УДК 004.056.5 (076.5)

Б. Я. Корнієнко, к.т.н., НАУ, м. Київ
А.В. Устьянцев, НАУ, м. Київ

ОБРОБКА ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ДИНАМІЧНОГО ХАОСУ

The article deals with compression and encryption of information using dynamic chaos, given the results of the research work of the generator of chaotic oscillations in various modes.

Вступ

Які недоліки в сучасних комп'ютерах? Якщо живий організм для існування в мінливому середовищі повинен володіти елементами хаотичної поведінки, то можна припустити, що і штучні системи, здатні адекватно взаємодіяти із змінним оточенням і вони повинні бути в тій або іншій мірі хаотичними. Сучасні комп'ютери такими не є. Вони є замкнутими системами з дуже великим, але кінцевим числом станів. Можливо, в майбутньому на основі динамічного хаосу створять комп'ютери нового типу - відкриті з термодинамічної точки зору системи, які здатні адаптуватися до умов зовнішнього середовища.

Проте вже сьогодні хаотичні алгоритми можуть успішно застосовуватися в комп'ютерних технологіях для зберігання, пошуку і захисту інформації. При вирішенні деяких завдань вони виявляються ефективнішими в порівнянні з традиційними методами. Це стосується, зокрема, до роботи з мультимедійними даними. На відміну від текстів і програм мультимедійна інформація вимагає іншого способу організації пам'яті. Мета користувачів - можливість пошуку мелодії, відеосюжету або потрібних фотографій не за їх атрибутами (назві директорії і файлу, даті створення і т. д.), а за змістом або асоціацією, щоб, наприклад, за фрагментом мелодії можна було знайти і відтворити музичний твір. Виявляється, такий асоціативний пошук можна здійснити за допомогою технологій на основі детермінованого хаосу.

Постановка задачі

В статті розглядається стиснення та кодування інформації за допомогою динамічного хаосу, наведені результати досліджень роботи генератора хаотичних коливань у різних режимах.

Нехай можна поставити у відповідність траєкторії конкретні дані, записані у вигляді визначеної послідовностей символів. Тоді частина траєкторій системи знаходилася б у взаємно однозначній відповідності з нашими інформаційними послідовностями. А оскільки кожна траєкторія - це вирішення рівнянь руху системи за певних початкових умов, то і будь-яку послідовність символів можна було б відновити шляхом розв`язання цих рівнянь, задавши як початкові умови невеликий її фрагмент. Таким чином

з’явилася б можливість асоціативного пошуку інформації, тобто пошуку за змістом.

Приклад використання технології – програмний комплекс "Незабудка", призначений для роботи з архівами неструктурованої інформації як на персональних комп’ютерах, так і на інформаційних серверах. "Незабудка" реалізована у вигляді пошукової машини, що працює під стандартними Інтернет-броузерамі типу Netscape і Explorer. Вся інформація в архіві записується і зберігається у вигляді траєкторій хаотичної системи. Для пошуку необхідних документів користувач складає запит шляхом набору в довільній формі декількох рядків тексту, що відноситься до змісту необхідного документа. У відповідь система видасть необхідний документ, якщо вхідна інформація достатня для його однозначного пошуку, або запропонує набір варіантів. При необхідності можна отримати і факсимільну копію знайденого документа. Наявність помилок в запиті не робить істотного впливу на якість пошуку.

Стиснення інформації

Розглянемо можливість застосування теорії хаосу для стиснення інформації. Як генератор хаосу використаний атрактор Лоренца, який описується наступною системою диференціальних рівнянь[1]:

$$\frac{dX}{dt} = \delta(Y - X), \frac{dY}{dt} = X(r - Z) - Y, \frac{dZ}{dt} = XY - bZ \qquad (1)$$

При значеннях параметрів r = 28 δ = 10, b = 8/3 атрактор Лоренца є хаотичною системою. Поведінка такої системи дуже чутлива до щонайменших змін початкових умов. Отже, змінюючи початкові умови, можна забезпечити велику різноманітність форми траєкторій. Атрактор Лоренца в роботі використаний для отримання ділянок кривих, за допомогою яких відбувається апроксимація початкового сигналу. Якщо для початкового сигналу вдається підібрати з бажаною точністю співпадаючу з ним криву, зшиту з декількох кривих, що є розв’язками системи рівнянь Лоренца, то замість зберігання і передачі значень сигналу можна зберігати і передавати тільки значення початкових умов, а також початкові і кінцеві значення тимчасового інтервалу для атрактора Лоренца. Тому об’єм даних істотно зменшується. Розроблена в середовищі MATLAB програма прочитує звуковий файл і підбирає близьку з бажаною точністю до форми цього сигналу криву, зшиту з декількох різних шматків вирішень системи рівнянь Лоренца. Причому ці шматки можуть бути різної довжини. На рис.1 (а) представлений звуковий сигнал з файлу «ding.wav» на тимчасовому проміжку від 0.85 до 0.88 секунд. На рис.1 (б) зображена крива, синтезована з розв`язку системи рівнянь Лоренца: f(t) = rX(t) + δ Y(t)+bZ(t).

Були задані початкові умови X(0)= 1, Y (0)= 0, Z (0)= 0 і значення коефіцієнтів r = 0.0003, δ = 0.0003, b = 0.0003. На рис.1(б) наведена крива f(t) на проміжку від 0.7 до 15.5 умовних одиниць. Видно, що при зсуві сигналу на

рис.1(б) по осі ординат на 3 одиниці і його зчитуванні справа наліво він практично співпадає на заданому тимчасовому інтервалі із звуковим сигналом на рис.1(а).

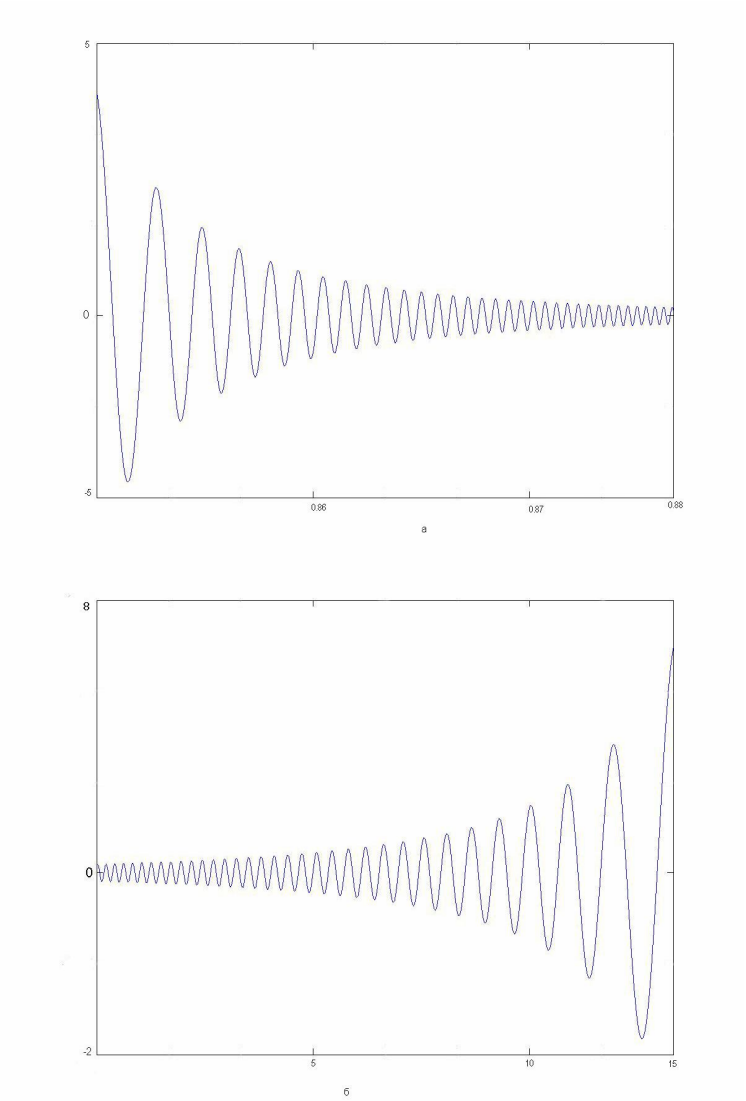


Рис.1. Графіки кривих: а – звукового сигналу; б – розв`язку системи рівнянь Лоренца

Кодування інформації

У зв'язку з бурхливим розвитком комп'ютерних мереж, Інтернет-технологій і бездротових систем зв'язку з'являється все більше завдань, які важко вирішити, використовуючи тільки традиційні підходи. Одним з альтернативних підходів є застосування теорії динамічного хаосу. Тут є два аспекти: інтенсивне зростання продуктивності процесорів, що зводить нанівець багато традиційних криптографічних рішень, стимулює розробку нових принципів кодування інформації; схеми кодування, засновані на хаосі, в більшості випадків виявляються повільнішими і криптографічно слабкішими, ніж їх традиційні аналоги. Слід зазначити, що хаотичні системи за своєю природою, як правило, безперервні. Тому багато методів шифрування, розроблені в традиційній криптографії, не застосовні для хаотичної.

Підбором параметрів і початкових умов атрактора Лоренца можна добитися збігу достатньою мірою окремих фрагментів шифрованого образу з образами, що генеруються за допомогою атрактора Лоренца. Тоді об'єм зашифрованої інформації істотно зменшиться, оскільки достатньо складний образ кодується відносно невеликою кількістю наборів параметрів і початкових умов атрактора Лоренца. Крім того, враховуючи, що атрактор Лоренца дуже чутливий до малих змін параметрів і початкових умов, досліджений метод проявляє високу стійкість до несанкціонованих спроб дешифровки інформації.

Недоліком є те, що значно збільшується час, необхідний для шифрування. Проведений аналіз показав ефективність дослідженого методу кодування.

Для генерування псевдовипадкової послідовності використовуємо рівняння [2]:

$$dx/dt = a(y-x), dy/dt = x(z-\beta), dz/dt = \gamma - xy, \qquad (2)$$

де a, β, γ - додатні коефіцієнти. Особливістю розв`язку цих рівнянь як системи, що володіє хаотичною динамікою, є висока чутливість до зміни параметрів. Саме ця властивість перешкоджає несанкціонованому дешифруванню при використанні для кодування інформації детермінованого хаосу.

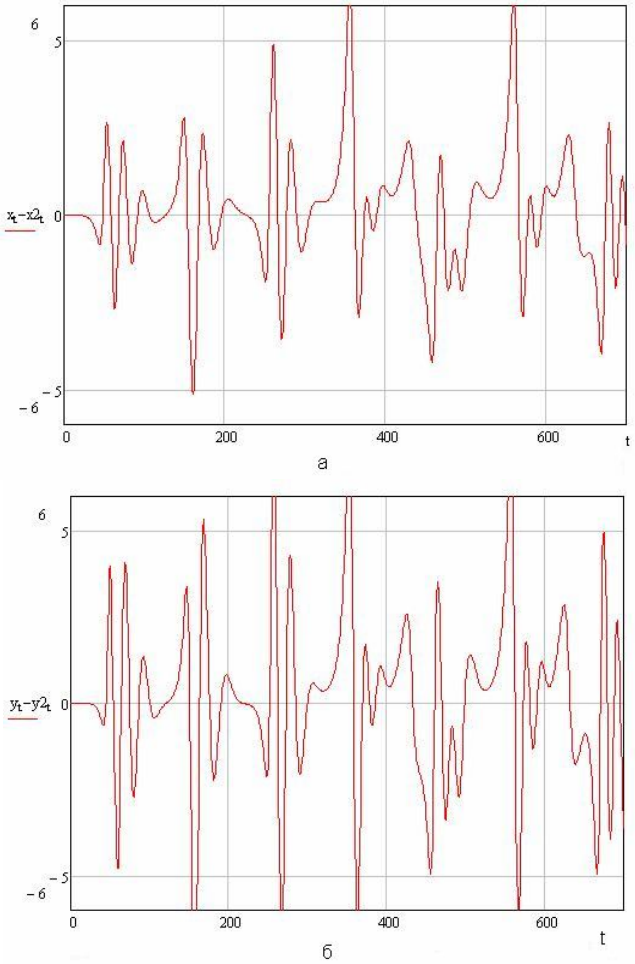
Для ілюстрації «чутливості» системи до зміни параметрів, проведемо порівняння коливання двох автономних систем, кожна з яких описується рівняннями (2) та відрізняється індексами $i(i = 1,2)$ при змінних і позитивних коефіцієнтах. У такому випадку:

$$\begin{aligned} dx_1/dt &= a_1(y_1 - x_1), \quad dx_2/dt = a_2(y_2 - x_2), \\ dy_1/dt &= x_1(z_1 - \beta_1), \quad dy_2/dt = x_2)z_2 - \beta_2), \\ dz_1/dt &= \gamma_1 - x_1 y_1, \quad dz_2/dt = \gamma_2 - x_2 y_2. \end{aligned} \qquad (3)$$

На рис.2 наведені фрагменти реалізації різних коливань при незначній відмінності параметрів a_1 і a_2; при цьому $\beta_1 = \beta_2 = 0,8,\ a_1 = 2,\ \gamma_1 = \gamma_2 = 1,2.$

Значення коефіцієнта a_2 дорівнює 2.1 (*а*), 2.01 (*б*) і 2.000001 (*в*). Початкові умови для всіх змінних дорівнюють 0,1.

При незначній різниці параметрів a_1 і a_2 ($a_1 - a_2 = 0.01$) коливання виникають з помітною затримки, яка збільшується з зменшенням величини $a_1 - a_2$ (*в*). Цю затримку, її умови можна розглядати як «перхідний» процес, легко виправити шляхом виключення початкової ділянки реалізації. Дана властивість необхідна при кодуванні інформації.



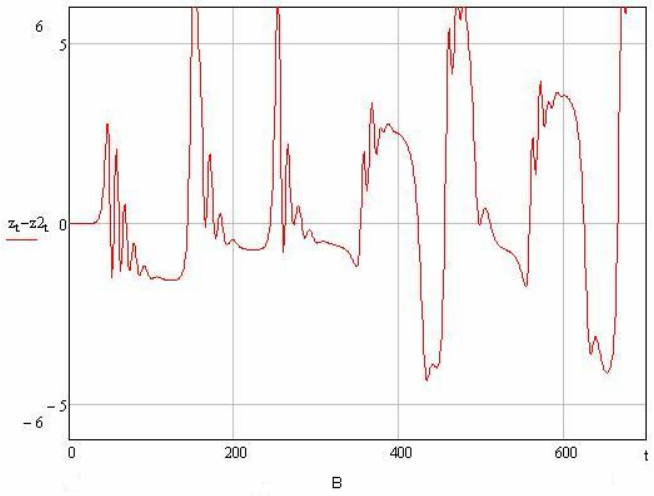


Рис.2. Фрагменти реалізації коливань для різних значень коефіцієнта a_2 а - a_2 =2.1, б - a_2 = 2.01, в - a_2 =2.000001

Використання хаотичних розв'язків розглянутої системи рівнянь дозволяє побудувати досить важкий шифр, який не піддається розкриттю, якщо не відомі точні значення початкових параметрів динамічної системи, за допомогою яких можна розв'язати дане рівняння.

Зв'язок за допомогою хаосу

У більшості сучасних систем зв'язку як носій інформації використовуються гармонійні коливання. Інформаційний сигнал в передавачі модулює ці коливання по амплітуді, частоті або фазі, а в приймачі інформація виділяється за допомогою зворотної операції - демодуляції. Накладення інформації на носій здійснюється або за рахунок модуляції вже сформованих гармонійних коливань, або шляхом управління параметрами генератора в процесі його роботи.

Аналогічним чином можна проводити модуляцію хаотичного сигналу. Проте можливості тут значно ширші. Гармонійні сигнали мають всього три керовані характеристики (амплітуда, фаза і частота). У разі хаотичних коливань навіть невеликі варіації в значенні параметра одного з елементів джерела хаосу приводять до змін характеру коливань, які можуть бути надійно зафіксовані приладами. Це означає, що у джерел хаосу із змінними параметрами елементів потенційно є великий набір схем введення інформаційного сигналу в хаотичний носій (схем модуляції). Сукупність перерахованих чинників стимулювала активні дослідження хаотичних комунікаційних систем.

Висновок

Хаос принципово володіє широким спектром частот, тобто відноситься до широкосмугових сигналів, інтерес до яких в радіотехніці традиційно пов'язаний з їх більшою інформаційною ємкістю в порівнянні з вузькосмуговими коливаннями. Широка смуга частот дозволяє збільшити швидкість передачі інформації, а також підвищити стійкість системи до негативних чинників. Широкосмугові і надширокосмугові системи зв'язки, засновані на хаосі, мають потенційні переваги перед традиційними системами з широким спектром за такими визначальними параметрами, як простота апаратної реалізації, енергетична ефективність і швидкість передачі інформації. Хаотичні сигнали можуть також служити для маскування інформації без використання розширення спектру, тобто при збігу смуги частот інформаційного сигналу і сигналу, що передається.

Таким чином, розглянуто можливості використання хаосу для обробки інформації. Зроблено аналіз експериментальних даних і теоретичних уявлень про інформаційні процеси в системах. Проведено експериментальне дослідження моделі для різних режимів роботи хаотичного генератора.

Отже, інформація може бути прихована і в сигналах, що виглядають шумоподібно. Інформація може бути ефективно передана і прийнята, за допомогою хаотичних сигналів.

1. *Дмитриев А.С., Клецов А.В., Лактюшкин А.М., Панас А.И., Старков С.О.* Сверхширокополосные коммуникационные системы на основе динамического хаоса, Успехи современной радиоэлектроники, 2008, №1, С. 4–18.
2. *Дмитриев А.С., Ефремова Е.В., Максимов Н.А., Григорьев Е.В.* Генератор хаотических колебаний сверхвысокочастотного диапазона на основе автоколебательной системы с 2,5 степенями свободы, Радиотехника и электроника, 2007, Т. 52. № 10, С. 1232-1240.