ДОПОВІДІ
НАЦІОНАЛЬНОЇ
АКАДЕМІЇ НАУК
УКРАЇНИ

8 • 2011

ІНФОРМАТИКА ТА КІБЕРНЕТИКА

УДК 681.62:655

Член-кореспондент НАН України **В. В. Грицик, І. М. Дронюк, М. А. Назаркевич**

Ідентифікація інформації на основі функціональних перетворень періодичних Ateb-функцій

Розроблено метод захисту інформації на основі теорії Ateb-функцій. Запропоновано метод обчислення періодичних Ateb-функцій на основі розкладів в ряди Фур'є та виконано порівняння з методом, що базується на рядах Тейлора. Ідентифікацію інформації реалізовано на основі ортогонального перетворення Уолша–Адамара.

Постановка задачі. У роботі [1] розроблено метод захисту інформації на основі теорії Ateb-функцій. Він полягає у побудові одиничних захисних елементів, які будуються Ateb-функціями з деякими параметрами. Ateb-функції отримуються розкладами в ряди Тейлора. Поряд з проблемою захисту виникає задача ідентифікації інформації. У даній роботі описано метод ідентифікації на основі використання ортогонального тригонометричного перетворення Фур'є Ateb-функцій. Із захищеної інформації виділяється одиничний елемент та перетворюється за допомогою функцій Уолша. Масив еталонів будується на основі Ateb-функцій та відображається у спектральну область. Ідентифікація полягає в порівнянні спектрів перетворення Уолша–Адамара одиничного елемента з еталоном.

Введемо в розгляд вираз

$$\omega = \frac{n+1}{2}\int\limits_0^y (1-\overline{v}^{n+1})^{-m/(m+1)}d\overline{v}, \tag{1}$$

де n, m визначені співвідношеннями

$$\frac{1}{n+1} > 0, \qquad \frac{1}{m+1} > 0. \tag{2}$$

У формулі (1) ω є функцією від y, а також від n і m. Розглядається обернена залежність y від ω, яка є одночасно функцією n і m, та називається синус Ateb-функції [2] $\mathrm{sa}(n, m, \omega)$.

Введемо в розгляд вираз

$$\omega = -\frac{m+1}{2}\int\limits_1^z (1-\overline{u}^{m+1})^{-n/(n+1)}d\overline{u}. \tag{3}$$

Залежність z від ω для інтеграла (3) є функцією n і m називається косинус Ateb-функції $\mathrm{ca}(m,n,\omega)$.

Для моделювання Ateb-функцій, заданих оберненими залежностями до (1), (3), використаємо розклади підінтегральних функцій у функціональні ряди Тейлора та Фур'є. Методи обчислень Ateb-функцій за допомогою розкладів в ряди Тейлора описані в [3]. Оскільки розглядаємо періодичні Ateb-функції, то для моделювання можна використати ряди Фур'є.

Зображення Ateb-функцій за допомогою розкладів в ряди Фур'є та порівняння з розкладами в ряди Тейлора. Періодичну функцію Ateb-синуса з періодом $2\Pi = [-\Pi, \Pi]$ можна розкласти в ряд Фур'є за формулами

$$\mathrm{sa}(n,m,\omega) = \sum_{k=1}^{\infty} b_k \sin\frac{k\pi\omega}{\Pi}, \tag{4}$$

де

$$b_k = \frac{1}{\Pi}\int\limits_{-\Pi}^{\Pi} \mathrm{sa}(n,m,y)\sin\frac{k\pi y}{\Pi}dy = \frac{n+1}{2\Pi}\int\limits_{-\Pi}^{\Pi}\sin\frac{k\pi y}{\Pi}\int\limits_{0}^{-1\leqslant y\leqslant 1}\frac{d\overline{y}}{(1-\overline{y}^{n+1})^{m/(m+1)}}dy. \tag{5}$$

Оскільки функція Ateb-синуса $\mathrm{sa}(n,m,\omega)$ є непарною, то в розкладі (4) відсутні коефіцієнти, що відповідають функції косинуса.

Функція Ateb-косинуса $\mathrm{ca}(m,n,\omega)$ є парною, тому в розкладі відсутні коефіцієнти, що відповідають функції синуса. Розклад в ряд Фур'є для Ateb-косинуса має вигляд

$$\mathrm{ca}(m,n,\omega) = \frac{a_0}{2} + \sum_{k=1}^{\infty} a_k \cos\frac{k\pi\omega}{\Pi}, \tag{6}$$

де

$$\begin{aligned} a_k &= \frac{1}{\Pi}\int\limits_{-\Pi}^{\Pi}\mathrm{ca}(m,n,x)\cos\frac{k\pi x}{\Pi}dx = -\frac{m+1}{2\Pi}\int\limits_{-\Pi}^{\Pi}\cos\frac{k\pi x}{\Pi}\int\limits_{1}^{-1\leqslant x\leqslant 1}\frac{d\overline{x}}{(1-\overline{x}^{m+1})^{n/(n+1)}}dx;\\ a_0 &= \frac{1}{\Pi}\int\limits_{-\Pi}^{\Pi}\mathrm{ca}(m,n,x)\,dx = -\frac{m+1}{2\Pi}\int\limits_{-\Pi}^{\Pi}\int\limits_{1}^{-1\leqslant x\leqslant 1}\frac{d\overline{x}}{(1-\overline{x}^{m+1})^{n/(n+1)}}dx. \end{aligned} \tag{7}$$

Використаємо формули (4)–(7) для обчислення періодичних Ateb-функцій. На рис. 1 наведено графіки Ateb-синуса, обчислені на основі рядів Тейлора та Фур'є. Результати обчислень обома методами збігаються до значень порядку 10^{-6}. Проведено оцінку похибки розрахунків обома методами для параметрів $m = n = 1$, що відповідає випадку збігу Ateb-функцій зі звичайними тригонометричними функціями. Отримані результати показують, що відносна похибка стає найбільшою при значеннях, близьких до $\pm\Pi/2$, і дорівнює 0,004138%, а в інших точках відносна похибка не менша 0,000015%. Тому розроблені обидва методи є ефективними для обчислень Ateb-функцій.

Ортогональні тригонометричні перетворення для Ateb-функцій. Для ідентифікації та відтворення інформації широко використовується математичний апарат ортогональних тригонометричних перетворень, зокрема перетворення Фур'є. Для вирішення завдання ідентифікації інформації, що захищена Ateb-функціями, застосовуємо ортогональні

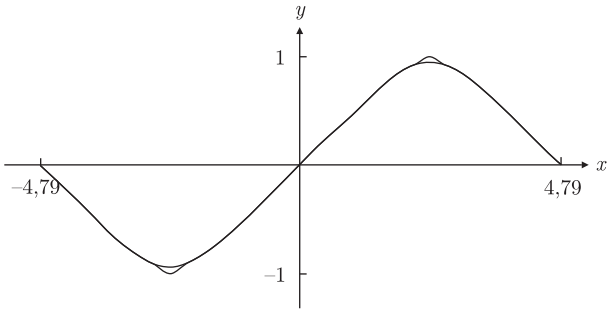

Рис. 1. Порівняння методів обчислень на основі рядів Тейлора та Фур'є для Ateb-синуса $\mathrm{sa}(1, 1/3, x)$ з півперіодом $\Pi = 4{,}7924838018$

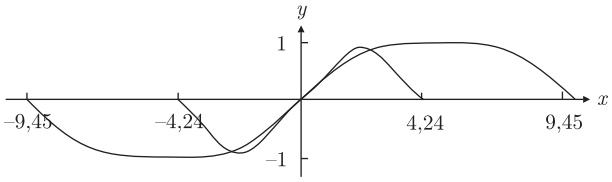

Рис. 2. Графіки Ateb-синуса $\mathrm{sa}(1; 0{,}1; x)$ з півперіодом $\Pi = 4{,}2428412259$ та $\mathrm{sa}(1; 2{,}5; x)$ з півперіодом $\Pi = 9{,}4550717143$

тригонометричні перетворення Фур'є та їх дискретний аналог — ортогональне перетворення Уолша–Адамара.

Враховуючи непарність Ateb-синуса $\mathrm{sa}(n, m, \omega)$, його можна зобразити у вигляді прямого синус-перетворення Фур'є $B(n, m, x)$ [4]

$$B(n, m, x) = \int\limits_{-\infty}^{\infty} \mathrm{sa}(n, m, \omega) \sin(x\omega)\, d\omega. \tag{8}$$

Тоді Ateb-синус подається оберненим синус-перетворенням Фур'є за формулою

$$\mathrm{sa}(n, m, \omega) = \frac{1}{\Pi} \int\limits_{0}^{\infty} B(n, m, x) \sin(x\omega)\, dx. \tag{9}$$

Використовуючи парність Ateb-косинуса $\mathrm{ca}(m, n, \omega)$, наведемо його у вигляді прямого косинус-перетворення Фур'є [4] $A(n, m, x)$

$$A(m, n, x) = \int\limits_{-\infty}^{\infty} \mathrm{ca}(m, n, \omega) \cos(x\omega)\, d\omega. \tag{10}$$

Тоді Ateb-косинус зображується оберненим косинус-перетворенням Фур'є за формулою

$$\mathrm{ca}(m, n, \omega) = \frac{1}{\Pi} \int\limits_{0}^{\infty} A(m, n, x) \cos(x\omega)\, dx. \tag{11}$$

Косинус та синус-перетворення Фур'є застосовують для неперервних функцій. Формули (8)–(11) використані для побудови неперервних спектрів Фур'є-образів функцій. Проте для задач, пов'язаних з інформаційними технологіями, більш доцільним є використання дискретних функцій та перетворень [5]. У цьому випадку застосовують дискретне перетворення Фур'є.

Ідентифікація інформації на основі перетворення Уолша-Адамара для Ateb-функцій. Функції Уолша є базисом для спектрального перетворення інформації, яка подана у дискретному вигляді. Наведемо функцію Ateb-синус на проміжку $[0, \Pi]$ рядом за ортонормованою системою функцій Уолша:

$$\mathrm{sa}\left(n, m, \frac{\omega}{\Pi}\right) = Y(n, m, 0) + \sum_{i=1}^{\infty} Y(n, m, i)\,\mathrm{wal}\left(i, \frac{\omega}{\Pi}\right), \tag{12}$$

де Π — період Ateb-функції, коефіцієнти $Y(n, m, i)$ задано формулами

$$Y(n, m, i) = \frac{1}{\Pi}\int_0^1 \mathrm{sa}\left(n, m, \frac{\omega}{\Pi}\right)\mathrm{wal}\left(i, \frac{\omega}{\Pi}\right)d\omega, \tag{13}$$

$\mathrm{wal}(i, \omega/\Pi)$ — функції Уолша, $i = 2^N$.

Аналогічно для Ateb-косинуса:

$$\mathrm{ca}\left(m, n, \frac{\omega}{\Pi}\right) = Y(m, n, 0) + \sum_{i=1}^{\infty} Y(m, n, i)\,\mathrm{wal}\left(i, \frac{\omega}{\Pi}\right), \tag{14}$$

де коефіцієнти $Y(n, m, i)$ задано формулами

$$Y(m, n, i) = \frac{1}{\Pi}\int_0^1 \mathrm{ca}\left(m, n, \frac{\omega}{\Pi}\right)\mathrm{wal}\left(i, \frac{\omega}{\Pi}\right)d\omega. \tag{15}$$

Якщо обчислення інтегрування у формулах (8), (10) проводити методом прямокутників [6], то дискретне перетворення Фур'є з точністю до постійного множника збігається з оцінкою для неперервних перетворень Фур'є. Для реалізації перетворення Уолша–Адамара побудовано матрицю Адамара, номери стовпців якої відповідають другому аргументу функції Уолша, а номери рядків — першому. Для обчислення обмежимося функціями Уолша при $N = 5$.

Формули (12) та (14) використано для побудови еталону одиничного елемента у процесі ідентифікації. Для реалізації алгоритму ідентифікації здійснюємо перетворення захищеної інформації у цифровий формат. Проводимо попередню обробку інформації: фільтрацію, відкидання шумів. Виділяємо одиничний елемент та відображаємо його у спектральну область за допомогою перетворення Уолша–Адамара. Підтвердження достовірності інформації реалізовано шляхом порівняння спектрів еталонного та отриманого одиничного елемента.

Результати досліджень. Таким чином, розроблено метод захисту та ідентифікації інформації, що базується на теорії Ateb-функцій та дискретних ортогональних тригонометричних перетвореннях. Запропоновано розклад у ряд Фур'є періодичних Ateb-функцій, реалізовано метод обчислення на цій основі та проведено порівняння результатів обчислень

з розкладами у ряди Тейлора. Для методу захисту необхідна висока точність обчислення, що підтверджено проведеними дослідженнями для обох методів. Побудовано графіки періодичних Ateb-функцій залежно від параметрів з використанням розкладів у ряди Тейлора та Фур'є. Для ідентифікації інформації запропоновано використати дискретне ортогональне перетворення Фур'є. За допомогою перетворення Уолша–Адамара проводиться ідентифікація інформації порівнянням з еталоном у спектральній області. Розроблений новий метод може бути використаний для захисту та ідентифікації інформації у надрукованому та електронному вигляді. На основі наведеного методу створено програмні засоби для ефективного захисту та ідентифікації інформації.

1. *Грицик В. В., Дронюк І. М., Назаркевич М. А.* Метод захисту та відтворення інформації засобами Ateb-функцій // Доп. НАН України. – 2008. – № 5. – С. 48–52.
2. *Сеник П. М.* Обращение неполной beta-функции // Укр. мат. журн. – 1969. – **21**, № 3. – С. 325–333.
3. *Грицик В. В., Дронюк І. М., Назаркевич М. А.* Математичні моделі алгоритмів і реалізація Ateb-функцій // Доп. НАН України. – 2007. – № 12. – С. 37–43.
4. *Яцимірський М. М.* Швидкі алгоритми ортогональних тригонометричних перетворень. – Львів: Академ. експрес, 1997. – 219 с.
5. *Рабинер Л., Гоулд Б.* Теория и применение цифровой обработки сигналов. – Москва: Мир, 1978. – 848 с.
6. *Фельдман Л. П., Петренко А. І., Дмитрієва О. А.* Чисельні методи в інформатиці. – Київ: Видавн. група BHV, 2006. – 480 с.

НУ "Львівська політехніка"

Надійшло до редакції 26.11.2010

Corresponding Member of the NAS of Ukraine **V. V. Hrytsyk, I. M. Dronyuk, M. A. Nazarkevych**

Information identification on the basis of functional transformations of periodic Ateb-functions

An information protection method on the basis of Ateb-functions is developed. A method of calculating the periodic Ateb-functions on the basis of the expansion in Fourier series is suggested, and a comparison with the method based on Taylor series is carried out. The information identification is realized by means of the Walsh–Hadamard orthogonal transformation.