УДК 681.3:519.62:519.711

С.Б. Приходько, А.В. Пухалевич

Національний університет кораблебудування імені адмірала Макарова, Миколаїв

ВИКОРИСТАННЯ СОНОГРАМ ДЛЯ ОЦІНКИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ СТОХАСТИЧНИХ ДИФЕРЕНЦІАЛЬНИХ РІВНЯНЬ ЗІ ЗМІННИМИ КОЕФІЦІЄНТАМИ

Наведено модифікований підхід для захисту мовної інформації, який оснований на використанні стохастичних диференціальних рівнянь зі змінними коефіцієнтами для нормалізованих звукових сигналів. Виконано оцінку захисту мовної інформації для наведеного підходу із застосуванням сонограм.

Ключові слова: *сонограма, захист мовної інформації, стохастичне диференціальне рівняння.*

Вступ

В галузі захисту інформації однією з актуальних є проблема порушення конфіденційності мовної інформації. 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 при захисті мовних сигналів 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 представляється СДР. В результаті рішення задачі параметричної ідентифікації знаходяться коефіцієнти СДР. Із чисельного рішення СДР визначаються значення білого шуму, який передається замість звукового сигналу. Поновлення сигналу виконується шляхом чисельного рішення 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. В [9] це обмеження вдалося зняти шляхом переходу до СДР зі змінними коефіцієнтами для нормалізованих звукових сигналів та запропоновано відповідний підхід для захисту мовної інформації. Але в [9] не було зроблено оцінку захисту мовної інформації для запропонованого підходу. Одним із способів оцінки захисту є застосування сонограм [10], який дозволяє визначити ступінь захищеності мовної інформації по графічним слідам початкового мовного сигналу на сонограмі зміненого мовного сигналу. **Ціль даної роботи** полягає у тому, щоб виконати оцінку захисту мовної інформації для запропонованого в [9] підходу із використанням сонограм.

Основний матеріал

Суть підходу, який був запропонований у [9], полягає у наступному. Спочатку будуємо СДР для нормалізованого мовного сигналу на основі застосування перетворення Джонсона і метода формуючих фільтрів так, як було запропоновано в [11]. Далі припускаємо, що хоча б один з коефіцієнтів в побудованому СДР залежить від часу і він може бути представлений додатком двох складових: постійною і пульсаційною. Потім з чисельного рішення цього СДР за ординатами нормалізованого звукового сигналу обчислюємо значення обраного коефіцієнту. Значення цього коефіцієнту використовуємо для захисту мовного сигналу. Поновлення початкового мовного сигналу виконуємо у зворотньому порядку. На основі чисельного рішення 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 рішення. Мовний сигнал $x(t)$ може бути перетворений у випадковий процес $z(t)$

з нормальним розподілом (нормалізований випадковий сигнал) за допомогою перетворення Джонсона із сім'ї S_U [7, 8]

$$z = \gamma + \eta \operatorname{Arsh}(\bar{x}),\ -\infty \le x \le +\infty, \qquad (1)$$

де $\bar{x} = (x - \varphi)/\lambda$; γ, η, λ, φ – параметри розподілу Джонсона, $-\infty < \gamma < \infty$, $\eta > 0$, $\lambda > 0$, $-\infty < \varphi < \infty$; $\operatorname{Arsh}(\bar{x}) = \ln\left[\bar{x} + \sqrt{(\bar{x})^2 + 1}\right]$.

Для сім'ї S_U функція щільності ймовірності задається як

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

На основі перетворення (1) 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.

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

$$d\mathbf{z}(t) = \mathbf{A}\mathbf{z}(t)dt + \mathbf{B}dw(t),\ \mathbf{z}(0) = \mathbf{v}. \qquad (2)$$

Тут $w(t)$ – скалярний стандартний вінеровський процес.

Базуючись на СДР (2), отримуємо СДР зі змінними коефіцієнтами

$$d\mathbf{z}(t) = \mathbf{A}(t)\mathbf{z}(t)dt + \mathbf{B}(t)dw(t),\ \mathbf{z}(0) = \mathbf{v}. \qquad (3)$$

На основі (3) складаємо різницеві рівняння. Використовуючи метод Ейлера для (3), різницеві рівняння записуються як

$$\mathbf{z}_{i+1} = \mathbf{z}_i + \left[\mathbf{A}_i\mathbf{z}_i + \mathbf{B}_i n(t_i)\right]\Delta t, \qquad (4)$$

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

На основі (4) за ординатами нормалізованого звукового сигналу обчислюємо значення обраного коефіцієнту, який є випадковим процесом і використовується для захисту мовної інформації.

Запропонований в [9] підхід розглянемо для випадку, коли сигнал $z(t)$ задається СДР

$$\ddot{z} + 2\alpha_z\dot{z} + c(t)z = 2\sqrt{D_z\alpha_z}\,\dot{n}(t), \qquad (5)$$

де $n(t)$ – білий шум; D_z – дисперсія $z(t)$; α_z – коефіцієнт загасання кореляційної функції $z(t)$; $c(t)$ – змінний коефіцієнт, $c(t) = \bar{c} + \tilde{c}(t)$; $\bar{c}$ – 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 (5) в систему

$$\begin{aligned} \dot{z}_1 &= z_2 + 2\sqrt{D_z\alpha_z}\,n(t); \\ \dot{z}_2 &= -4\alpha_z\sqrt{D_z\alpha_z}\,n(t) - 2\alpha_z z_2 - c(t)z_1. \end{aligned} \qquad (6)$$

За методом Ейлера для системи (6) отримуємо наступні рівняння:

$$\begin{aligned} z_{1_{i+1}} &= z_{1_i} + z_{2_i}\Delta t + 2\zeta_i\sqrt{D_z\alpha_z N_0\Delta t}; \\ z_{2_{i+1}} &= z_{2_i} - 4\alpha_z\zeta_i\sqrt{D_z\alpha_z N_0\Delta t} - \\ &\quad - 2\alpha_z z_{2_i}\Delta t - c(t_i)z_{1_i}\Delta t. \end{aligned} \qquad (7)$$

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

На основі (7) 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 зворотньому порядку. За значеннями $\tilde{c}(t)$ на основі (7) знаходимо ординати $z(t)$. А на основі перетворення Джонсона (1) за ординатами $z(t)$ поновлюємо значення ординат мовного сигналу $x(t)$.

Практичні результати. На основі (7) 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 44100 Гц) наведений на рис. 1. Змінений мовний сигнал – $\tilde{c}(t)$ – представлений на рис. 2. Поновлений мовний сигнал виглядає практично як і початковий (рис. 1).

Отримані з допомогою програми Cool Edit сонограми мовних сигналів наведені на рисунках 3 і 4. Сонограма початкового мовного сигналу наведена на рис. 3. Сонограма зміненого мовного сигналу – $\tilde{c}(t)$ – представлена на рис. 4.

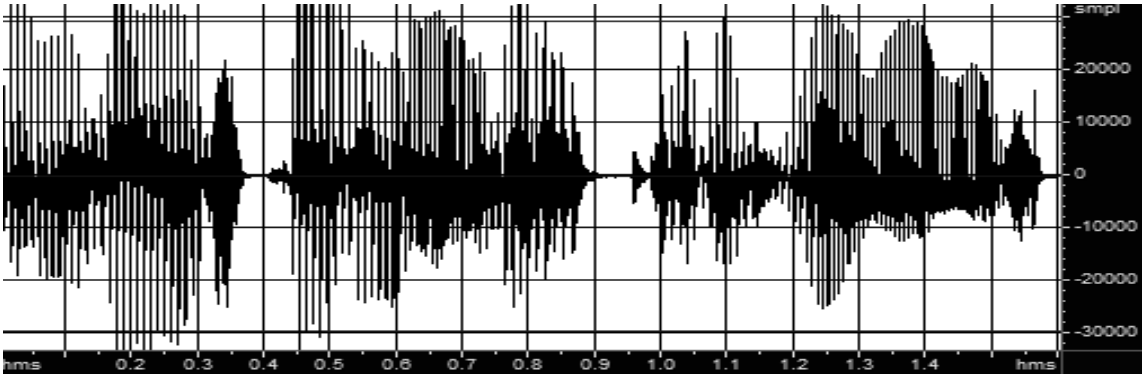

Рис. 1. Початковий мовний сигнал $x(t)$

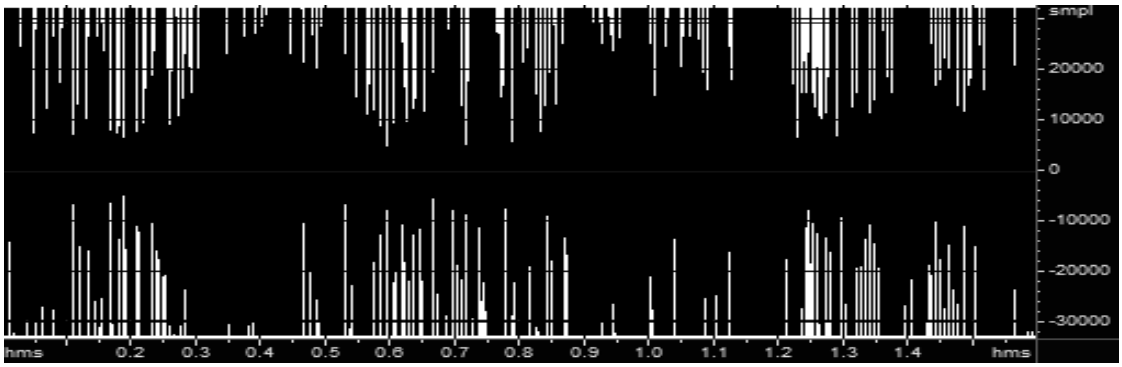

Рис. 2. Змінений мовний сигнал

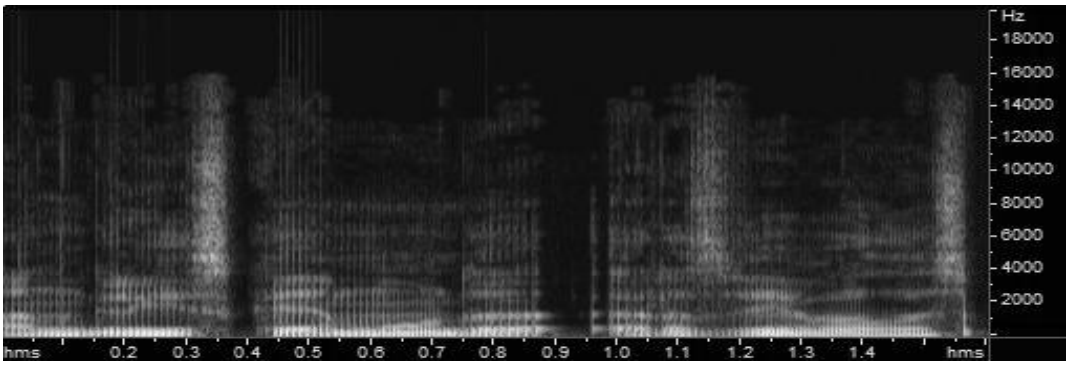

Рис. 3. Сонограма початкового мовного сигналу $x(t)$

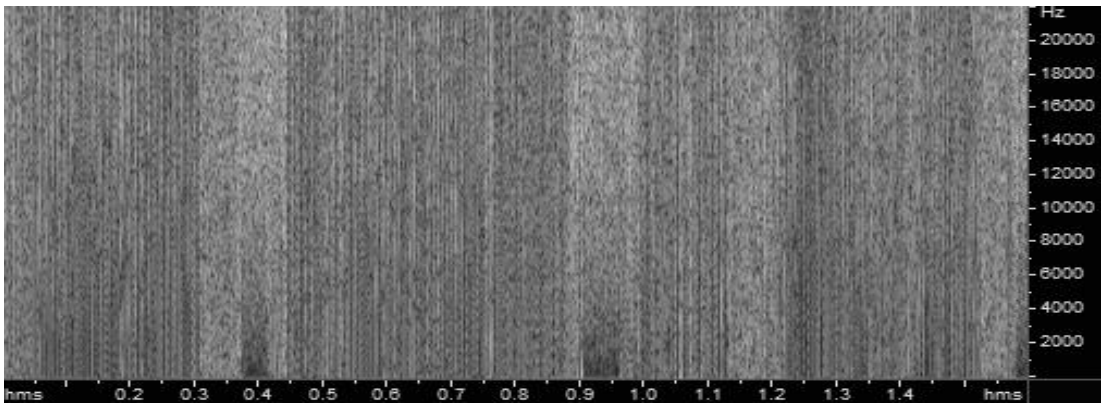

Рис. 4. Сонограма зміненого мовного сигналу $\tilde{c}(t)$

Аналіз вказаних сонограм показує відсутність слідів початкового мовного сигналу в сонограмі зміненого сигналу, тому що амплітуди початкового мовного сигналу в основному розташовані в нижній смузі частот, в той час як амплітуди зміненого сигналу приблизно рівномірно розташовані по всій смузі частот. Це свідчить про добрий ступінь захисту мовного сигналу для підходу, основаному на представленні нормалізованого мовного сигналу СДР зі змінними коефіцієнтами.

Висновки

Наведений в роботі підхід для захисту мовної інформації оснований на представленні нормалізованого мовного сигналу СДР зі змінними коефіцієнтами і заміні значень його ординат значеннями відповідного коефіцієнту СДР. Програмна реалізація обчислення значень коефіцієнту $\tilde{c}(t)$ і поновлення мовного сигналу у випадку його представлення СДР 2-го порядку, а також оцінка захисту із використанням сонограм показали працездатність наведеного підходу. На сонограмі зміненого сигналу відсутні сліди початкового мовного сигналу, що свідчить про добрий ступінь захисту мовного сигналу на основі застосування СДР зі змінними коефіцієнтами. У подальшому дослідження планується вести у напрямку удосконалення математичної моделі мовного сигналу та оцінки його захисту за допомогою інших методів.

Список літератури

1. Gutowitz H. Cryptography with Dynamical Systems [Електронний ресурс] / ESPCI, Laboratoire d'Electronique, Paris, France, 1995. [Електронний ресурс]. – 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. – [Електронний ресурс]. – Режим доступу: http://kitson.netfirms.com/ chaos.

3. Kosarev L. Chaos and Cryptography / L. Kosarev. – 2001. – [Електронний ресурс]. – 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 // Тр. Одес. политехн. ун-та. – 2003. – Вип. 2 (20). – С. 163-166.

5. Приходько С.Б. Применение стохастических дифференциальных уравнений для защиты информации в звуковых файлах / С.Б. Приходько // Зб. наук. 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 // Сб. научных тр. НГУ. – Днепропетровск, 2004. – № 19, Т. 2. – 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 міжн. конф. ІОН – 2004, 28 вересня – 16 жовтня, 2004 р. Зб. мат-в конференції. 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, 2004. – № 5 (398). – С. 117-125. – ISBN 966-321-022-2.

9. Приходько С.Б. Захист мовної інформації на основі стохастичних диференціальних рівнянь зі змінними коефіцієнтами для нормалізованих звукових сигналів / С.Б. Приходько // Вісник Вінницького політехнічного інституту. – 2009. – № 1 (82). – С. 72-75. – ISSN 1997-9266.

10. Халяпин Д.Б. Использование сонограмм для оценки качества активной защиты речевого сигнала / Д.Б. Халяпин, А.А. Рюмин // Информационное противодействие угрозам терроризма. – 2005. – № 4. – [Электронный ресурс]. – Режим доступа: http://www.contrterror. tsure.ru/site/magazine4/06-37-HalyapinRyu-min.htm.

11. Приходько С.Б. Методи побудови математичних моделей нормалізованих сигналів нелінійних стохастичних диференціальних систем / С.Б. Приходько // Тези доповідей міждерж. науково-методич. конф. "Проблеми математичного моделювання 28-30 травня 2008 р. – Дніпродзержинськ: ДДТУ, 2008. – С. 137-139.

Надійшла до редколегії 18.03.2009

Рецензент: д-р техн. наук, проф. К.В. Кошкін, Національний університет кораблебудування імені адмірала Макарова, Миколаїв.

ИСПОЛЬЗОВАНИЕ СОНОГРАММ ДЛЯ ОЦЕНКИ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ НА ОСНОВЕ СТОХАСТИЧЕСКИХ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ С ПЕРЕМЕННЫМИ КОЭФФИЦИЕНТАМИ

С.Б. Приходько, А.В. Пухалевич

Приведен модифицированный подхода для защиты речевой информации, который основан на использовании стохастических дифференциальных уравнений с переменными коэффициентами для нормализированных речевых сигналов. Выполнена оценка защиты речевой информации для приведенного подхода с применением сонограмм.

Ключевые слова: *сонограмма, защита языковой информации, стохастическое дифференциальное уравнение.*

THE APPLICATION OF SONOGRAMS FOR THE PROTECTION ESTIMATION OF SPEECH INFORMATION BASED ON STOCHASTIC DIFFERENTIAL EQUATIONS WITH VARIABLE COEFFICIENTS

S.B. Prikhodko, A.V. Puhalevich

The modified approach for speech information protection based on the use of stochastic differential equations with variable coefficients for normalize speech signals is described. The protection estimation of the speech information for the described approach with use of sonograms is evaluated.

Keywords: *protection to language information, differential equation.*