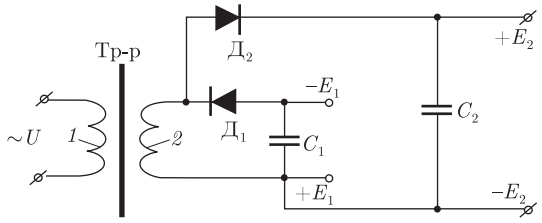

Рис. 4

Приведенные схемы дифференцирующих звеньев экспериментально проверены в Институте проблем машиностроения им. А. Н. Подгорного НАН Украины. Было показано, что схема рис. 2 имеет преимущества перед схемой рис. 1. Самое важное, что она более быстродействующая.

1. *Гинзбург С. Г.* Методы решения задач по переходным процессам в электрических цепях. – Москва: Сов. радио, 1959. – 404 с.
2. *Степаненко И. П.* Основы теории транзисторов и транзисторных схем. – Москва: Госэнергоиздат, 1963. – 376 с.

Институт проблем машиностроения им. А. Н. Подгорного НАН Украины, Харьков

Поступило в редакцию 26.03.2007

УДК 681.62:655

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

Метод захисту та відтворення інформації засобами Ateb-функцій

A method of defense of information in acts that can be used in the pre-print preparation of a model is developed. The method can be used for paper and electronic carriers and is based on the application of networks of the unique form that are the plots of solutions of a system of nonlinear differential equations. These solutions are presented in terms of the orthonormalized system of periodic Ateb-functions. On this basis, a method for the identification of acts in an array is proposed.

Важливе значення для захисту інформації від несанкціонованого використання і підробки мають спеціальні методи, що використовуються на стадії попередньої електронної обробки макету видання. В даній роботі пропонується новий підхід, який може бути використаний для захисту всіх документів, що проходять додрукарську підготовку цінних паперів, бланків суворої звітності, векселів, акцизних марок тощо, а також для захисту будь-яких електронних документів, розміщених у загальне користування (Internet, intranet тощо).

1. Теоретичне обгрунтування методу захисту інформації засобами Ateb-функцій. Розглянемо нелінійне диференціальне рівняння

$$\frac{d^2Y(x)}{dx^2}\left(\frac{dY(x)}{dx}\right)^{\nu}+\lambda Y(x)=0, \tag{1}$$

де x — біжуча координата; λ — параметр, який буде визначений нижче; ν — параметр, що визначає степінь нелінійності ($\nu=0,1,\ldots$). Додамо до (1) крайову умову, яку функція $Y(x)$ повинна задовольняти

$$Y(x)|_{x=0}=Y(x)|_{x=l}=0. \tag{2}$$

Лінійно-незалежні розв'язки (1) виражаються у вигляді [1]

$$Y(x)=X_0\begin{cases}\mathrm{sa}\left(1,\dfrac{1}{v+1},\left(\lambda\dfrac{v+2}{2X_0^v}\right)^{1/(v+2)}x\right),\\ \mathrm{ca}\left(1,\dfrac{1}{v+1},\left(\lambda\dfrac{v+2}{2X_0^v}\right)^{1/(v+2)}x\right),\end{cases} \tag{3}$$

де $\mathrm{sa}(1,m,nx)$, $\mathrm{ca}(1,m,nx)$ — Ateb-функції, $m=1/(\nu+1)$, $n=\lambda(v+2)/(2X_0^{\nu})$; X_0 — довільна стала. Якщо $m=1$, $n=1$, то $\mathrm{sa}(1,1,1x)=\sin x$ і $\mathrm{ca}(1,1,1x)=\cos x$. Параметр l з умови (2) відповідає періоду Ateb-функцій і задається формулою

$$\Pi(m,n)=B\left(\frac{1}{m+1},\frac{1}{n+1}\right)=(n+1)\int\limits_0^1\frac{d\zeta}{(1-\zeta^{n+1})^{m/(m+1)}}, \tag{4}$$

де $\Pi(m,n)$ — період Ateb-функції; B — Beta-функція.

Задовольняючи (2), отримаємо ортонормовану систему періодичних Ateb-функцій $\{Y_k$, $k=0,1,2,\ldots\}$ у вигляді (3) [1], причому λ дорівнює

$$\lambda_k=\frac{2X_0^v}{v+2}\left(\Pi_x\frac{k}{l}\right)^{v+2},\qquad \nu=0,1,\ldots, \tag{5}$$

де Π_x — період Ateb-функції, що задається формулою

$$\Pi_x=(n+1)\int\limits_0^x\frac{d\zeta}{(1-\zeta^{n+1})^{m/(m+1)}}.$$

Підставляючи (5) у (3), ортонормовану систему періодичних Ateb-функцій $Y_k(x,m,n_k)$ подаємо у вигляді

$$Y_k(x,m,n_k)=X_0\begin{cases}\mathrm{sa}(1,m,n_kx),\\ \mathrm{ca}(1,m,n_kx),\end{cases} \tag{6}$$

де

$$m=\frac{1}{\nu+1},\qquad n_k=\left(\lambda_k\frac{v+2}{2X_0^v}\right)^{1/(v+2)}. \tag{7}$$

Ортонормована система періодичних Ateb-функцій $Y_k(x, m, n_k)$ у вигляді (6), (7) є основою методу побудови сіток для захисту інформації. Розвиток інформаційних та апаратних засобів дає можливість легко та швидко проводити моделювання Ateb-функцій. Нами проведено дослідження залежностей характеру поведінки Ateb-функцій від параметрів m, n_k [2].

На основі форми кривих зроблено висновок про суттєву залежність характеру поведінки Ateb-функцій від параметрів m, n, що дає можливість використати їх для побудови ефективних методів захисту та ідентифікації інформації.

2. Опис методу захисту. Розглянемо технологічні процеси додрукарської підготовки макетів видання. Один з методів підготовки макету до тиражування полягає у створенні PostScript-файла. PostScript є мовою програмування, у якій базою опису кривих у символах шрифта стали криві Безьє. PostScript стала універсальною мовою керування вивідними пристроями. На сьогодні це основна мова для виведення інформації. Тому у розробленому методі захисні сітки будуємо за допомогою PostScript.

На останньому етапі додрукарської підготовки сьогодні відома і широко поширена технологія створення pdf–файлів. Даний формат файлів є захищеним. За його допомогою можна друкувати зображення найвищої якості, а також цей формат найчастіше вживається для публікації матеріалів в Інтернеті. Тому запропонований метод реалізується при створенні документів найвищої якості. Він складається з таких кроків.

1. Звичайними засобами переводимо у PostScript-файл потрібну інформацію.

2. Для захисту інформації у PostScript-файл вбудовується програмний код для побудови захисних сіток у вигляді (6) з унікальним набором параметрів m і n з (7), де $n = n_k$ при деякому фіксованому k.

Формулу побудови захищеного зображення можна подати у вигляді

$$\widetilde{v}(x, y, m, n) = v(x, y) + \eta(x, y, m, n), \tag{8}$$

де $v(x, y)$ — початкове зображення; $\eta(x, y, m, n)$ — накладене зображення у вигляді кривих графіків Ateb-функцій; $\widetilde{v}(x, y, m, n)$ — захищене зображення; x, y — координати точки зображення. Координати точки зображення формуються таким чином: беремо біжуче значення x $x \in [0, l]$, обчислюємо y за формулами (6), (7) і перераховуємо у відповідні координати пікселів зображення. Розмножуємо отримані криві, використовуючи формули паралельного перенесення, стиску, розтягу та повороту навколо фіксованої точки. Будуємо відповідні криві. В разі потреби отриману захисну сітку можна повторювати. PostScript-технологія дає можливість накладати на початкове зображення криві Ateb-функцій. Таким чином формується PostScript-файл захищеної інформації.

3. Зі сформованого PostScript-файлу генерується pdf-файл.

Таким чином, запропонованим методом на зображенні документа, що потрібно захистити, буде накладено систему кривих унікальної будови, характер якої залежить від параметрів (7). Проілюструємо роботу методу на прикладах створених нами захисних сіток різної конфігурації. На рис. 1 показано графік Ateb-косинуса, який взято за основу побудованих захисних сіток на рис. 2.

На рис. 2, *а* захисна сітка будується способом паралельного перенесення за координатою y. На рис. 2, *б* захисна сітка утворена методом повороту на кут 10°. Зображення на рис. 2, *в* будується аналогічно рис. 2, *б*, але при цьому застосовується стиск по горизонталі початкової кривої. На рис. 2, *г* показано копіювання сітки. Розроблений метод на базі PostScript-технології дозволяє масштабувати, переносити, повертати і копіювати створені

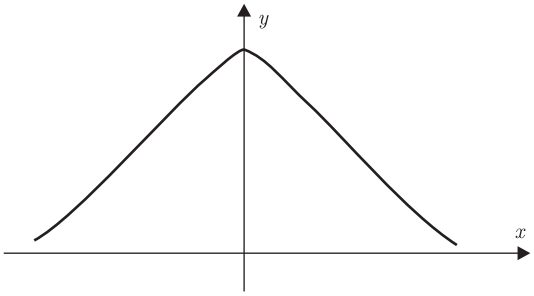

Рис. 1. Графік Ateb-косинуса при $m = 1$, $n = 1/3$

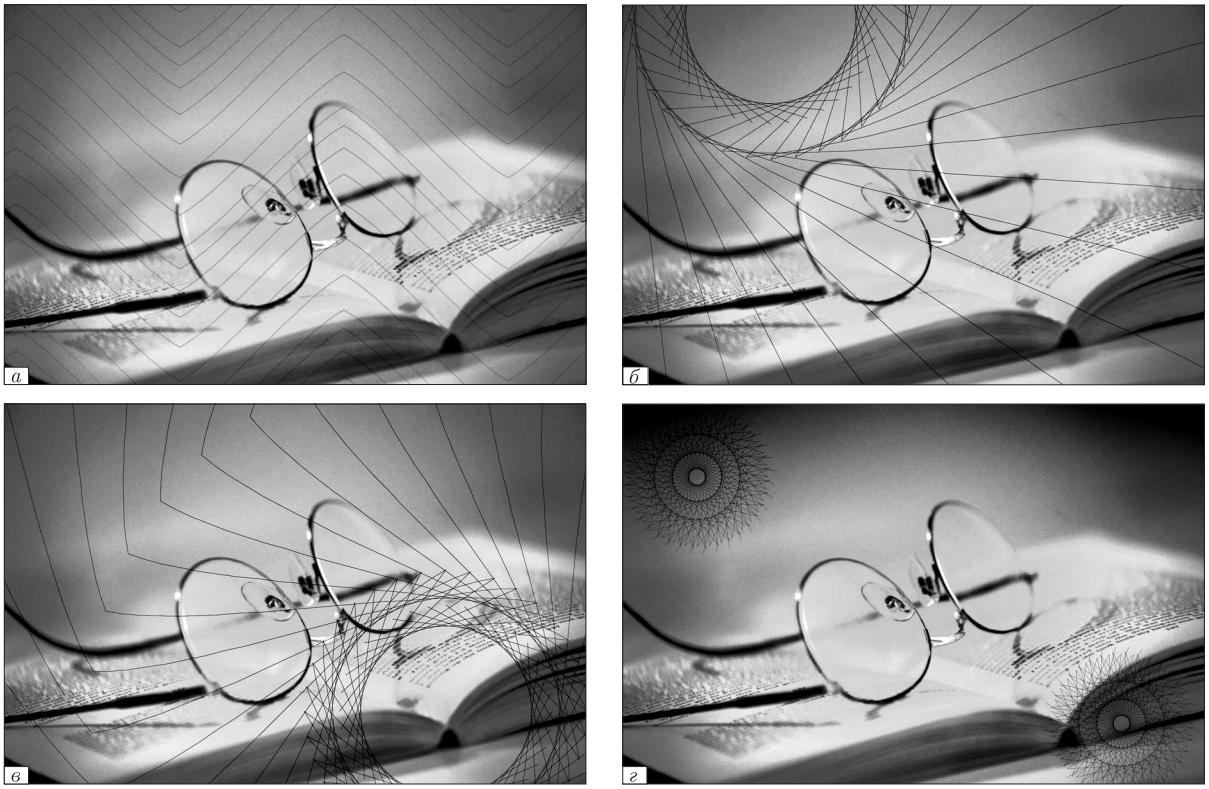

Рис. 2. Захисна сітка, отримана: *а* — паралельним перенесенням; *б* — поворотом; *в* — поворотом і стиском; *г* — стиском та копіюванням

захисні сітки, що продемонстровано на рис. 2, *а*, *б*, *в*, *г*. Для ілюстрації методу вибрано зображення з нейтральним змістом. У даній роботі підготовлено матеріал чорно-білого зображення. Але даний метод дозволяє широко застосовувати різні кольори, товщину ліній та насичення, тому може бути використаний для захисту цінних паперів, бланків суворої звітності, векселів, акцизних марок, а також для захисту будь-яких електронних документів.

3. Метод ідентифікації документів у масиві. Нехай маємо масив N документів $\{D_1, D_2, \ldots, D_N\}$. Кожен документ характеризується своїм набором q параметрів, один з яких, нехай x_1^i, є ключовим

$$D_i = D_i(x_1^i, x_2^i, \ldots, x_q^i), \qquad i = 1, \ldots, N. \tag{9}$$

Для захисту кожному документу D_i додатково присвоюємо набір двох унікальних параметрів m^i, n^i. Для цього набору параметрів будуємо систему Ateb-функцій, зображення яких накладаються до даного документа,

$$D_i = D_i(x_1^i, x_2^i, \ldots, x_q^i, m^i, n^i), \qquad i = 1, \ldots, N. \tag{10}$$

Формулу побудови захищеного i-го зображення у випадку N документів можна подати, аналогічно (8), у вигляді

$$\widetilde{v}^i(x, y, m^i, n^i) = v^i(x, y) + \eta^i(x, y, m^i, n^i), \tag{11}$$

де m^i, n^i — унікальний набір параметрів, притаманний тільки зображенню $\widetilde{v}^i$ відповідного документа D_i. Таким чином, кожний з N-документів захищений власним унікальним набором кривих захисної сітки. Вигляд сіток формується у програмному коді залежно від значень параметрів m^i, n^i.

При ідентифікації документа D_i за характером кривих розпізнаємо значення параметрів m^i, n^i, що однозначно визначені для кожного документа. Це дозволяє однозначно визначити ключове x_1^i, а отже весь набір q параметрів $x_1^i, x_2^i, \ldots, x_q^i$. У випадку, коли існує таке p, що

$$x_p^i \neq x_{p0}^i,$$

де x_{p0}^i — початкове значення параметра x_p^i документа D_i, це свідчить про підробку документа.

Таким чином, в роботі запропоновано новий підхід до захисту інформації на стадії попередньої електронної обробки макету видання, що базується на теорії Ateb-функцій. Подано теоретичне обгрунтування, описаний алгоритм реалізації. Розглянутий метод дозволяє легко змінювати конфігурацію сіток, товщину, колір та насичення ліній. Роботу проілюстровано на прикладах. Розроблений метод дає зображення найвищої якості, тому може бути використаний для захисту як звичайних документів, так і документів суворої звітності, а також електронних документів загального користування.

На основі даного методу запропоновано спосіб ідентифікації документів, що базується на присвоєнні кожному документу унікальних параметрів захисту.

1. *Сокіл Б. І.* Про асимптотичні наближення розв'язку для одного нелінійного неавтономного рівняння // Укр. мат. журн. – 1997. – **49**, № 11. – С. 1580–1583.
2. *Грицик В. В., Назаркевич М. А.* Математичне моделювання складних процесів із істотною нелінійністю на базі Ateb-функцій // Інформаційні технології і системи. – 2006. – **9**, № 1. – С. 13–18.

Державний науково-дослідний інститут інформаційної інфраструктури Держкомзв'язку та інформації України та НАН України, Львів
Національний університет "Львівська політехніка"

Надійшло до редакції 04.12.2007