ПРИМЕНЕНИЕ СТОХАСТИЧЕСКИХ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ С ПЕРЕМЕННЫМИ КОЭФФИЦИЕНТАМИ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В ЗВУКОВЫХ ФАЙЛАХ

Сергей Приходько

Национальный университет кораблестроения имени адмирала Макарова
Проспект Героев Сталинграда, 9, Николаев, 54025, Украина,
тел.: (0512) 42-44-70, E-mail: sbp@usmtu.edu.ua

Аннотация

Рассматривается модифицированный подход для защиты речевой информации, который основан на применении нормализированных стохастических дифференциальных уравнений (СДУ) с переменными коэффициентами. Для примера приводится применение СДУ второго порядка для защиты речевой информации в wav-файлах.

Введение

В области защиты информации одной из актуальных является проблема нарушение конфиденциальности информации, в том числе и речевой. В компьютерных системах эта проблема решается путем защиты информации с помощью методов криптографии. Однако сейчас, помимо использования хорошо известных криптографических алгоритмов, наблюдается поиск новых решений.

К сравнительно новым решениям в области криптографии можно отнести применение теории детерминированного хаоса [1-3]. Однако у динамических хаотических систем имеется ряд отрицательных свойств (например, существование непредсказуемо коротких длин орбит), что в криптографии неприемлемо. Другим менее известным решением для защиты информации является применение СДУ. В [4, 5] для защиты звуковой информации на основе СДУ был предложен следующий подход. Звуковой сигнал или его часть представляется СДУ. В результате решения задачи параметрической идентификации находятся коэффициенты СДУ. Из численного решения СДУ определяются значения белого шума, который передается вместо звукового сигнала. Восстановление сигнала выполняется путем численного решения СДУ с соответствующими коэффициентами и значениями белого шума. В [6] вместо белого шума было предложено применять одну из компонент СДУ. В [7, 8] данный подход был модифицирован: вместо компоненты СДУ для защиты звукового сигнала было предложено применить одну из преобразованных компонент СДУ. Такая модификация помимо повышения стойкости защиты, с одной стороны, позволила упростить решение задачи параметрической идентификации в случае применения преобразования Джонсона, которое обеспечивает переход к нормально распределенной преобразованной компоненте, а с другой стороны, дала возможность получать компоненту с заданной спектральной плотностью. Однако все предложенные ранее решения имеют одно существенное ограничение: незначительный временной интервал, на котором звуковой случайный сигнал приближенно можно считать стационарным. Указанное ограничение связано с использованием в качестве математической модели звукового сигнала СДУ с постоянными коэффициентами. Снять данное ограничение возможно путем применения для описания звукового сигнала СДУ с переменными коэффициентами. Поэтому цель данной работы состоит в том, чтобы показать возможность защиты речевой информации на основе применения СДУ с переменными коэффициентами и предложить соответствующий подход.

Суть предлагаемого подхода состоит в следующем. Сначала строим СДУ для нормализованного звукового случайного сигнала на основе применения преобразования Джонсона и метода формирующих фильтров так, как было предложено в [9]. Далее полагаем хотя бы один из коэффициентов в построенном СДУ для нормализованного звукового случайного сигнала зависящим от времени. Затем из численного решения этого СДУ по ординатам нормализованного звукового сигнала вычисляем значения выбранного коэффициента, который является случайным процессом. Значения этого коэффициента записываем в звуковой файл вместо исходного речевого сигнала, что и обеспечивает защиту информации. Восстановление исходного речевого сигнала выполняем в обратном порядке. На основе численного решения СДУ для нормализованного звукового случайного сигнала по значениям соответствующего коэффициента, который использовался для защиты информации, находим значения нормализованного звукового случайного сигнала, по которым, используя преобразование Джонсона, восстанавливаем первоначальный речевой сигнал.

Теоретическое решение

Звуковой случайный сигнал $x(t)$ может быть преобразован в случайный процесс $z(t)$ с нормальным распределением (нормализованный случайный сигнал) на основе преобразования

Джонсона. В общем случае преобразование Джонсона имеет вид [10]

$$z = \gamma + \eta h(x, \varphi, \lambda);\ \eta > 0;\ -\infty < \gamma < \infty;\ \lambda > 0;\ -\infty < \varphi < \infty, \tag{1}$$

где h – произвольная функция; η, γ, λ, φ – параметры распределения Джонсона.

Джонсон предложил три различных семейства функций h. Как показали исследования, для случайных звуковых сигналов (прежде всего речевых) с распределением ординат с большим эксцессом (больше 4) лучше всего подходит преобразование семейства S_U, для которого

$$h(x, \varphi, \lambda) = \mathrm{Arsh}(\bar{x}), \qquad -\infty \le x \le +\infty, \tag{2}$$

где $\bar{x} = (x - \varphi)/\lambda$; $\mathrm{Arsh}(\bar{x}) = \ln\left[\bar{x} + \sqrt{(\bar{x})^2 + 1}\right]$.

Для семейств S_U функция плотности вероятности задается как

$$f_U(x) = \frac{\eta}{\sqrt{2\pi\left\{(x-\varphi)^2 + \lambda^2\right\}}} \exp\left\{-\frac{1}{2}\left[\gamma + \eta\,\mathrm{Arsh}(\bar{x})\right]^2\right\}. \tag{3}$$

Параметры функции плотности вероятности γ, η, λ та φ для выбранного семейства распределений Джонсона, в том числе и (3), в общем случае можно найти путем решения следующей задачи математического программирования:

$$\theta = \arg\min_{\theta}\left\{\sum_{j=1}^{m}\left[y(x_j) - f(x_j, \theta)\right]^2\right\}, \tag{4}$$

где θ – вектор неизвестных параметров, $\theta = \{\gamma, \eta, \lambda, \varphi\}$; x_j – значение случайной величины x в середине j-го подинтервала; $y(x_j)$ – значение ординаты гистограммы при значении x_j; $f(x_j, \theta)$ – выражение функции плотности вероятности при значении x_j; m – количество подинтервалов гистограммы. Заметим, что при использовании формулы (3), в качестве значения $y(x_j)$ необходимо брать отношение относительной частоты в j-ом подинтервале к длине j-го подинтервала Δx [11].

Параметры функции (3) также можно найти из решения систем нелинейных алгебраических уравнений, которые составляются из равенств соответствующих аналитических выражений для статистических моментов первых четырех порядков и их оценок, вычисленных по гистограмме [11].

После нахождения параметров функции плотности вероятности (3) ординат звукового случайного сигнала $x(t)$ выполняем на основе преобразования Джонсона (1) с функцией h (2) нормализацию $x(t)$, получая при этом случайный сигнал $z(t)$. По реализации нормализованного случайного сигнала $z(t)$ оцениваем его спектральную плотность и аппроксимируем ее дробно-рациональной функцией вида

$$S_\zeta(\omega) = \frac{1}{2\pi} \cdot \frac{|H(i\omega)|^2}{|F(i\omega)|^2},$$

где

$$F(x) = \sum_{k=0}^{n} a_k x^k,\ a_n = 1,\ H(x) = \sum_{k=0}^{m} b_k x^k,\ m \le n-1,$$

при этом корни многочленов $F(x)$ и $H(x)$ лежат в левой полуплоскости.

Далее, используя метод формирующих фильтров, получаем СДУ для нормализованного сигнала, которое в общем случае может быть представлено как

$$d\mathbf{z}(t) = \mathbf{A}\mathbf{z}(t)dt + \mathbf{B}dw(t),\ \mathbf{z}(0) = \mathbf{v}. \tag{5}$$

Здесь $w(t)$ – скалярный стандартный винеровский процесс,

$$\mathbf{A}=\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{bmatrix},\ \mathbf{B}=\begin{bmatrix} 0 \\ \dots \\ 0 \\ q_{n-m} \\ q_{n-m+1} \\ \dots \\ q_n \end{bmatrix},$$

$\{a_0,\dots,a_{n=1}\}$ – коэффициенты многочлена $F(x)$, а параметры $\{q_{n-m},\dots,q_n\}$ определяются по рекуррентным формулам:

$$q_{n-m}=b_m,\ q_k=b_{n-k}-\sum_{i=n-m}^{k-1}a_{n-k+i}q_i,\ k=n-m+1,\dots,n,$$

где $\{b_0,\dots,b_m\}$ – коэффициенты многочлена $H(x)$.

Основываясь на структуре СДУ (5), можно записать СДУ с переменными коэффициентами

$$d\mathbf{z}(t)=\mathbf{A}(t)\mathbf{z}(t)dt+\mathbf{B}(t)dw(t),\ \mathbf{z}(0)=\mathbf{v}. \tag{6}$$

На основе (6) можно составить разностные уравнения. Используя метод Эйлера для (6), разностные уравнения записываются как

$$\mathbf{z}_{i+1}=\mathbf{z}_i+\left[\mathbf{A}_i\mathbf{z}_i+\mathbf{B}_i n(t_i)\right]\Delta t, \tag{7}$$

где $n(t_i)$ – ордината белого шума в момент времени t_i; Δt – шаг по времени.

На основе (7) по ординатам нормализованного звукового сигнала вычисляем значения выбранного коэффициента, который является случайным процессом и используется для защиты речевой информации.

Предложенный подход рассмотрим для случая, когда функция плотности вероятности ординат звукового сигнала $x(t)$ имеет вид (3), а полученный с помощью (1) и (2) сигнал $z(t)$ задается СДУ

$$\ddot{z}+2\alpha_z\dot{z}+c(t)z=2\sqrt{D_z\alpha_z}\dot{n}(t), \tag{8}$$

где $n(t)$ – белый шум; D_z – дисперсия $z(t)$; α_z – коэффициент затухания корреляционной функции $z(t)$; $c(t)$ – переменный коэффициент, который используется для защиты речевой информации.

Обозначив, $z_1=z(t)$ и $z_2=\dot{z}(t)-2\sqrt{D_z\alpha_z}n(t)$ преобразуем уравнение (8) в систему

$$\begin{aligned} \dot{z}_1&=z_2+2\sqrt{D_z\alpha_z}n(t); \\ \dot{z}_2&=-4\alpha_z\sqrt{D_z\alpha_z}n(t)-2\alpha_z z_2-c(t)z_1. \end{aligned} \tag{9}$$

Метод Эйлера для системы (9) дает следующие уравнения:

$$\begin{aligned} z_{1_{i+1}}&=z_{1_i}+z_{2_i}\Delta t+2\zeta_i\sqrt{D_z\alpha_z N_0\Delta t}; \\ z_{2_{i+1}}&=z_{2_i}-4\alpha_z\zeta_i\sqrt{D_z\alpha_z N_0\Delta t}-2\alpha_z z_{2_i}\Delta t-c(t_i)z_{1_i}\Delta t. \end{aligned} \tag{10}$$

Здесь N_0 – интенсивность белого шума; ζ_i – i-е значение нормально распределенной случайной величины с нулевым математическим ожиданием и дисперсией равной единице.

На основе (10) по ординатам нормализованного звукового сигнала $z(t)$ вычисляем значения выбранного коэффициента $c(t)$, которые записываем в звуковой файл вместо исходного речевого сигнала $x(t)$.

Исходный речевой сигнал $x(t)$ восстанавливаем в обратном порядке. По значениям коэффициента $c(t)$ на основе (10) находим ординаты нормализованного звукового сигнала $z(t)$. А на

основе преобразования Джонсона (1) с функцией h (2) по ординатам $z(t)$ восстанавливаем значения ординат исходного речевого сигнала $x(t)$.

Как показали эксперименты с реальными речевыми сигналами в wav-файлах, коэффициент $c(t)$ является случайным процессом близким к цветному шуму. При восстановлении речевых сигналов наблюдается незначительная потеря качества, которая на слух не заметна.

Литература:

[1] H. Gutowitz, "Cryptography with Dynamical Systems", ESPCI, Laboratoire d'Electronique, Paris, France, 1995, http://www.santafe.edu/~hag/crypto/crypto.html.
[2] L. Kosarev, "Chaos and Cryptography", 2001, http://rfic.ucsd.edu/chos/ws2001/kosarev.pdf.
[3] W. K. Wong, "Chaotic Encryption Technique", City University of Hong Kong, Department of Electronic Engineering, Hong Kong, 1999, http://kitson.netfirms.com/chaos.
[4] С. Б. Приходько, "Применение стохастических дифференциальных уравнений для защиты звуковой информации", Тр. Одес. политехн. ун-та, 2003, Вип.2 (20), С.163-166.
[5] С. Б. Приходько, "Применение стохастических дифференциальных уравнений для защиты информации в звуковых файлах", Зб. наук. праць УДМТУ, Миколаїв: УДМТУ, 2003, № 6 (392), С.133-140.
[6] С. Б. Приходько, "Применение компонент стохастических дифференциальных уравнений для защиты информации в звуковых файлах", Сборник научных трудов НГУ, Днепропетровск: НГУ, 2004, № 19, том 2, С.182–187.
[7] S. Prikhodko, "The application of Johnson transform and stochastic differential equations for protection of the information in sound files", «Інтернет – Освіта – Наука – 2004», четверта міжнародна конференція ІОН–2004, 28 вересня – 16 жовтня, 2004 р. Збірник матеріалів конференції. Том 2, Вінниця: УНІВЕРСУМ-Вінниця, 2004, С.471-475.
[8] С. Б. Приходько, "Применение преобразования компонент стохастических дифференциальных уравнений для защиты от несанкционированного прослушивания информации в звуковых файлах", Зб. наук. праць НУК, Миколаїв: НУК, 2004, № 5 (398), С.117-125.
[9] С. Б. Приходько, "Методи побудови математичних моделей нормалізованих сигналів нелінійних стохастичних диференціальних систем", Тези доповідей міждерж. науково-методич. конф. "Проблеми математичного моделювання" (28-30 травня 2008 р., м. Дніпродзержинськ), Дніпродзержинськ: ДДТУ, 2008, С.137-139.
[10] М. Кендалл, А. Стюарт, "Теория распределений", Пер. с англ./ Под ред. А.Н.Колмогорова, М.: Наука, Гл. ред. физ.-мат. лит., 1966, 588 с.
[11] С. Б. Приходько, "Методичні вказівки до виконання лабораторних робіт з дисципліни "Обробка експериментальних даних на ЕОМ"". – Миколаїв: НУК, 2005. – 52 с.