УДК 681.3:519.62:519.711

С. Б. Приходько, к. т. н., доц.

ЗАХИСТ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ СТОХАСТИЧНИХ ДИФЕРЕНЦІАЛЬНИХ РІВНЯНЬ ЗІ ЗМІННИМИ КОЕФІЦІЄНТАМИ ДЛЯ НОРМАЛІЗОВАНИХ ЗВУКОВИХ СИГНАЛІВ

Запропоновано модифікований підхід для захисту мовної інформації, який оснований на використанні стохастичних диференціальних рівнянь зі змінними коефіцієнтами для нормалізованих звукових сигналів.

Вступ

В галузі захисту інформації однією з актуальних є проблема порушення кон-фіденційності інформації, в тому числі і мовної. В комп'ютерних системах ця проблема вирішується шляхом захисту інформації за допомогою засобів криптографії. Але зараз, окрім використання добре відомих криптографічних алгоритмів, спостерігається пошук нових рішень.

До відносно нових рішень в галузі криптографії можна віднести застосування теорії детермінованого хаосу [1—3]. Але у динамічних хаотичних систем є ряд негативних властивостей (наприклад, існування непередбачено коротких довжин орбіт), що у криптографії неприпустимо. Іншим менш відомим рішенням для захисту інформації є застосування стохастичних диференціальних рівнянь (СДР). В [4, 5] для захисту звукової інформації на основі СДР було запропоновано наступний підхід. Звуковий сигнал або його частина зображується СДР. В результаті розв'язання задачі параметричної ідентифікації знаходяться коефіцієнти СДР. Числовим розв'язанням СДР визначаються параметри білого шуму, який передається замість звукового сигналу. Поновлення сигналу виконується шляхом числового розв'язання СДР з відповідними коефіцієнтами і значеннями білого шуму. В [6] замість білого шуму було запропоновано застосовувати одну з компонент СДР. В [7, 8] зазначений підхід було модифіковано: замість компоненти СДР для захисту звукового сигналу було запропоновано застосувати одну з перетворених компонент СДР. Така модифікація окрім покращення захисту, с одного боку, дозволила спростити рішення задачі параметричної ідентифікації, а з іншого боку, дала можливість отримувати компоненту з заданою спектральною щільністю. Але всі запропоновані раніше рішення мають одне суттєве обмеження: незначний часовий інтервал, на якому звуковий випадковий сигнал наближено можна вважати стаціонарним. Вказане обмеження зв'язано з використанням у якості математичної моделі звукового сигналу СДР з постійними коефіцієнтами. Зняти це обмеження можна шляхом переходу до СДР зі змінними коефіцієнтами. Тому *мета роботи* полягає у тому, щоб показати можливість захисту мовної інформації на основі застосування СДР зі змінними коефіцієнтами для нормалізованих звукових сигналів і запропонувати відповідний підхід.

Суть підходу, який пропонується, полягає у такому. Спочатку будуємо СДР для нормалізованого мовного сигналу на основі застосування перетворення Джонсона і метода формувальних фільтрів так, як було запропоновано в [9]. Далі припускаємо, що хоча б один з коефіцієнтів в побудованому СДР залежить від часу і він може бути зображений додатком двох складових: постійною і пульсаційною. Потім числовим розв'язанням цього СДР за ординатами нормалізованого звукового сигналу обчислюємо значення обраного коефіцієнта. Значення його записується в звуковий файл замість початкового мовного сигналу, що і забезпечує захист мовної інформації. Поновлення початкового мовного сигналу виконуємо у зворотному порядку. На основі числового розв'язання СДР для нормалізованого мовного сигналу за значеннями відповідного коефіцієнту, який використовувався для захисту інформації, знаходимо значення нормалізованого звукового випадкового сигналу, за якими, використовуючи перетворення Джонсона, поновлюємо мовний сигнал.

Теоретичне обґрунтування запропонованого підходу

Мовний сигнал $x(t)$ може бути перетворений у випадковий процес $z(t)$ з нормальним розподілом (нормалізований випадковий сигнал) за допомогою перетворення Джонсона [10]

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

де h — довільна функція; γ, η, λ, ϕ — параметри розподілу Джонсона.

Джонсон запропонував три різні сім'ї функцій h. Як показали дослідження [7, 8], для мовних сигналів, розподіл ординат яких має великий ексцес (більше за 4), краще всього підходить перетворення з сім'ї S_U, для якої

$$h(x, \phi, \lambda) = \operatorname{Arsh}(\bar{x}), \quad -\infty \le x \le +\infty \text{ (сім'я } S_U), \tag{2}$$

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

Для сім'ї S_U функції щільності ймовірності задається як

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

Параметри γ, η, λ та ϕ для (3), можна знайти шляхом розв'язання такої задачі математичного програмування:

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

де θ — вектор невідомих параметрів, $\theta = \{\gamma, \eta, \lambda, \phi\}$; x_j — значення випадкової величини x в середині j-го підінтервалу; $y(x_j)$ — значення ординати гістограми для значення x_j; $f(x_j, \theta)$ — вираз функції щільності ймовірності для значення x_j; m — кількість підінтервалів гістограми.

Далі на основі перетворення Джонсона (1) з функцією h (2) виконуємо нормалізацію $x(t)$, отримуючи при цьому випадковий сигнал $z(t)$. За реалізацією нормалізованого випадкового сигналу $z(t)$ оцінюємо його спектральну щільність і апроксимуємо її дробово-раціональною функцією

$$S_z(\omega) = \frac{1}{2\pi} \cdot \frac{\left|H(i\omega)\right|^2}{\left|F(i\omega)\right|^2},$$

де $F(x) = \sum_{k=0}^{n} a_k x^k$, $a_n = 1$, $H(x) = \sum_{k=0}^{m} b_k x^k$, $m \le n-1$, причому корені багаточленів $F(x)$ і $H(x)$ лежать у лівій півплощині.

Використовуючи метод формувальних фільтрів, отримуємо СДР для $z(t)$

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

де $w(t)$ — скалярний стандартний вінеровський процес,

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

$\{a_0, \dots, a_{n=1}\}$ — коефіцієнти $F(x)$, а параметри $\{q_{n-m}, \dots, q_n\}$ визначаються за рекурентними

формулами: $q_{n-m} = b_m$, $q_k = b_{n-k} - \sum_{i=n-m}^{k-1} a_{n-k+i} q_i$, $k = n-m+1,\ldots,n$; $\{b_0, \ldots, b_m\}$ — коефіцієнти багаточлену $H(x)$.

Базуючись на СДР (5), отримуємо СДР зі змінними коефіцієнтами

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

На основі (6) складаємо різницеві рівняння. Використовуючи метод Ейлера для (6), різницеві рівняння записуються як

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

де $n(t_i)$ — ордината білого шуму в момент часу t_i; Δt — крок за часом.

На основі (7) за ординатами нормалізованого звукового сигналу обчислюємо значення обраного коефіцієнту, який є випадковим процесом і використовується для захисту мовної інформації.

Запропонований підхід розглянемо для випадку, коли отриманий за допомогою (1) і (2) сигнал $z(t)$ задається СДР

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

де $n(t)$ — білий шум; D_z — дисперсія $z(t)$; α_z — коефіцієнт загасання кореляційної функції $z(t)$; $c(t)$ — змінний коефіцієнт, $c(t) = \overline{c} + \tilde{c}(t)$; $\overline{c}$ — постійна складова $c(t)$; $\tilde{c}(t)$ — змінна (пульсаційна) складова $c(t)$, яка використовується для захисту мовної інформації.

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

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

За методом Ейлера для системи (9) отримуємо такі рівняння:

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

Тут N_0 — інтенсивність білого шуму; ζ_i — i-те значення нормально розподіленої випадкової величини з нульовим математичним сподіванням і одиничною дисперсією.

На основі (10) за ординатами нормалізованого звукового сигналу $z(t)$ обчислюємо значення $\tilde{c}(t)$, які записуємо в звуковий файл замість відповідних ординат початкового мовного сигналу $x(t)$.

Початковий мовний сигнал $x(t)$ поновлюємо у зворотному порядку. За значеннями $\tilde{c}(t)$ на основі (10) знаходимо ординати $z(t)$. А на основі перетворення Джонсона (1) з функцією h (2) за ординатами $z(t)$ поновлюємо значення ординат сигналу $x(t)$.

Практичні результати

На основі (10) для захисту мовної інформації в wav-файлах були створені дві програми. Перша програма змінює початковий wav-файл: значення мовного сигналу замінюються значеннями коефіцієнту $\tilde{c}(t)$. Після прослуховування зміненого wav-файлу чути лише шум. Звуковий сигнал у зміненому wav-файлі поновлюється за допомогою другої програми. При цьому отримуємо wav-файл з практично початковим мовним сигналом. У разі застосування розроблених програм до різних мовних сигналів спостерігалася незначна втрата їх якості, яка на слух практично не помітна. Результати роботи програм для одного з мовних сигналів наведені на рисунках 1 і 2. Початковий мовний сигнал (частота дискретизації 22050 Гц) наведений на рис. 1.

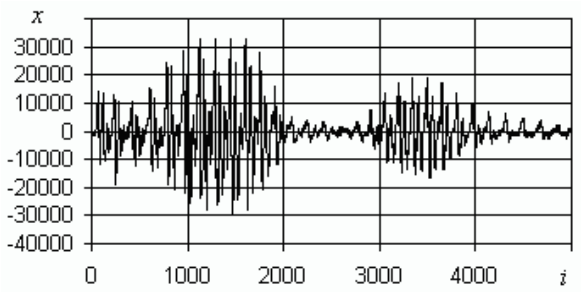

Рис. 1. Початковий мовний сигнал $x(t)$

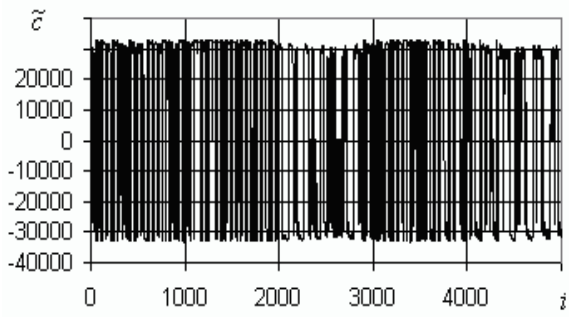

Рис. 2. Змінений мовний сигнал ($\tilde{c}$)

Змінений мовний сигнал — $\tilde{c}(t)$ — зображений на рис. 2. Поновлений мовний сигнал виглядає практично як і початковий (рис. 1).

Висновки

Модифікований підхід для захисту інформації в звукових файлах оснований на зображені нормалізованого мовного сигналу СДР зі змінними коефіцієнтами і заміні значень його ординат значеннями відповідного коефіцієнта СДР. Програмна реалізація обчислення значень коефіцієнта $\tilde{c}(t)$ і поновлення мовного сигналу у випадку його зображення СДР 2-го порядку показала працездатність запропонованого підходу. У поновлених мовних сигналів спостерігалася незначна втрата якості, яка на слух не помітна. Надалі дослідження планується вести у напрямку удосконалення математичної моделі мовного сигналу.

СПИСОК ЛІТЕРАТУРИ

1. Gutowitz H. Cryptography with Dynamical Systems / H. Gutowitz // ESPCI, Laboratoire d'Electronique, Paris, France, 1995. — Режим доступу : http://www.santafe.edu/~hag/crypto/crypto.html.

2. Wong K. Chaotic Encryption Technique / K. Wong // City University of Hong Kong, Department of Electronic Engineering, Hong Kong, 1999. — Режим доступу : http://kitson.netfirms.com/chaos.

3. Kosarev L. Chaos and Cryptography / L. Kosarev // 2001. — Режим доступу : http:// rfic.ucsd.edu/chos/ws2001/kosarev.pdf.

4. Приходько С. Б. Применение стохастических дифференциальных уравнений для защиты звуковой информации / С. Б. Приходько // Труды Одесского. политехнического университета, 2003. — Вип.2 (20). — С. 163—166.

5. Приходько С. Б. Применение стохастических дифференциальных уравнений для защиты информации в звуковых файлах / С. Б. Приходько // Збірник наукових праць УДМТУ. — Миколаїв : УДМТУ, 2003. — № 6 (392). — С. 133—140.

6. Приходько С. Б. Применение компонент стохастических дифференциальных уравнений для защиты информации в звуковых файлах / С. Б. Приходько // Сборник научных трудов НГУ. — Днепропетровск: НГУ, 2004. — Т. 2, № 19. — С. 182—187. — ISBN 966-8271-69-6.

7. Prikhodko S. The application of Johnson transform and stochastic differential equations for protection of the information in sound files / S. Prikhodko // Інтернет—Освіта—Наука—2004 : четверта міжнародна. конференція. ІОН–2004, 28 вересня — 16 жовтня, 2004 р. : зб. матеріалів конф. Т. 2. — Вінниця : УНІВЕРСУМ-Вінниця, 2004. — С. 471—475.

8. Приходько С. Б. Применение преобразования компонент стохастических дифференциальных уравнений для защиты от несанкционированного прослушивания информации в звуковых файлах / С. Б. Приходько // Зб. наук. праць НУК. — Миколаїв : НУК, 2004. — № 5 (398). — С. 117—125. — ISBN 966-321-022-2.

9. Приходько С. Б. Методи побудови математичних моделей нормалізованих сигналів нелінійних стохастичних диференціальних систем / С. Б. Приходько // Проблеми математичного моделювання (28—30 травня 2008 р., м. Дніпродзержинськ) : тези доп. міждержавна наук.-методич. конф. — Дніпродзержинськ : ДДТУ, 2008. — С. 137—139.

10. Кендалл М. Теория распределений / М. Кендалл, А. Стюарт ; пер. с англ. ; под ред. А. Н. Колмогорова. — М. : Наука. Гл. ред. физ.-мат. лит., 1966. — 588 с.

Рекомендована кафедрою захисту інформації

Надійшла до редакції 8.09.08
Рекомендована до друку 20.10.08

Приходько Сергій Борисович — доцент кафедри інформаційних управляючих систем та технологій.

Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв