$

Прореженные матрицы $\mathbf{C}^1(6)$ формируются, как и прореженные матрицы $\mathbf{A}^1(6)$, но вспомогательная матрица $\mathbf{Y}^1(6,3)$ используется инверсная. Прореженные матрицы $\mathbf{B}^1(6)$ создаются, как и прореженные матрицы $\mathbf{A}^1(6)$, но в качестве исходных прореженных матриц выбираются матрицы из (7), при этом вспомогательная матрица $\mathbf{Y}^1(6,3)$ используется прямая. Прореженные матрицы $\mathbf{D}^1(6)$ формируются, как и прореженные матрицы $\mathbf{C}^1(6)$, но вспомогательная матрица $\mathbf{Y}^1(6,3)$ используется инверсная.

Алгоритм третий. Прореженные матрицы $\mathbf{A}^2(6)$ формируются так же, как и прореженные матрицы $\mathbf{A}^0(6)$ по первому алгоритму, но во вспомогательной матрице $\mathbf{Y}^2(3,6)$ переставляются блоки половинок матрицы $\mathbf{Y}^0(3,6)$. Например, из

$$\mathbf{Y}_0^0(3,6)=\left[\begin{array}{ccc|ccc}+&-&+&+&+&+\\-&-&-&+&-&+\\+&-&+&+&+&+\end{array}\right],\ \text{получают}\ \mathbf{Y}_0^2(3,6)=\left[\begin{array}{ccc|ccc}+&+&+&+&-&+\\+&-&+&-&-&-\\+&+&+&+&-&+\end{array}\right]=\begin{bmatrix}+&+&+&+&-&+\\+&-&+&-&-&-\\+&+&+&+&-&+\end{bmatrix}.$$

Для исходных прореженных матриц из (2) получаем

$$\mathbf{A}_0^2(6)=\begin{bmatrix}-&-&-&+&-&+\\+&+&+&+&-&+\\+&-&+&+&+&+\\+&-&+&-&-&-\\+&-&+&+&+&+\\+&+&+&+&-&+\end{bmatrix},\ \mathbf{A}_1^2(6)=\begin{bmatrix}-&-&-&+&-&+\\+&+&-&+&+&+\\+&+&+&-&+&+\\+&-&+&-&-&-\\+&+&+&+&+&-\\-&+&+&+&+&+\end{bmatrix},\ \mathbf{A}_2^2(6)=\begin{bmatrix}-&+&-&+&-&-\\+&+&+&+&-&+\\+&+&+&-&+&+\\+&-&-&-&+&-\\+&-&+&+&+&+\\-&+&+&+&+&+\end{bmatrix},$$

$$\mathbf{A}_3^2(6)=\begin{bmatrix}-&-&+&+&+&+\\+&+&-&-&+&+\\-&+&+&-&+&+\\+&+&+&-&-&+\\-&+&+&+&+&-\\-&+&+&-&+&+\end{bmatrix},\ \mathbf{A}_4^2(6)=\begin{bmatrix}-&+&+&+&+&-\\+&+&+&-&-&+\\-&+&+&-&+&+\\+&+&-&-&+&+\\-&-&+&+&+&+\\-&+&+&-&+&+\end{bmatrix},\ \mathbf{A}_5^2(6)=\begin{bmatrix}-&+&+&+&+&-\\+&-&+&+&-&+\\+&+&-&-&+&+\\+&+&-&-&+&+\\+&-&+&+&-&+\\-&+&+&+&+&-\end{bmatrix}.$$

Прореженные матрицы $\mathbf{C}^2(6)$ создаются так же, как и прореженные матрицы $\mathbf{A}^2(6)$, но помимо перестановки блоков половинок матрицы $\mathbf{Y}^0(3,6)$, матрица $\mathbf{Y}^2(3,6)$ инвертируется. Прореженные матрицы $\mathbf{B}^2(6)$ строятся, как и прореженные матрицы $\mathbf{A}^2(6)$, но в качестве исходных выбираются комбинации прореженных матриц из (7). Для формирования вспомогательных матриц $\mathbf{Y}^2(3,6)$ выполняются перестановки блоков половинок матриц $\mathbf{Y}^2(3,6)$, а сами прореженные матрицы используются прямые. Прореженные матрицы $\mathbf{D}^2(6)$ формируются, как и прореженные матрицы $\mathbf{A}^2(6)$, но после перестановки блоков половинок матриц $\mathbf{Y}^0(3,6)$, матрица $\mathbf{Y}^2(6,3)$ инвертируется.

Таким образом, по каждому из трех алгоритмов, получено по 6 прореженных матриц $\mathbf{A}^0(6)$, $\mathbf{A}^1(6)$, $\mathbf{A}^2(6)$, $\mathbf{B}^0(6)$, $\mathbf{B}^1(6)$, $\mathbf{B}^2(6)$, $\mathbf{C}^0(6)$, $\mathbf{C}^1(6)$, $\mathbf{C}^2(6)$, $\mathbf{D}^0(6)$, $\mathbf{D}^1(6)$ и $\mathbf{D}^2(6)$ которые сведены в табл. 1.

Таблица 1

Прореженные матрицы порядка $N/2=6$

Первая группа				Вторая группа			
Первая пара		Вторая пара		Первая пара		Вторая пара	
$\mathbf{A}^0(6)$	$\mathbf{B}^0(6)$	$\mathbf{C}^0(6)$	$\mathbf{D}^0(6)$	$\mathbf{A}^1(6)$	$\mathbf{B}^1(6)$	$\mathbf{C}^1(6)$	$\mathbf{D}^1(6)$
− − − + − +	− − + − + +	− − − + − +	− − + − + +	− − − − − −	− + + − + +	− + − + − +	− − + + + −
+ − + + + +	+ + + − − −	− + − − − −	− − − + + +	− + + − + +	− + − − + −	− − + + + −	− − − + + +
+ − + + + +	+ − − + + −	+ − + + + +	+ − − + + −	+ + + + + +	+ + − + + −	+ − + − + −	+ − − − + +
− − − + − +	− − + − + +	+ + + − + −	+ + − + − −	− + + − + +	− − + − − +	− − + + + −	− + + + − −
+ − + + + +	+ + + − − −	+ − + + + +	+ + + − − −	+ + + + + +	+ − + + − +	+ − + − + −	+ + + − − −
+ − + + + +	+ − − + + −	− + − − − −	− + + − − +	− + + − + +	+ − − + − −	− − + + + −	+ + − − − +
− − − + − +	− − + − + +	− − − + − +	− − + − + +	− − − − − −	− + + − + +	− + − + − +	− − + + + −
+ + + + + −	− + + − + −	− − − − − +	+ − − + − +	− + + − + +	− + − − + −	− − + + + −	− − − + + +
+ + + − + +	− − + + + −	+ + + − + +	− − + + + −	+ + + + + +	− + + − + +	+ − + − + −	− − + + + −
− − − + − +	− − + − + +	+ + + − + −	+ + − + − −	+ + − + + −	− − + − − +	+ − − − + +	− + + + − −
+ + + + + −	− + + − + −	+ + + + + −	− + + − + −	+ + + + + +	− + + − + +	+ − + − + −	− − + + + −
+ + + − + +	− − + + + −	− − − + − −	+ + − − − +	+ − + + − +	+ − − + − −	+ + + − − −	+ + − − − +
− + − + − −	− + + − + −	− + − + − −	− + + − + −	− − − − − −	− + + − + +	− + − + − +	− − + + + −
+ − + + + +	− − + − + +	− + − − − −	+ + − + − −	+ − + + − +	+ − − + − −	+ + + − − −	+ + − − − +
+ + + − + +	− − + + + −	+ + + − + +	− − + + + −	+ + + + + +	− + + − + +	+ − + − + −	− − + + + −
− + − + − −	− + + − + −	+ − + − + +	+ − − + − +	+ + − + + −	− − + − − +	+ − − − + +	− + + + − −
+ − + + + +	− − + − + +	+ − + + + +	− − + − + +	+ + + + + +	− + + − + +	+ − + − + −	− − + + + −
+ + + − + +	− − + + + −	− − − + − −	+ + − − − +	− + + − + +	− + − − + −	− − + + + −	− − − + + +
− − + + + +	− − − − − +	− − + + + +	− − − − − +	− + + − + +	− − − − − −	− − + + + −	− + − + − +
− + + + + −	+ + + − + −	+ − − − − +	− − − + − +	− + + − + +	− + − − + −	− − + + + −	− − − + + +
− + + − + +	+ − + + + −	− + + − + +	+ − + + + −	− + + − + +	+ + + + + +	− − + + + −	+ − + − + −
− − + + + +	− − − − − +	+ + − − − −	+ + + + + −	+ + − + + −	− − + − − +	+ − − − + +	− + + + − −
− + + + + −	+ + + − + −	− + + + + −	+ + + − + −	− + + − + +	+ + + + + +	− − + + + −	+ − + − + −
− + + − + +	+ − + + + −	+ − − + − −	− + − − − +	+ − + + − +	+ − − + − −	+ + + − − −	+ + − − − +
− + + + + −	− + − − − −	− + + + + −	− + − − − −	− + + − + +	− − − − − −	− − + + + −	− + − + − +
− − + + + +	+ − + − + +	+ + − − − −	− + − + − −	+ − + + − +	+ − − + − −	+ + + − − −	+ + − − − +
− + + − + +	+ − + + + −	− + + − + +	+ − + + + −	− + + − + +	+ + + + + +	− − + + + −	+ − + − + −
− + + + + −	− + − − − −	+ − − − − +	+ − + + + +	+ + − + + −	− − + − − +	+ − − − + +	− + + + − −
− − + + + +	+ − + − + +	− − + + + +	+ − + − + +	− + + − + +	+ + + + + +	− − + + + −	+ − + − + −
− + + − + +	+ − + + + −	+ − − + − −	− + − − − +	− + + − + +	− + − − + −	− − + + + −	− − − + + +
− + + + + −	− + − − − −	− + + + + −	− + − − − −	− + + − + +	− − − − − −	− − + + + −	− + − + − +
+ − + + − +	+ + + − + −	− + − − + −	− − − + − +	+ − + + − +	+ − − + − −	+ + + − − −	+ + − − − +
+ + − − + +	+ + + − + −	+ + − − + +	+ + + − + −	+ + − + + −	+ + + + + +	+ − − − + +	+ − + − + −
− + + + + −	− + − − − −	+ − − − − +	+ − + + + +	+ + − + + −	+ − − + − −	+ − − − + +	+ + − − − +
+ − + + − +	+ + + − + −	+ − + + − +	+ + + − + −	+ − + + − +	+ + + + + +	+ + + − − −	+ − + − + −
+ + − − + +	+ + + − + −	− − + + − −	− − − + − +	− + + − + +	+ − − + − −	− − + + + −	+ + − − − +
Третья группа							
Первая пара		Вторая пара		Первая пара		Вторая пара	
$\mathbf{A}^2(6)$	$\mathbf{B}^2(6)$	$\mathbf{C}^2(6)$	$\mathbf{D}^2(6)$	$\mathbf{A}^2(6)$	$\mathbf{B}^2(6)$	$\mathbf{C}^2(6)$	$\mathbf{D}^2(6)$
− − − + − +	− − + − + +	− − − + − +	− − + − + +	− − + + + +	− − − − − +	− − + + + +	− − − − − +
+ + + + − +	− − − + + +	− − − − + −	+ + + − − −	+ + − − + +	− + − + + +	− − + + − −	+ − + − − −
+ − + + + +	+ − − + + −	+ − + + + +	+ − − + + −	− + + − + +	+ − + + + −	− + + − + +	+ − + + + −
+ − + − − −	− + + − − +	− + − + + +	+ − − + + −	+ + + − − +	− − + − − −	− − − + + −	+ + − + + +
+ − + + + +	+ + + − − −	+ − + + + +	+ + + − − −	− + + + + −	+ + + − + −	− + + + + −	+ + + − + −
+ + + + − +	+ + − + − −	− − − − + −	− − + − + +	− + + − + +	+ + − + − +	+ − − + − −	− − + − + −
− − − + − +	− − + − + +	− − − + − +	− − + − + +	− + + + + −	− + − − − −	− + + + + −	− + − − − −
+ + − + + +	− + − − + +	− − + − − −	+ − + + − −	+ + + − − +	− + + + − +	− − − + + −	+ − − − + −
+ + + − + +	− − + + + −	+ + + − + +	− − + + + −	− + + − + +	+ − + + + −	− + + − + +	+ − + + + −
+ − + − − −	− + + − − +	− + − + + +	+ − − + + −	+ + − − + +	− − − − + −	− − + + − −	+ + + + − +
+ + + + + −	− + + − + −	+ + + + + −	− + + − + −	− − + + + +	+ − + − + +	− − + + + +	+ − + − + +
− + + + + +	+ + − − − +	+ − − − − −	− − + + + −	− + + − + +	+ + − + − +	+ − − + − −	− − + − + −
− + − + − −	− + + − + −	− + − + − −	− + + − + −	− + + + + −	− + − − − −	− + + + + −	− + − − − −
+ + + + − +	− + + − − +	− − − − + −	+ − − + + −	+ − + + − +	− + − + + +	− + − − + −	+ − + − − −
+ + + − + +	− − + + + −	+ + + − + +	− − + + + −	+ + − − + +	+ + + − + −	+ + − − + +	+ + + − + −
+ − − − + −	− + − − + +	− + + + − +	+ − + + − −	+ + − − + +	− − − − + −	− − + + − −	+ + + + − +
+ − + + + +	− − + − + +	+ − + + + +	− − + − + +	+ − + + − +	+ + + − + −	+ − + + − +	+ + + − + −
− + + + + +	+ + − − − +	+ − − − − −	− − + + + −	− + + + + −	− + − + + +	+ − − − − +	+ − + − − −

Исследованиями установлено, что для построения $\Pi(N)$-класса СДР порядка $N=12$ необходимо для каждой группы прореженных матриц из табл. 1 воспользоваться фиксированными конструкциями, представленными в табл. 2. Символ «$\Diamond$» обозначает перемежение (процедура обратная прореживанию (2)) соответствующих прореженных матриц. Возможны и другие структуры конструкций, однако в табл. 2 все конструкции имеют простейший (канонический) вид. Для построения порождающего класса, СДР, полученные по фиксированным конструкциям (табл. 2) необходимо инвертировать.

Табл. 2. Фиксированные конструкции прореженных матриц для построения порождающего класса СДР

$\mathbf{A}_0(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_0(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_0(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_1(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_1(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_1(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_2(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_2(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_2(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_3(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_3(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_3(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_4(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_4(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_4(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_5(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_5(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_5(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_0(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_0(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_0(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_1(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_1(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_1(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_2(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_2(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_2(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_3(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_3(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_3(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_4(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_4(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_4(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)$
$\mathbf{A}_5(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{D}_k(6)$	$\mathbf{A}_5(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{B}_i(6)\Diamond\mathbf{C}_j(6)$	$\mathbf{A}_5(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{B}_i(6)$

Прежде чем приступить к созданию порождающего класса совершенных двоичных решеток полученные прореженные матрицы (табл. 1) необходимо размножить.

Матрицы $\mathbf{A}_0(6)$, $\mathbf{A}_1(6)$, $\mathbf{A}_2(6)$, $\mathbf{A}_3(6)$, $\mathbf{A}_4(6)$ и $\mathbf{A}_5(6)$ зафиксированы, как указано в табл. 2, и не размножаются. Прореженные матрицы $\mathbf{B}(6)$ из всех трех групп размножаются с помощью операций циклического сдвига строк и столбцов. Количество возможных циклических сдвигов строк для первой группы — три $(\overline{0,2})$, а столбцов — шесть $(\overline{0,5})$. Количество возможных циклических сдвигов строк для второй группы — шесть $(\overline{0,5})$, а столбцов — три $(\overline{0,2})$. Для прореженных матриц $\mathbf{B}(6)$ из третьей группы возможны два варианта выполнения циклических сдвигов: либо по строкам — три $(\overline{0,2})$ сдвига, а столбцам — шесть $(\overline{0,5})$, либо по строкам — шесть $(\overline{0,5})$ сдвигов, а столбцам — три $(\overline{0,2})$. И, таким образом, в результате размножения из каждой матрицы $\mathbf{B}(6)$ для каждой группы получим их мощность

$$\Psi_{\mathbf{B}(6)}=18. \tag{8}$$

Прореженные матрицы $\mathbf{C}(6)$ и $\mathbf{D}(6)$ сформированные по трем алгоритмам размножаются с помощью операций циклического сдвига строк и столбцов. Количество возможных циклических сдвигов по строкам и столбцам — шесть $(\overline{0,5})$. Таким образом, в результате размножения из каждой прореженной матрицы $\mathbf{C}(6)$ и $\mathbf{D}(6)$ получим

$$\Psi_{\mathbf{C}(6)}=\Psi_{\mathbf{D}(6)}=36 \tag{9}$$

матриц.

Следует заметить, что существуют некоторые ограничения на использование комбинаций прореженных матриц при построении СДР порождающего класса (табл. 2):

– можно использовать только комбинации прореженных матриц, построенные по одному алгоритму или полученных в результате их размножения; например, $\mathbf{A}^0(N/2)$, $\mathbf{B}^0(N/2)$, $\mathbf{C}^0(N/2)$ и $\mathbf{D}^0(N/2)$ или $\mathbf{A}^2(N/2)$, $\mathbf{B}^2(N/2)$, $\mathbf{C}^2(N/2)$ и $\mathbf{D}^2(N/2)$;

– прореженные матрицы $\mathbf{A}(N/2)$ и $\mathbf{B}(N/2)$, построенных по одной комбинации из (5) или полученных в результате размножения, используются только совместно; например, $\mathbf{A}_2^0(N/2)$ и $\mathbf{B}_2^0(N/2)$ или $\mathbf{A}_4^1(N/2)$ и $\mathbf{B}_4^1(N/2)$. Количество таких комбинаций с учетом того, что матрицы $\mathbf{A}(6)$ зафиксированы (табл. 2) и (8) определяется выражением

$$\Psi_{\mathbf{A}(6)\mathbf{B}(6)} = \Psi_{\mathbf{A}^0(6)} \cdot \Psi_{\mathbf{B}^0(6)} = \Psi_{\mathbf{A}^1(6)} \cdot \Psi_{\mathbf{B}^1(6)} = \Psi_{\mathbf{A}^2(6)} \cdot \Psi_{\mathbf{B}^2(6)} = 18 \qquad (10)$$

– используются только вместе и прореженные матрицы $\mathbf{C}(N/2)$ и $\mathbf{D}(N/2)$ сформированные по одной комбинации из (7) или полученных в результате их размножения; например, $\mathbf{C}_3^2(N/2)$ и $\mathbf{D}_3^2(N/2)$ или $\mathbf{C}_5^1(N/2)$ и $\mathbf{D}_5^1(N/2)$; количество таких сочетаний для одной комбинации (7) с учетом (9)

$$\Psi_{\mathbf{C}(6)}\Psi_{\mathbf{D}(6)} = \Psi_{\mathbf{C}^0(6)}\Psi_{\mathbf{D}^0(6)} = \Psi_{\mathbf{C}^1(6)}\Psi_{\mathbf{D}^1(6)} = \Psi_{\mathbf{C}^2(6)}\Psi_{\mathbf{D}^2(6)} = 36 \cdot 36,$$

а с учетом шести комбинаций из (7)

$$\Psi_{\mathbf{C}(6)\mathbf{D}(6)} = 6 \cdot \Psi_{\mathbf{C}(6)}\Psi_{\mathbf{D}(6)}; \qquad (11)$$

– прореженные матрицы $\mathbf{A}(N/2)$ и $\mathbf{B}(N/2)$ сформированные по одной комбинации из (4), или матрицы, полученные в результате их размножения, можно использовать с прореженными матрицами $\mathbf{C}(N/2)$ и $\mathbf{D}(N/2)$, сформированными по другой комбинации из (4), но при этом они все должны быть построены по одному алгоритму; например, $\mathbf{A}_4^1(N/2)$, $\mathbf{B}_4^1(N/2)$, $\mathbf{C}_5^1(N/2)$ и $\mathbf{D}_5^1(N/2)$.

В качестве примера с использованием процедуры перемежения, обратной процедуре прореживания (2), сформирована СДР $\mathbf{H}_0(12)$ для прореженных матриц $\mathbf{A}_4^1(N/2)$, $\mathbf{B}_4^1(N/2)$, $\mathbf{C}_5^1(N/2)$ и $\mathbf{D}_5^1(N/2)$ по выражению (табл. 2) $\mathbf{A}_4(6)\Diamond\mathbf{B}_l(6)\Diamond\mathbf{C}_j(6)\Diamond\mathbf{D}_k(6)$ и СДР $\mathbf{H}_1(12)$ — по выражению $\mathbf{A}_4(6)\Diamond\mathbf{B}_l(6)\Diamond\mathbf{D}_k(6)\Diamond\mathbf{C}_j(6)$

$$\mathbf{H}_0(12) = \begin{bmatrix} - & - & + & - & + & - & - & - & + & - & + & - \\ - & - & - & + & + & - & + & + & + & - & - & + \\ + & + & - & - & + & - & + & + & - & - & + & - \\ + & + & + & + & + & - & - & - & - & - & - & + \\ - & + & + & + & + & + & - & + & + & + & + & + \\ + & + & - & - & - & + & - & - & + & + & + & - \\ + & - & + & - & - & + & + & - & + & - & - & + \\ + & + & - & + & - & - & - & - & + & - & + & + \\ - & + & + & + & + & + & - & + & + & + & + & + \\ + & + & + & - & + & + & - & - & - & + & - & - \\ - & - & + & + & + & - & - & - & + & + & + & - \\ - & + & - & + & + & - & + & - & + & - & - & + \end{bmatrix}, \quad \mathbf{H}_1(12) = \begin{bmatrix} - & - & + & - & + & - & - & - & + & - & + & - \\ - & - & + & - & - & + & + & + & - & + & + & - \\ + & + & - & - & + & - & + & + & - & - & + & - \\ + & + & + & + & - & + & - & - & - & - & + & - \\ - & + & + & + & + & + & - & + & + & + & + & + \\ + & + & - & - & + & - & - & - & + & + & - & + \\ + & - & + & - & - & + & + & - & + & - & - & + \\ + & + & + & - & - & - & - & - & - & + & + & + \\ - & + & + & + & + & + & - & + & + & + & + & + \\ + & + & - & + & + & + & - & - & + & - & - & - \\ - & - & + & + & + & - & - & - & + & + & + & - \\ + & - & + & - & - & + & - & + & - & + & + & - \end{bmatrix}.$$

Мощность порождающего класса совершенных двоичных решеток размера 12×12

$$\Psi = 2 \cdot 3 \cdot 36 \cdot \Psi_{\mathbf{A}(6)\mathbf{B}(6)} \cdot \Psi_{\mathbf{C}(6)\mathbf{D}(6)}, \qquad (12)$$

где 2 — коэффициент учитывающий инверсию СДР;

3 — количество алгоритмов построения прореженных матриц;

36 — количество фиксированных конструкций (табл. 2).

Числовое значение мощности СДР порождающего П(12)-класса порядка $N=12$, созданных по предложенному конструктивному методу, после подстановки в (12) значения выражений (10), (11)

$$\Psi = 2\cdot 3\cdot 36\cdot \Psi_{A(6)B(6)}\cdot 6\cdot \Psi_{C(6)}\cdot \Psi_{D(6)} = 2\cdot 3\cdot 36\cdot 18\cdot 6\cdot 36\cdot 36 = 2^9 3^{10} = 30\,233\,088$$

матриц.

Заключение

Такие огромные мощности класса порождающих СДР порядка $N=12$ привлекательны для криптографической передачи данных, так как позволяют передать большой объем информации. Так произведение Л.Н. Толстого «Война и мир» содержит 3 198 976 символов и это произведение, без смены ключа, описанным криптографическим методом, можно передать 9,45 раз. В дальнейшем предстоит разработать алгоритмы построения порождающих классов больших порядков.

Список литературы

1. Chan, W.K. Summary of perfect $s\times t$ arrays, $1\le s\le t\le 100$ / W.K. Chan, M.K. Siu // Electronics letters. — 1991. — Vol. 27 № 9. — P. 709—710.

2. Мазурков, М.И. Классы эквивалентных и порождающих совершенных двоичных решеток для CDMA-технологий / М.И. Мазурков, В.Я. Чечельницкий // Изв. вузов Радиоэлектроника. — 2003. — № 5. — С. 54—63.

3. Мазурков, М.И. Метод защиты информации на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Изв. вузов Радиоэлектроника. — 2008. — № 11. — С. 53—57.

4. Чечельницкий, В.Я. Метод криптографической передачи данных на основе совершенных двоичных решеток / В.Я. Чечельницкий, П. Мурр // Защита информации. — 2008. — № 2(38). — С. 32—38.

5. Мазурков, М.И Свойства полного класса совершенных двоичных решеток на 36 элементов / М.И. Мазурков, В.Я. Чечельницкий // Изв. вузов Радиоэлектроника. — 2004. — № 6. — С. 56—64.

Предложен конструктивный метод построения порождающего класса совершенных двоичных решеток размера 12x12 для криптографической передачи информации и получена оценка его мощности.
Ключевые слова: совершенные двоичные решетки, порождающий класс, криптография.

Запропоновано конструктивний метод побудови породжуючого класу досконалих двійкових решіток розміру 12x12 для криптографічного передачі інформації та знайдено оцінку його потужності.

A constructive method which generates a class of perfect binary arrays size 12x12 for cryptographic information transfer and obtain an estimate of its power.

Рецензент: Хорошко В.О.
Надійшла 27.05.2010

УДК 004.056.5

Борисенко И.И. (ОНПУ)

МОДЕЛИ ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИОННОГО КОНТЕЙНЕРА И АНАЛИЗ СОСТОЯНИЯ ЕГО ЗАЩИЩЕННОСТИ

Введение

В настоящее время количество областей, в которых средства электронной связи заменяют бумажную переписку, быстро увеличивается. В результате увеличивается и доступный для перехвата объем информации (носящий конфиденциальный характер), а сам перехват становится более легким [1]. Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии, которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде и представляют собой