КРАТКИЕ СООБЩЕНИЯ

УДК [517.938 + 519.713 / .718]: 621.398

А. В. Ушаков, Е. С. Яицкая

МОДИФИКАЦИЯ МАТРИЦ СИСТЕМАТИЧЕСКИХ ПОМЕХОЗАЩИЩЕННЫХ КОДОВ В ЗАДАЧЕ ОБЕСПЕЧЕНИЯ СКРЫТНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

С помощью невырожденных матричных мультипликативных компонентов формируются банки образующих и проверочных матриц систематических помехозащищенных кодов.

Ключевые слова: *помехозащищенный код, образующая и проверочная матрицы, матричный мультипликативный компонент, скрытность.*

Рассматривается задача обеспечения скрытности передачи информации с помощью двоичных кодов, преобразование которых в функциональной среде „кодер—канал—декодер—коррекция“ осуществляется [1] в соответствии с векторно-матричными соотношениями

$$y = a\mathbf{G};\ f = y \oplus \xi;\ E = f\mathbf{H};\ \hat{\xi} = E\mathbf{H}^{+};\ \hat{y} = f \oplus \hat{\xi},$$

где a, y, ξ, f, E, $\hat{\xi}$, $\hat{y}$ — вектор-строки соответственно информационного (k) кода, помехозащищенного (n,k) кода (ПЗК), кода помехи в канальной среде (КС), искаженного в КС ПЗК, кода синдрома искажения, кода коррекции, откорректированного принятого из КС кода; $\mathbf{G}$ — $(k \times n)$-образующая и $\mathbf{H}$ — $(n \times m)$-проверочная матрицы ПЗК; $n - k = m$ — число проверочных разрядов ПЗК.

Утверждение 1. Пара $(\mathbf{G}, \mathbf{H})$ порождает ПЗК при необходимом условии

$$\mathbf{GH} = \mathbf{O}. \qquad \square\ (1)$$

Доказательство утверждения строится на использовании системы соотношений

$$y = a\mathbf{G}; f = y \oplus \xi; E = f\mathbf{H} = (y \oplus \xi)\mathbf{H} = (a\mathbf{G} \oplus \xi)\mathbf{H} = a\mathbf{GH} \oplus \xi\mathbf{H}\big|_{\xi=0} =$$

$$= a\mathbf{GH}\big|_{\forall a} = \mathbf{O} \to \mathbf{GH} = \mathbf{O}. \qquad \blacksquare$$

Утверждение 2. Умножение матриц $\mathbf{G}$ слева и $\mathbf{H}$ справа соответственно на невырожденные произвольные $(k \times k)$-матрицу $\mathbf{Q}$ и $(m \times m)$-матрицу $\mathbf{P}$ порождают матрицы $\tilde{\mathbf{G}} = \mathbf{QG}$ и $\tilde{\mathbf{H}} = \mathbf{HP}$. При этом

$$\tilde{\mathbf{G}}\tilde{\mathbf{H}} = \mathbf{O}. \qquad \square\ (2)$$

Доказательство строится на использовании условия (1) в цепочке равенств

$$\tilde{\mathbf{G}}\tilde{\mathbf{H}} = \mathbf{QGHP} = \mathbf{Q}(\mathbf{GH})\mathbf{P} = \mathbf{Q}(\mathbf{O})\mathbf{P} = \mathbf{O}. \qquad \blacksquare$$

Невырожденность матриц $\mathbf{Q}$ и $\mathbf{P}$ обеспечивается выбором их в виде:

1) матриц перестановок, при этом мощности получаемых множеств матриц составят величины $\left[\{\mathbf{Q}\}\right]=k!$, $\left[\{\mathbf{P}\}\right]=m!$;

2) $\mathbf{Q}=\mathbf{N}_{\mathbf{Q}}^{l_{\mathbf{Q}}}$, $l_{\mathbf{Q}}=\overline{0,\nu_{\mathbf{Q}}-1}$, и $\mathbf{P}=\mathbf{N}_{\mathbf{P}}^{l_{\mathbf{P}}}$, $l_{\mathbf{P}}=\overline{0,\nu_{\mathbf{P}}-1}$, где $(k\times k)$-матрица $\mathbf{N}_{\mathbf{Q}}$ и $(m\times m)$-матрица $\mathbf{N}_{\mathbf{P}}$ имеют соответственно характеристическими многочленами неприводимые, принадлежащие максимальным показателям [2] $\nu_{\mathbf{Q}}=\max\arg\left\{\mathbf{N}_{\mathbf{Q}}^{\nu_{\mathbf{Q}}}=\mathbf{I}\right\}=2^k-1$ и $\nu_{\mathbf{P}}=\max\arg\left\{\mathbf{N}_{\mathbf{P}}^{\nu_{\mathbf{P}}}=\mathbf{I}\right\}=2^m-1$, так что $\left[\{\mathbf{Q}\}\right]=2^k-1$, $\left[\{\mathbf{P}\}\right]=2^m-1$.

Процедура максимизации значений $\left[\{\mathbf{Q}\}\right]$ и $\left[\{\mathbf{P}\}\right]$ может быть осуществлена с помощью данных приводимой ниже таблицы.

$k\,(m)$	1	2	3	4	5	7	11	15	26
$k!(m!)$	1	2	6	24	120	5040	3,99+7	1,31E+12	4,03E+26
$2^k-1(2^m-1)$	1	3	7	15	31	127	2047	3,28E+4	6,71E+7

Предложенные процедуры проиллюстрируем примером $(n,k)=(7,4)$ — ПЗК с образующим многочленом $g(x)=x^3+x+1$. Код характеризуется [2] матрицами

$$\mathbf{G}=\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix},\quad \mathbf{H}=\begin{bmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix}^T.$$

Согласно данным таблицы матрицы $\mathbf{Q}$ и $\mathbf{P}$ строим соответственно в форме матрицы перестановок и процедуры:

$$\mathbf{Q}=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix},\quad \mathbf{P}=\mathbf{N}_{\mathbf{P}}^{l_{\mathbf{P}}}\Big|_{l_{\mathbf{P}}=4}=\begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix}^4=\begin{bmatrix}1&1&1\\0&1&1\\1&1&0\end{bmatrix},$$

так что образующая $\tilde{\mathbf{G}}$ и проверочная $\tilde{\mathbf{H}}$ матрицы получают представление

$$\tilde{\mathbf{G}}=\mathbf{QG}=\begin{bmatrix}0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\\1&0&0&0&1&0&1\end{bmatrix},\quad \tilde{\mathbf{H}}=\mathbf{HP}=\begin{bmatrix}0&0&1&1&1&0&1\\0&1&0&0&1&1&1\\1&0&0&1&1&1&0\end{bmatrix}^T.$$

При этом (см. таблицу) $\left[\left\{\tilde{\mathbf{G}},\tilde{\mathbf{H}}\right\}\right]=\left[\{\mathbf{Q}\}\right]\cdot\left[\{\mathbf{P}\}\right]=7\cdot 24=168$.

Основной результат. Полученные банки $\left\{\tilde{\mathbf{G}}\right\}$ и $\left\{\tilde{\mathbf{H}}\right\}$ модифицированных образующих $\tilde{\mathbf{G}}$ и проверочных $\tilde{\mathbf{H}}$ матриц порождают мощность $\left[\left\{\tilde{\mathbf{G}},\tilde{\mathbf{H}}\right\}\right]=\left[\{\mathbf{Q}\}\right]\cdot\left[\{\mathbf{P}\}\right]$ возможных реализаций помехозащитных преобразований кодов, что позволяет обеспечить частичную скрытность процесса передачи информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Ушаков А. В., Яицкая Е. С.* Рекуррентное систематическое помехозащитное преобразование кодов: возможности аппарата линейных двоичных динамических систем // Изв. вузов. Приборостроение. 2011. Т. 54, № 3. С. 17—25.

2. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976. 600 с.

Сведения об авторах

Анатолий Владимирович Ушаков — д-р техн. наук, профессор; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра систем управления и информатики;
E-mail: ushakov-AVG@yandex.ru

Елена Сергеевна Яицкая — аспирант; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра систем управления и информатики;
E-mail: yaitskayaes@mail.ru

Рекомендована кафедрой
систем управления и информатики

Поступила в редакцию
07.10.11 г.