УДК 621.372.037.372;621.391.26

МНОГОМЕРНОЕ ВЕКТОРНОЕ ПРЕДСТАВЛЕНИЕ МОМЕНТНЫХ ВЕЛИЧИН СИГНАЛА С ИХ КОРРЕЛЯЦИОННО-МАТРИЧНОЙ ОБРАБОТКОЙ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ

канд. техн. наук Д.С. РЯБЕНКО, С.В. ЛАВРОВ
(Полоцкий государственный университет)

Оценка защищенности речевой информации на всех стадиях жизненного цикла информационных систем и их составных элементов остается сложной научной задачей, несмотря на использование новых перспективных моделей помехоустойчивых сигналов с оптимальной их обработкой. Важнейшим средством обработки аналоговых и цифровых сигналов для оценки защиты речевой информации остается корреляционный метод [1].

Ключевые слова: *аналоговый и цифровой сигнал, корреляционный метод, матричная обработка.*

Корреляционная функция периодических процессов характеризует взаимную связь двух мгновенных значений различных сигналов с временным сдвигом τ [2]. Преобразование Фурье корреляционной функции определяет спектральное распределение средней мощности периодических сигналов и спектральное распределение энергии апериодических сигналов с конечной энергией [2]. Для двух действительных периодических процессов с одинаковой основной частотой его взаимная корреляционная функция

$$R_{v_1 v_2}(\tau) = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} v_1(t) v_2(t+\tau)\,\mathrm{d}t.$$

Важно, что взаимная корреляционная функция устанавливается по разности фаз исходных сигналов и разности фаз их соответствующих гармоник.

Коэффициент корреляции пары случайных величин является мерой линейной связи, т.е. с какой точностью одна величина может быть выражена через другую.

Коэффициент взаимной корреляции [3]

$$r(v_1, v_2) = \frac{R_{v_1 v_2}}{\sigma_{v_1}\sigma_{v_2}} = \frac{R_{v_1 v_2}}{\sqrt{R(v_1 \cdot v_1)\cdot R(v_2 \cdot v_2)}},$$

где $R_{v_1 v_2}$ – взаимная корреляционная функция;

σ^2 – дисперсия.

Совокупность двух или нескольких случайных величин является многомерным вектором [4] в виде матрицы порядка $n \times n$.

$$K = \begin{bmatrix} K_{11} & K_{12} & ... & K_{1n} \\ K_{21} & K_{22} & ... & K_{2n} \\ ... & ... & ... & ... \\ K_{n1} & K_{n2} & ... & K_{nn} \end{bmatrix}.$$

Члены, не лежащие на главной диагонали, представляют взаимную корреляционную функцию, связанные с составляющими векторного процесса. Члены, связанные с составляющими векторного процесса и находящиеся на главной диагонали, представляют автокорреляционную функцию (АКФ). АКФ является средней мощностью процесса $w(t)$.

Опираясь на симметричность корреляционной матрицы (1), ее представляют в виде

$$R_{ij} = \begin{bmatrix} R_{11} & R_{12} & ... & R_{1n} \\ & R_{22} & ... & R_{2n} \\ ... & ... & ... & ... \\ & & ... & R_{nn} \end{bmatrix}. \quad (1)$$

Если случайные величины X_1, X_2,… X_n попарно некоррелированы, т.е. $R_{ij} = 0$ при $i \neq j$, матрица принимает вид

$$R_{ij} = \begin{bmatrix} R_{11} & 0 & 0 & ... & 0 \\ & R_{22} & 0 & ... & 0 \\ & & R_{33} & ... & 0 \\ & & & ... & ... \\ & & & ... & R_{nn} \end{bmatrix}. \tag{2}$$

Единичную матрицу коэффициентов корреляции формируют из матрицы (2):

$$r_{ij} = \begin{bmatrix} 1 & r_{12} & ... & r_{1n} \\ & 1 & ... & r_{2n} \\ ... & ... & ... & ... \\ & & ... & 1 \end{bmatrix}, \tag{3}$$

Такую матрицу (3) называют диагональной.

В работе [5] представлены теоремы о числовых характеристиках функций случайных величин при случайном числе их слагаемых. Сложение некоррелированных случайных векторов $\vec{v_1}$ и $\vec{v_2}$ на плоскости $x0y$ с составляющими (X_1, Y_1) и (X_2, Y_2) при случайном числе их слагаемых позволяет определить векторную сумму $\vec{v} = \vec{v_1} + \vec{v_2}$ и их векторные составляющие $X = \left(X_1 + X_2\right)$ и $Y = \left(Y_1 + Y_2\right)$, числовую характеристику случайного вектора $\vec{v}$, дисперсию и корреляционный момент D_x, D_y и K_{xy}. По теории сложения дисперсий и корреляционных моментов составляющих каждого из векторов $\vec{v_1}$ и $\vec{v_2}$:

$$D_x = \left(D_{x_1} + D_{x_2}\right);$$
$$D_y = \left(D_{y_1} + D_{y_2}\right);$$
$$K_{xy} = \left(K_{x_1 y_1} + K_{x_2 y_2}\right).$$

Результаты обобщаются на произвольное число слагаемых некоррелированных систем случайных величин для n-мерных случайных векторов:

$\vec{x}$ с составляющими X_1, X_2, …, X_n;

$\vec{y}$ с составляющими Y_1, Y_2, …, Y_n.

Их векторная сумма $\vec{Z} = \vec{x} + \vec{y}$ имеет корреляционную матрицу, элементы которой получаются суммированием элементов.

Вероятность p_{ij} того, что случайная величина X примет значение x_i, а Y – y_i, можно выразить следующей формулой

$$p_{ij} = P\left\{X = x_i, Y = y_i\right\}.$$

Событие $\left\{X = x_i, Y = y_i\right\}$ есть произведение событий $\left\{X = x_i\right\}$ на $\left\{Y = y_i\right\}$. Для двух случайных величин $\left\{X, Y\right\}$ матрицу распределения $p_{ij}\,(i = 1, 2, ...n;\ j = 1, 2, ...m)$ представим таблицей [6].

Таблица – Представление матрицы распределения для двух случайных величин

	y_1	y_2	y_3	…	y_j	…	y_m
x_1	p_{11}	p_{12}	p_{1j}	…	p_{1j}	…	p_{1m}
x_2	p_{21}	p_{22}	p_{23}	…	p_{2j}	…	p_{2m}
…	…	…	…	…	…	…	…
x_i	p_{i1}	p_{i2}	p_{i3}	…	p_{ij}	…	p_{im}
…	…	…	…	…	…	…	…
x_n	p_{n1}	p_{n2}	p_{n3}	…	p_{nj}	…	p_{nm}

Сумма всех вероятностей p_{ij} данной матрицы равна единице как сумма вероятностей полной группы несовместимых событий $\sum_{i=1}^{n}\sum_{j=1}^{m} p_{ij} = 1$.

Закон распределения системы n случайных величин необходим в исследовательских целях. Для случайной величины x корреляционная матрица представляется в виде [6]

$$R_{ij} = \begin{bmatrix} R_{11} & R_{12} & \ldots & R_{1n} \\ R_{21} & R_{22} & \ldots & R_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ R_{n1} & R_{n2} & \ldots & R_{nn} \end{bmatrix}. \tag{4}$$

Матрица симметрична относительно главной диагонали. По главной диагонали матрицы (4) дисперсии равны $D_1 = D_1(x_1),\ D_2 = D_2(x_2),\ \ldots,\ D_n = D_n(x_n)$, $D_{ii} = R_{ii} = R_{ii}\left[x_i x_i\right],\ \ i = \left[1, 2, \ldots, n\right]$.

Геометрическую интерпретацию корреляции можно получить сравнением двух векторов. На рисунке 1 показаны два вектора V_1 и V_2 и разложение каждого из них на ортогональные составляющие.

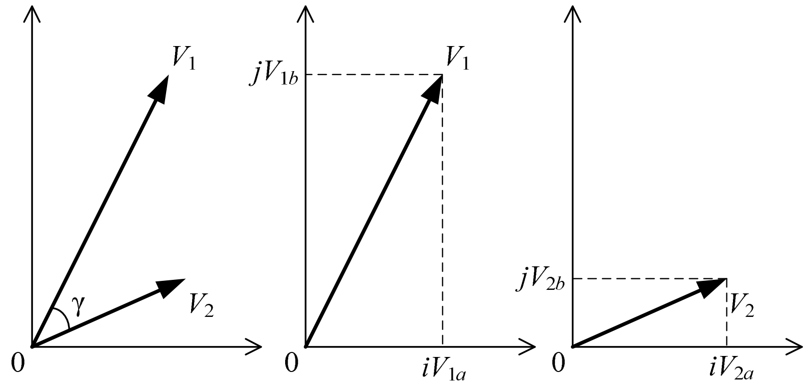


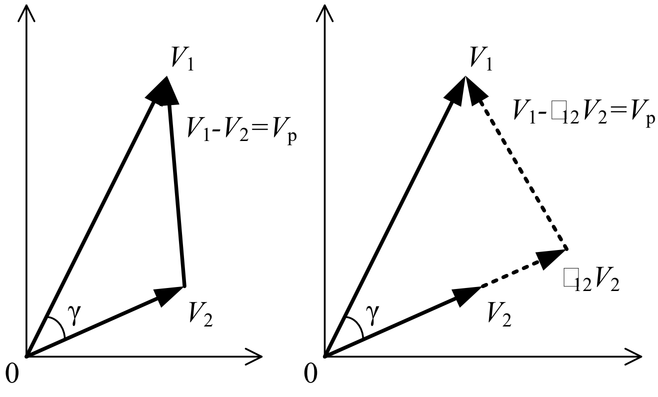
Рисунок 1. – Векторы V_1 и V_2 и их разложение на ортогональные составляющие

Определим количественную меру степени подобия V_1 и V_2. Один из подходов заключается в образовании разностного вектора $V_р$ (рисунок 2, *а*). Если $V_р = 0$, то векторы V_1 и V_2 идентичны. Когда $V_р \neq 0$, подбирают значение V_2 для уменьшения $V_р$. Рассмотрим вектор

$$V_р = V_1 - c_{12} V_2,$$

где c_{12} – вещественная постоянная.

Из рисунка 2, *б* видно, что $V_р$ имеет наименьшее значение, когда ортогонален $c_{12}V_2$. Тогда вектор V_1 состоит из составляющей $c_{12}V_2$, которая отличается от V_2 только по величине, и составляющей $V_р$, ортогональной V_2.



а *б*

Рисунок 2 – Образование разностного вектора

Из рисунка 2, *б* найдём постоянную

$$c_{12} = |V_1| \cos\gamma / |V_2|.$$

Если угол $\gamma = 90^{\circ}$ (V_1 и V_2 ортогональны), то $c_{12} = 0$, а векторы V_1 и V_2 отличаются друг от друга максимально возможным образом, то есть некоррелированны. В противоположном случае, если угол $\gamma = 0$, c_{12} будет просто отношением амплитуд векторов, и $c_{12} = 1$, если $|V_1| = |V_2|$.

Альтернативное уравнению выражение можно получить, обратившись к определению скалярного произведения двух векторов. Если γ – угол между двумя векторами, тогда

$$V_1 \cdot V_2 = |V_1||V_2| \cos\gamma,$$

откуда

$$c_{12} = V_1 \cdot V_2 \big/ |V_2|^2 .$$

Определим далее значение c_{12} так, чтобы его можно было применить к сравнению функций, отличных от простых двумерных векторов. Запишем разложение V_1 и V_2 на прямоугольные составляющие

$$\left.\begin{aligned} V_1 &= iV_{1a} + jV_{1b}; \\ V_2 &= iV_{2a} + jV_{2b}; \\ V_\text{р} &= i\left(V_{1a} - c_{12}V_{2a}\right) + j\left(V_{1b} - c_{12}V_{2b}\right). \end{aligned}\right\}$$

Квадрат модуля (величины) $V_\text{р}$ равен сумме квадратов его ортогональных составляющих:

$$\left|V_\text{р}\right|^2 = \left|V_1 - c_{12}V_2\right|^2 = \left(V_{1a} - c_{12}V_{2a}\right)^2 + \left(V_{1b} - c_{12}V_{2b}\right)^2 .$$

В более общей форме

$$\left|V_\text{р}\right|^2 = \sum_{k=a}^{b} \left(V_{1k} - c_{12}V_{2k}\right)^2 .$$

Следовательно, значение c_{12}, которое минимизирует $\left|V_\text{р}\right|^2$, минимизирует также и $\left|V_\text{р}\right|$. Поэтому уравнение можно дифференцировать по c_{12} и, приравняв нулю, решить относительно c_{12}:

$$\frac{\partial \left|V_\text{р}\right|^2}{\partial c_{12}} = \frac{\partial}{\partial c_{12}} \left[\sum_{k=a}^{b} \left(V_{1k}^2 - 2c_{12}V_{1k}V_{2k} + c_{12}^2 V_{2k}^2 \right) \right] = 0;$$

$$\frac{\partial \left|V_\text{р}\right|^2}{\partial c_{12}} = 2c_{12} \sum_{k=a}^{b} V_{2k}^2 - 2 \sum_{k=a}^{b} V_{1k}V_{2k} = 0;$$

$$c_{12} = \sum_{k=a}^{b} V_{1k}V_{2k} \Bigg/ \sum_{k=a}^{b} V_{2k}^2 .$$

Числитель в уравнении является по определению скалярным произведением V_1 и V_2, а знаменатель представляет собой квадрат модуля V_2. Постоянную c_{12} получили минимизацией квадрата разности между V_1 и V_2.

В этом примере для минимизации вектора разности следовало бы изменять величину не модуля V_2, а модуля V_1. Такая операция дает в результате следующее выражение:

$$c_{12} = \sum_{k=a}^{b} V_{1k}V_{2k} \Bigg/ \sum_{k=a}^{b} V_{1k}^2 .$$

Если записать $V_2 = c_{12}V_1 + V_\text{р}$, увидим, что V_2 можно разложить на составляющие: одна будет отличаться от V_1 только по модулю, другая – $V_\text{р}$, ортогональная V_1.

Заключение. Применяя методы представления, становится возможным введение и широкое использование методики снижения полей рассеивания.

Метод взаимной корреляции (векторное его представление) позволяет реализовать компенсацию полей рассеивания формированием взаимопротивоположной направленности векторов.

Авторы благодарят научного руководителя, доктора технических наук, профессора В.К. Железняка, за оказанную помощь в проводимых исследованиях.

ЛИТЕРАТУРА

1. Железняк, В.К. Защита информации от утечки по техническим каналам : учеб. пособие / В.К. Железняк. – СПб. : ГУАП, 2006. – 188 с.
2. Стейн, С. Принципы современной теории связи и их применение к передаче дискретных сообщений / С. Стейн, Дж. Джонс. – М. : Связь, 1971. – 376 с.
3. Гихман, И.И. Введение в теорию случайных процессов / И.И. Гихман, А.В. Скороход. – М. : Наука, 1977. – 558 с.
4. Мидлтон, Д. Введение в статистическую теорию связи / Д. Мидлтон. – М. : Сов. радио, 1961. – 782 с.
5. Вентцель, Е.С. Теория вероятностей: учеб. для вузов / Е.С. Вентцель. – М. : Наука, 1964. – 576 с.
6. Вентцель, Е.С., Теория вероятностей и ее инженерное приложение / Е.С. Вентцель, Л.А. Овчаров. – М. : Наука, 1988. – 480 с.

Поступила 02.03.2018

MULTIDIMENSIONAL VECTOR REPRESENTATION OF MOMENTUM SIGNAL VALUES WITH THEIR CORRELATION-MATRIX TREATMENT FOR ESTIMATION OF PROTECTION OF VOICE INFORMATION

D. RYABENKO, S. LAVROV

Evaluation of the security of speech information at all stages of the life cycle of information systems and their constituent elements remains a complex scientific task, in spite of the use of new promising models of noise-immune signals with optimal processing. The most important means of processing analog and digital signals for evaluating the protection of voice information remains the correlation method.

Keywords: *analog and digital signal, correlation method, matrix processing.*