$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. После этого последовательность действий для определения параметров матрицы $A_н$ будет такая же, как описано выше, за исключением того, что под входным будем понимать изображение, полученное из входного изображения путем применения преобразования зеркального отражения.

Заключение

Итак, в данной работе на основе методов одномерной нормализации разработан алгоритм нормализации плоских изображений для общего случая, когда заранее не известен вид геометрического преобразования, формирующего разницу между эталонным и входным изображениями.

В основу общего алгоритма положено исследование разложения матрицы центроаффинного преобразования в суперпозицию матриц поворота, неоднородного изменения масштаба и еще одного поворота, возможно в сочетании с зеркальным отражением. Рассмотрено свойство преобразования неоднородного изменения масштаба по взаимно перпендикулярным направлениям, заключающегося в максимальном и минимальном изменении коэффициентов масштаба по этим направлениям.

Особое внимание уделено вопросу присутствия зеркального отражения, его обнаружению методом одномерной нормализации.

Литература: 1. *Путятин Е.П.* Обработка изображений в робототехнике. М.: Машиностроение, 1990. 320с. 2. *Акивис М.А., Гольдберг В.В.* Тензорное исчисление. М.: Наука, 1969. 352с. 3. *Мышкис А.Д.* Лекции по высшей математике. М.: Наука, 1964. 608с. 4. *Беллман Р.* Введение в теорию матриц М.: Наука, 1969. 368с. 5. *Моденов П.С.* Аналитическая геометрия. М.: Изд-во МГУ, 1969. 698с. 6. *Путятин Е.П., Яковлева Е.В., Любченко В.А.* Исследование инвариантных прямых и их применение в алгоритмах нормализации изображений // АСУ и приборы автоматики. № 109. 7. *Путятин Е.П., Яковлева Е.В., Любченко В.А.* Разложение матрицы центроаффинного преобразования для нормализации изображений // Радиоэлектроника и информатика. 1998. № 4. С. 91-94.

Поступила в редколлегию 05.11.99

Рецензент: д-р техн. наук Сироджа И.Б.

Путятин Евгений Петрович, д-р техн. наук, профессор, зав. кафедрой информатики ЭВМ ХТУРЭ. Научные интересы: обработка и распознавание изображений. Адрес: Украина, 61726, Харьков, пр. Ленина,14, тел. 40-94-19.

Яковлева Елена Владимировна, аспирант кафедры информатики ХТУРЭ. Научные интересы: обработка и распознавание изображений. Адрес: Украина, 61726, Харьков, пр. Ленина, 14, тел. 40-94-19. E-mail: jakovleva@altavista.net

Луцив Вячеслав Валериевич. Научные интересы: компьютерная графика, разработка высокопроизводительных алгоритмов обработки графической информации. Адрес: Украина, 61726, Харьков, пр. Ленина,14, тел. 40-94-19. E-mail: lslav@altavista.net

УДК 621.391

ГЕНЕРАЦИЯ УЗКОПОЛОСНЫХ ИМИТАЦИОННЫХ СЛУЧАЙНЫХ ПРОЦЕССОВ

ТИХОНОВ В.А., РУСАНОВСКИЙ Д.Е., ТИХОНОВ Д.В.

Разрабатываются методы генерации стационарных случайных процессов по заданным параметрам СПМ с помощью авторегрессионных формирующих фильтров. Показывается связь параметров АР модели и характеристик процесса, таких как центральная частота и ширина полосы по уровню 0,5 СПМ. Особый интерес представляет методика получения случайных процессов, содержащих один и более максимумов в СПМ. Приведенные примеры АР моделирования имитационных процессов подтверждают предложенный метод.

Модель авторегрессии (АР) применяется для решения двух основных задач: получения вероятностных характеристик случайного процесса по заданной выборке и формирования реализаций случайного процесса, когда его характеристики заданы. Обычно в научной литературе основное внимание уделяется решению первой задачи. Между тем, широкое применение методов статистического моделирования требует, как правило, предварительного получения имитационного процесса. Используемые для этих целей методы не обладают достаточной гибкостью и простотой. Конструктивные свойства модели АР дают возможность сравнительно простыми способами получить имитационные случайные процессы с заданными статистическими характеристиками. В качестве таковых можно использовать ширину полосы и центральную частоту спектральной плотности мощности (СПМ), частоту осцилляций и коэффициент демпфирования корреляционной функции имитируемого процесса. Кроме этого, можно получать случайные процессы с заданными видами корреляционной функции и СПМ.

В основу модели АР положена корреляция отсчета случайного процесса в текущий момент времени с некоторым конечным или бесконечным числом отсчетов в предыдущие моменты времени. В уравнении АР текущий отсчет представляется взвешенной суммой предыдущих с некоторыми коэффициентами веса [1]:

$$x_t = \sum_{j=1}^{p} \Phi_j x_{t-j} + a_t \quad , \qquad (1)$$

где Φ_j – коэффициенты АР; a_t – некоррелированные случайные отсчеты, называемые ошибкой предсказания; p – порядок модели АР.

Из (1) видно, что построение модели АР случайного процесса сводится к определению порядка p, нахождению коэффициентов АР и дисперсии ошибки предсказания с помощью системы $p+1$ уравнений Юла-Уокера:

$$R_i - \sum_{j=1}^{p} \Phi_j R_{j-i} = 0\,,\ i = 1 \div p\ , \quad (2а)$$

$$R_0 - \sum_{j=1}^{p} \Phi_j R_j = D_a\ . \quad (2б)$$

Здесь $R_i = E\{x_t x_{t-i}\}$ – значения функции корреляции случайного процесса; D_a – дисперсия ошибок предсказания модели АР; R_0 – дисперсия случайного процесса x_t.

Порядок процесса АР определяется с использованием различных критериев, как правило, основанных на минимизации некоторой теоретико-информационной функции [2].

В задачах статистического моделирования часто возникает необходимость генерации случайного процесса с заданной корреляционной функцией или с заданной формой и характеристиками СПМ. Для этих целей эффективно применять генератор процесса АР, использующий алгоритм (1). Генерация случайного процесса осуществляется методом, порождающим случайный процесс. Последний в виде белого шума пропускается через формирующий фильтр, параметры которого определяются соответствующей моделью АР.

Выражение для спектра модели АР имеет вид [1]

$$P(f) = D_a \Big/ \left| 1 - \sum_{i=1}^{p} \Phi_i e^{-ji2\pi fT} \right|^2\ , \quad (3)$$

где T – интервал дискретизации процесса.

Из условия устойчивости формирующего АР фильтра с рациональной передаточной функцией следует условие стационарности АР процесса. Для проверки стационарности случайного АР процесса используется характеристическое уравнение

$$\Phi(z) = z^p - \Phi_1 z^{p-1} - \ldots - \Phi_p = 0\,. \quad (4)$$

Если корни (4) лежат внутри единичного круга на комплексной плоскости, то процесс АР удовлетворяет условию стационарности.

Уравнение (4) можно представить в виде

$$\Phi(z) = \prod_{i=1}^{p} (z - c_i) = 0, \quad (5)$$

где c_i – корни характеристического уравнения (4). Сравнив (4) и (5), найдем связь между коэффициентами АР и корнями c_i. Приведем соответствующие формулы для $p = 1 \div 3$:

$$\Phi_{1,1} = c_{1,1}\ ; \quad (6а)$$

$$\Phi_{2,1} = c_{2,1} + c_{2,2}\,,$$

$$\Phi_{2,2} = -c_{2,1} c_{2,1}\,; \quad (6б)$$

$$\Phi_{3,1} = c_{3,1} + c_{3,2} + c_{3,3}\,,$$

$$\Phi_{3,2} = -(c_{3,1} c_{3,2} + c_{3,2} c_{3,3} + c_{3,1} c_{3,3})\,,$$

$$\Phi_{3,3} = c_{3,1} c_{3,2} c_{3,3}\ . \quad (6в)$$

Корни характеристического уравнения (4) полностью описывают модель АР. Если корень действительный, то его можно представить в виде экспоненциальной функции [3]:

$$c = e^{-\pi \Delta f T}\,, \quad (7)$$

где Δf – ширина полосы максимума спектра по уровню 0,5. Комплексные корни характеристического уравнения являются комплексно-сопряжёнными и описываются выражениями

$$c_1 = e^{-\pi \Delta f T - j2\pi f_h T}\ ,\quad c_2 = e^{-\pi \Delta f T + j2\pi f_h T}\,. \quad (8)$$

Комплексные корни характеризуют максимумы спектра (полюса передаточной функции) на частоте, близкой к $f = f_h$ – собственной частоте модели АР с поправкой на затухание.

Используя данное представление корней и формулы (6а), (6б), (6в), несложно представить коэффициенты АР как функции от центральной частоты максимума и его полосы пропускания:

$$\Phi = F(f_i, \Delta f_i)\,. \quad (9)$$

Конструктивные свойства модели АР дают возможность сравнительно простыми способами сгенерировать имитационные случайные процессы с заданными спектральными и статистическими характеристиками. В качестве таковых можно использовать ширину полосы и центральную частоту СПМ, частоту осцилляций и коэффициент демпфирования корреляционной функции имитируемого процесса. Для подтверждения предложенного метода генерации АР процесса рассмотрим некоторые примеры определения параметров генераторов АР процесса, когда заданы характеристики СПМ.

Сначала генерируем процесс, имеющий следующие характеристики СПМ: $p = 2$, $\Delta f_1 = 5$, $f_1 = 20$ при $T = 0{,}01$. Используя формулы (8) и (6б), получаем значения коэффициентов АР: $\Phi_{2,1} = 0{,}53$; $\Phi_{2,2} = -0{,}73$.

Спектральная плотность мощности генерируемого процесса, рассчитанная по формуле (3), представлена сплошной линией S_1 на рис.1. По найденным коэффициентам сгенерирован АР процесс и получены выборочные оценки коэффициентов АР и СПМ с использованием формул (2а), (2б) и (4). Оценка СПМ имитационного случайного АР процесса дана пунктирной линией S_2.

На рис 2. приведена СПМ генерируемого процесса АР и его выборочная оценка СПМ процесса АР третьего порядка со следующими параметрами:

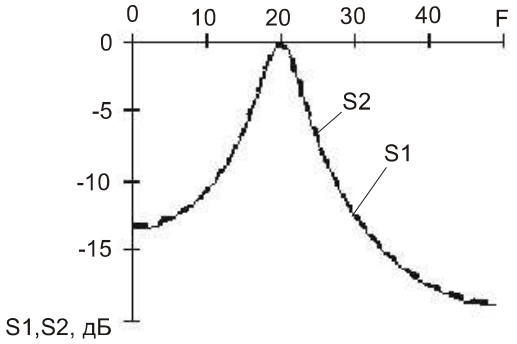

Рис. 1

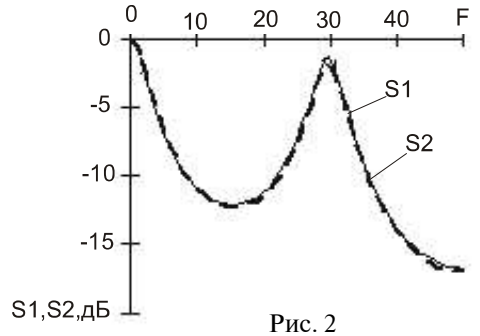

Рис. 2

$\Delta f_0 = 5$; $\Delta f_1 = 5$; $f_1 = 30$. Значения рассчитанных коэффициентов АР формирующих фильтров составляли:

$$\Phi_{3,1} = 0{,}326; \Phi_{3,2} = -0{,}280; \Phi_{3,3} = 0{,}624.$$

Анализ графиков показывает, что отклонения между задаваемой СПМ и его оценкой незначительны. Данные показатели являются приемлемыми для большинства инженерных приложений. Предложенный метод генерации имитационных коррелированных случайных процессов превосходит существующие аналоги [4].

Литература: 1. *Бокс Дж. , Дженкинс Г.* Анализ временных рядов: Пер.с англ. М.: Мир.1974. Вып.1. 406 с. 2. *Марпл.мл. С.Л.* Цифровой спектральный анализ и его приложения: Пер. с англ.М.: Мир, 1990. 584 с. 3. *Кармалита В.А.* Цифровая обработка случайных колебаний. М: Машиносроение,1986. 80 с. 4. *Быков В.В.* Цифровое моделирование в статистической радиотехнике. М: Сов. радио, 1971. 326 с.

Поступила в редколлегию 11.10.99

Рецензент: д-р техн. наук Кравченко Н.И.

Тихонов Вячеслав Анатольевич, канд. техн. наук, доцент кафедры РТС ХТУРЭ. Научные интересы: радиолокация, распознавание образов, статистические модели. Адрес: Украина, 61078, Харьков, ул. Каразина, 7/9, кв. 9, тел. 40-95-87, 47-03-91.

Русановский Дмитрий Евгеньевич, студент гр. АРТ-95-1 ХТУРЭ. Научные интересы: цифровая обработка речи – кодирование, сжатие речи, статистическое моделирование. Хобби: программирование, Web-дизайн. Адрес: Украина, 61118, г.Южный, ул. Освобождения-2.

e-mail: d_rusanovsky@aport.ru

Тихонов Дмитрий Вячеславович, студент гр. ИСПР-98-1 ХТУРЭ. Научные интересы: искусственный интеллект, распознавание речи, программирование. Адрес: Украина, 61078, Харьков, ул. Каразина 7/9, кв. 9, тел. 47-03-91.

УДК 519.713

ЭФФЕКТИВНАЯ РЕАЛИЗАЦИЯ ОПЕРАЦИИ ВОЗВЕДЕНИЯ В СТЕПЕНЬ БОЛЬШИХ ЦЕЛЫХ ЧИСЕЛ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ МЕТОДОМ ПРЕДВЫЧИСЛЕНИЙ ПО ФИКСИРОВАННОМУ ОСНОВАНИЮ

ГОРБЕНКО И.Д., ЛАВРИНЕНКО Д.И.

Проводится сравнительный анализ алгоритмов для операции возведения в степень по модулю целых чисел большой разрядности. Описывается алгоритм с использованием набора предвычисленных значений по фиксированному основанию. Предлагается параллельная модификация такого алгоритма. Приводятся результаты применения данных алгоритмов для наиболее распространённых схем и алгоритмов в криптографии.

1. Введение

В ряде несимметричных криптографических алгоритмов [1], а также в алгоритмах и средствах криптоанализа такого класса [2] арифметические операции выполняются над числами x, разрядность которых L_x значительно превышает разрядную сетку L_p современных вычислительных средств. Такие числа известны как числа многократной точности. Основные операции, которые выполняются над ними, это сложение, вычитание, умножение, деление и возведение в степень по модулю N. Проведенные исследования показали, что наиболее часто в криптопреобразованиях используется операция возведения в степень по модулю. Вычислительная сложность данной операции носит полиномиальный характер, причём порядок и коэффициенты полиномов, описывающих вычислительную сложность, зависят от применяемых математических методов и алгоритмов умножения, деления и возведения в степень по модулю. Достаточно подробно методы и алгоритмы возведения в степень по модулю рассмотрены в [3].

Применение при выполнении операции умножения по модулю преобразования Монтгомери или преобразования Барретта [3], а также использование при возведении в степень по модулю блочного метода [4] позволили уменьшить вычислительную сложность этих операций. Такое уменьшение эквивалентно повышению скорости преобразований. Несмотря на определённое уменьшение вычислительной сложности операции возведения в степень, её величина остаётся всё ещё значительной, а выполнение требований по увеличению скорости криптографических преобразований – проблематичным. В связи с этим дальнейшее уменьшение вычислительной сложности операции возведения в степень по модулю чисел большой разрядности остаётся актуальной задачей.