Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
https://doi.org/10.36930/40330211
Article received 14.04.2023
Article accepted 25.04.2023
UDC 004.8
Correspondence author: Yu. A. Lukashchuk urijlukas@gmail.com
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)

І. Г. Цмоць, Ю. А. Лукащук
Національний Університет "Львівська Політехніка", м. Львів, Україна

УЗАГАЛЬНЕНА АНАЛІТИЧНА МОДЕЛЬ ПОПЕРЕДНІХ НАЛАШТУВАНЬ ДЛЯ НЕЙРОПОДІБНОГО КРИПТОГРАФІЧНОГО ШИФРУВАННЯ ДАНИХ

Розроблено узагальнену аналітичну модель попередніх налаштувань для реалізації нейроподібного шифрування даних. Основними компонентами є блок формування архітектури нейроподібної мережі, блок обчислення матриць вагових коефіцієнтів і блок обчислення таблиць макрочасткових добутків, реалізація якої забезпечує зменшення часу налаштування. Проаналізовано останні дослідження та публікації щодо актуальності проблем під час реалізації нейроподібного криптографічного шифрування даних. Саме тут на допомогу приходить узагальнена аналітична модель попередніх налаштувань. У роботі сформульовано правила для формування архітектури нейроподібної мережі. Структура нейроподібної мережі для криптографічного шифрування даних визначається кількістю нейроподібних елементів. Також розроблено блок обчислення матриць вагових коефіцієнтів. Для цього використано метод сингулярного розкладу матриці та метод обертання Якобі, для знаходження власних векторів і власних значень. Розроблено імітаційну модель для демонстрації роботи цього блоку обчислення, як приклад використано навчальну матрицю розмірністю 13×16 з попередньо заданою архітектурою. Розроблено блок обчислення макрочасткових добутків на підставі таблично-алгоритмічного методу. Розроблено імітаційну модель на підставі матриці вагових коефіцієнтів з розрядністю 8 та заданою архітектурою нейроподібної мережі. Також для обох блоків обчислення розроблено гнучкий користувацький інтерфейс та описано детальне користування ним. Для реалізації поставлених задач обрано мову програмування C# і середовище розроблення Visual Studio 2022. Як технологію розроблення обрано Windows Forms. Для матричних операцій було підключено бібліотеку Accord.Math. Практичною цінністю є те, що розроблені засоби забезпечують швидке обчислення коефіцієнтів для заданої архітектури нейромережі. У підсумку використання такої узагальненої моделі попередніх налаштувань забезпечить швидкість та безпеку шифрування даних.

Ключові слова: нейроподібна мережа; нейроелементи; макрочасткові добутки; таблично-алгоритмічний метод; метод сингулярного розкладу матриці; метод обертання Якобі; власні вектори; власні значення.

Вступ / Introduction

Питання безпечного шифрування даних має вирішальне значення в сучасному цифровому світі, де конфіденційна інформація постійно передається та зберігається онлайн. Криптографічні методи широко використовуються для забезпечення конфіденційності та цілісності даних, але традиційні криптографічні методи можуть бути вразливими до атак хакерів та інших зловмисників.

Нейроподібне криптографічне шифрування даних – це новий перспективний підхід, який використовує штучні нейронні мережі для шифрування та дешифрування даних. Цей підхід базується на принципі того, що нейронні мережі можуть вивчати складні шаблони та взаємозв'язки в даних, що робить їх добре придатними для завдань шифрування.

Однак однією з проблем під час реалізації нейроподібного криптографічного шифрування даних є визначення оптимальних попередніх налаштувань для нейронної мережі. Саме тут на допомогу приходить узагальнена аналітична модель попередніх налаштувань, оскільки вона забезпечує системний підхід для визначення оптимальних налаштувань для заданого набору даних та задачі шифрування.

Отже, розроблення узагальненої аналітичної моделі попередніх налаштувань для нейроподібного криптографічного шифрування даних є актуальною темою дослідження, оскільки вона має потенціал для підвищення безпеки та ефективності шифрування даних у різних сферах, зокрема у фінансах, охороні здоров'я та державному управлінні.

Об'єкт дослідження – побудова аналітичної моделі попередніх налаштувань для нейроподібної мережі.

Предмет дослідження – методи і засоби побудови узагальненої аналітичної моделі попередніх налаштувань для нейроподібного криптографічного шифрування даних, яка спрямована на підвищення безпеки та ефективності криптографічних систем завдяки використанню нейронних мереж.

Мета роботи – розробити узагальнену аналітичну модель для нейроподібного криптографічного шифру-

Інформація про авторів:
Цмоць Іван Григорович, д-р техн. наук, професор, кафедра автоматизованих систем управління.
Email: Ivan.tsmots@gmail.com; https://orcid.org/0000-0002-4033-8618
Лукащук Юрій Андрійович, аспірант, кафедра автоматизованих систем управління.
Email: urijlukas@gmail.com; https://orcid.org/0000-0002-8933-8635

Цитування за ДСТУ: Цмоць І. Г., Лукащук Ю. А. Узагальнена аналітична модель попередніх налаштувань для нейроподібного криптографічного шифрування даних. Науковий вісник НЛТУ України. 2023, т. 33, № 2. С. 78–83.
Citation APA: Tsmots, I. H., & Lukashchuk, Yu. A. (2023). Generalized analytycal model of presetting for neural cryptographic data encryption. *Scientific Bulletin of UNFU*, 33(2), 78–83. https://doi.org/10.36930/40330211

вання даних, яка спрямована на підвищення безпеки та ефективності шифрування даних порівняно з наявними методами. Робота також має на меті дослідити ефективність запропонованої моделі за допомогою різних симуляцій та експериментів.

Для досягнення зазначеної мети визначено такі основні завдання дослідження:

- проаналізувати останні дослідження та публікації;
- розробити блок формування архітектури нейроподібної мережі;
- розробити блок обчислення значень елементів матриць вагових коефіцієнтів на підставі вдосконаленого методу сингулярного розкладу матриці;
- розробити блок обчислення значень елементів таблиць макрочасткових добутків.

Аналіз останніх досліджень та публікацій. Проаналізувавши публікації [4, 6, 19], з'ясовано, що нейромережевий криптографічний захист даних переважно реалізується програмним способом. Основним недоліком такої реалізації є складність забезпечення режиму реального часу.

У роботах [4, 13, 28, 29] розглянуто шляхи адаптації автоасоціативної нейронної мережі з неітераційним навчанням до задач криптографічного захисту даних. Особливістю функціонування такої нейромережі є можливість попереднього обчислення вагових коефіцієнтів і їх подальше використання у шифруванні даних.

У роботах [2, 11, 12, 13, 28, 29] проаналізовано основні шляхи розвитку бортових засобів криптографічного захисту передачі даних у реальному часі, який показав, що перспективним шляхом розвитку є використання нейромережевих методів для шифрування та дешифрування даних [10, 25, 27].

Аналізуючи роботи [2, 11, 12, 24], встановлено, що для попереднього обчислення вагових коефіцієнтів використовується метод головних компонент, який застосовує систему власних векторів, які відповідають власним значенням коваріаційної матриці вхідних даних.

Аналіз методів обчислення скалярного добутку з ваговими коефіцієнтами, які є наперед відомими [17, 20, 21, 22] показав, що одним із найефективнішних методів є таблично-алгоритмічний, який зводиться до операцій читання макрочасткових добутків, додавання та зсуву. Недоліком цього методу є те, що він орієнтований на роботу із вхідними даними та ваговими коефіцієнтами у форматі з фіксованою комою.

Результати дослідження та їх обговорення / Research results and their discussion

Виконання нейроподібного криптографічного шифрування / дешифрування даних передбачає здійснення попередніх налаштувань. Такі налаштування зводяться до вибору структури нейроподібної мережі, обчислення матриці вагових коефіцієнтів і таблиці макрочасткових добутків. Узагальнена аналітична модель попередніх налаштувань запишеться так:

$$P_{Mi} = f_{P_{Mi}}(f_W(f_{(X\to Nm)})), \quad (1)$$

де: P_{Mi} – макрочастковий добуток; $f_{P_{Mi}}$ – обчислення таблиці макрочасткових добутків P_{Mi}; f_W – обчислення матриці вагових коефіцієнтів; $f_{(X\to Nn)}$ – формування структури нейроподібної мережі, параметри якої визначаються розрядністю m повідомлення X та розрядністю входів нейроелемента n.

Із формули (1) видно, що модель попередніх налаштувань реалізується на базі трьох компонентів: перший – формування структури нейроподібної мережі; другий – обчислення матриці вагових коефіцієнтів; третій – обчислення таблиці макрочасткових добутків.

Блок формування архітектури нейроподібної мережі. Структура нейроподібної мережі для криптографічного шифрування даних визначається кількістю нейроподібних елементів, які обчислюються за формулою

$$N = n/m, \quad (2)$$

де N – кількість нейроелементів. Для системи команд управління, розрядність якої m = 16, кількість нейроподібних елементів N може бути 16, 8, 4 і 2 із розрядністю входів n відповідно 1, 2, 4, 6 і 8.

Імітаційна модель обчислення матриць вагових коефіцієнтів. Для обчислення матриці вагових коефіцієнтів використаємо метод сингулярного розкладу матриці (англ. *Singular Value Decomposition*, далі SVD):

$$A = UDV^T, \quad (3)$$

де: A – матриця вхідних даних $N\times n$; U – ліва сингулярна матриця $N\times N$, стовпці містять власні вектори матриці AA^T; D – діагональна матриця $N\times n$, що містить сингулярні (власні) значення; V – права сингулярна матриця n x n, стовпці містять власні вектори матриці A^TA.

Розрахунок власних значень і власних векторів виконується за методом обертання Якобі, за якого обчислення власних значень і власних векторів симетричної матриці здійснюється ітераційним шляхом. Такий процес обчислення власних векторів відомий як діагоналізація. Для побудови цієї послідовності використовується спеціально підібрана матриця обертання J_i, норма наддіагональної частини якої обчислюється так:

$$\left\|A^{(i)}\right\|_{off} = \sqrt{\sum_{1\le j<\kappa\le v}\left(a_{jk}^{(i)}\right)^2} \quad (4)$$

та зменшується при кожному двосторонньому обертанні матриці

$$A^{(i+1)} = J_i^T \cdot A^{(i)} \cdot J_i . \quad (5)$$

Для розрахунку матриці U за методом Якобі передається результат добутку AA^T, а для знаходження матриці V – результат добутку A^TA. При знаходженні матриці D достатньо взяти власні значення, які були знайдені при розрахунку матриці U чи матриці V і розмістити їх на головній діагоналі. Після знаходження матриць U, V та D відбувається розрахунок вагових коефіцієнтів за такою формулою:

$$Aw = UD, \quad (6)$$

де: A – вхідна матриця розмірністю $N\times n$; W – матриця вагових коефіцієнтів розмірністю $n\times n$. Обчислення матриці вагових коефіцієнтів W виконується за такою формулою:

$$w = A^{-1} \cdot UD , \quad (7)$$

де матриця A^{-1} дорівнює:

$$A^{-1} = VD^{-1} \cdot U^T . \quad (8)$$

Підставивши (8) у (7), отримаємо формулу для обчислення вагових коефіцієнтів, яка запишеться так:

$$w = VD^{-1} \cdot U^T \cdot UD . \quad (9)$$

Розмірність таблиць вагових коефіцієнтів визначається кількістю нейроподібних елементів, на підставі яких синтезована нейроподібна мережа. Так, для шифрування команд управління використовуються нейроподібні мережі з кількістю нейроподібних елементів 16,

8, 4, і 2. Розмірність матриць вагових коефіцієнтів для таких нейроподібних мереж відповідно буде 16×16, 8×8, 4×4, 2×2.

Для обчислення вагових коефіцієнтів, які використовуються при криптографічному шифруванні вхідних повідомлень, було розроблено імітаційну модель. Реалізацію імітаційної моделі обчислення вагових коефіцієнтів здійснено мовою програмування C# у середовищі розроблення Visual Studio 2022 з використанням технології розроблення Windows Forms. Розроблена імітаційна модель забезпечує обчислення матриці вагових коефіцієнтів для вибраної архітектури нейроподібної мережі.

Для навчання системи використовувалась матриця із 16-ти розрядних повідомлень (табл. 1).

Табл. 1. Навчальна матриця / Learning matrix

1	1	0	1	1	0	0	1	0	1	1	0	1	0	1	1
1	0	0	0	0	1	1	0	0	1	0	1	1	0	1	1
1	0	1	0	1	0	0	0	1	1	1	0	1	0	1	0
1	0	0	0	1	0	1	1	0	0	0	1	0	1	1	1
0	1	0	0	1	1	0	1	1	1	1	0	0	0	0	1
1	0	0	1	0	0	1	1	0	1	1	1	0	1	0	0
0	1	0	0	0	0	1	0	0	1	0	0	1	0	0	0
0	0	1	0	0	1	0	1	0	1	0	0	0	1	1	1
1	0	0	1	1	1	0	0	0	1	0	1	0	0	1	0
0	1	1	0	1	1	1	1	1	1	1	1	0	1	0	0
1	0	1	0	0	0	1	1	1	1	0	0	0	0	0	1
0	1	0	1	0	1	0	1	0	1	1	1	0	0	0	1
0	1	1	0	0	0	1	1	0	1	0	0	0	1	0	1

Розроблено користувацький інтерфейс імітаційної моделі обчислення вагових коефіцієнтів (рис. 1).

Рис. 1. Користувацький інтерфейс імітаційної моделі обчислення вагових коефіцієнтів / User interface of the simulation model for calculating weighting coefficients

1. Користувацький інтерфейс імітаційної моделі обчислення вагових коефіцієнтів забезпечує такі можливості:

- *Input Data* – ввід даних про архітектуру нейроподібної мережі:
- *Bit size of message* – числове поле для введення розрядності повідомлення;
- *Bit size of inputs* – числове поле для введення розрядності входів;
- *Neural Elements* – маркер, який відображає кількість нейроподібних елементів;
- *Inputs Amount* – маркер, у якому відображається кількість входів;
- *Message* – текстове поле для введення повідомлення для шифрування.
- *Get init mat* – кнопка, яка відповідає за завантаження навчальної матриці в аплікацію, та відображення її у *Learning matrix/Decimal matrix*
- *SVD* – кнопка, яка запускає алгоритм навчання нейромережі для лінійного шифрування даних;
- *Weights* – кнопка, яка запускає алгоритм навчання нейромережі. Результат записується у відповідні таблиці *Weights.*

2. *Learning matrix/Decimal matrix* – спеціальний об'єкт *DataGridView*, у якому відображається вхідна матриця для навчання нейромережі.

3. *Improved SVD approach/Nonlinear approach* – контейнер *b*, який містить результат знаходження вагових коефіцієнтів, а також засоби шифрування та дешифрування вхідного повідомлення:

- *Weights* – спеціальний об'єкт DataGridView, у якому відображається матриця вагових коефіцієнтів;
- *Coefficients* – спеціальний об'єкт DataGridView, у якому відображаються коефіцієнти, необхідні для нелінійного шифрування даних.

4. *Encryption* – спеціальний підрозділ, який відповідає за шифрування даних:

- *Input* – відображає вхідне повідомлення для шифрування;
- *Result* – відображає результат шифрування.

Розроблена імітаційна модель обчислення вагових коефіцієнтів просто налаштовується для обчислення значень елементів матриць вагових для різних архітектур нейроподібних мереж.

Імітаційна модель обчислення таблиць макрочасткових добутків. Обчислення значень елементів таблиць макрочасткових добутків для вагових коефіцієнтів з плавучою комою $W_j = w_j 2^{E_{Wj}}$ (де w_j – мантиса W_j вагового коефіцієнта, E_{W_j} – порядок W_j вагового коефіцієнта) передбачає виконання таких операцій:

- визначення найбільшого спільного порядку вагових коефіцієнтів E_{Wmax} ;
- обчислення різниці порядків для кожного W_j вагового коефіцієнта $\Delta E_{W_j} = E_{Wmax} - E_{W_j}$;
- зсунення вправо мантиси w_j на різницю порядків ΔE_{W_j} ;
- визначення максимальної кількості розрядів переповнення q для макрочасткових добутків P_{Mi};

- отримання масштабованих мантис w_j^h шляхом їх зсуву вправо на q розрядів переповнення обчислених макрочасткових добутків P_{Mi};
- додавання до найбільшого спільного порядку E_{Wmaxc} кількості розрядів переповнення $E_{Wmax}^h = E_{Wmax} + q$.

Значення елементів таблиці макрочасткових добутків можна обчислити за такою формулою:

$$P_{Mi} = \begin{cases} 0, \quad \text{якщо} \quad x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 0; \\ w_1^h, \quad \text{якщо} \quad x_{1i} = 1, \quad x_{2i} = x_{3i} = \ldots = x_{Ni} = 0; \\ w_2^h, \quad \text{якщо} \quad x_{1i} = 0, x_{2i} = 1, x_{3i} = \ldots = x_{Ni} = 0; \\ w_1^h + w_2^h, \quad \text{якщо} \quad x_{1i} = 1, x_{2i} = 1, x_{3i} = \ldots = x_{Ni} = 0; \\ \vdots \\ w_j^h, j = \overline{2, N}, \cdots \text{якщо} \quad x_{1i} = 0, x_{2i} = x_{3i} = \ldots = x_{Ni} = 1; \\ w_j^h, j = \overline{1, N}, \quad \text{якщо} \quad x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 1, \end{cases} \quad (10)$$

де: $x_{ji}, j = \overline{1, N}$ – адресні входи таблиці, w_j^h – мантиса W_j вагового коефіцієнта, зведена до найбільшого спільного порядку. Кількість таблиць макрочасткових добутків для шифрування/дешифрування команд дорівнює кількості нейроподібних елементів у мережі. Обсяг пам'яті, потрібної для зберігання таблиці макрочасткових добутків, становить:

$$Q=2^k, \quad (11)$$

де k – кількість входів нейроподібного елемента.

Для нейроподібних мереж із 16, 8, 4 і 2 нейроподібними елементами кількість таблиць та їх обсяги відповідно дорівнюють: 16 таблиць обсягом $Q=2^{16}$; 8 таблиць.

Для реалізації імітаційної моделі обчислення значень елементів таблиці макрочасткових добутків обрано мову програмування C#, середовище розроблення Visual Studio 2022, а технологію розроблення Windows Forms (рис. 2).

Для демонстрації роботи програми було підготовлено приклад для роботи з такою архітектурою: $m = 2$, $k = 8$, $N = 8$, а також матрицею вагових коефіцієнтів для нейроподібної мережі з 8-ма нейроелементами. Обчислені значення елементів матриці вагових коефіцієнтів наведено в табл. 2.

Табл. 2. Матриця вагових коефіцієнтів / Weighting coefficient matrix

0,2365	-0,0436	-0,0413	0,0702	0,2453	-0,097	-0,8856	0,2861
0,1322	-0,4923	-0,0464	-0,1332	-0,8273	-0,0889	-0,1668	0,0035
0,1567	0,3824	0,2335	0,8059	-0,3371	-0,0931	0,0096	0,0525
0,2542	0,4588	0,6344	-0,5124	-0,1834	0,1373	-0,0836	0,0219
0,2234	-0,0371	0,0224	0,0668	0,0859	-0,0083	-0,2139	-0,9438
0,5489	-0,2009	0,1376	-0,0496	0,2193	-0,6944	0,3128	0,0929
0,3888	0,5098	-0,7202	-0,1861	-0,1812	-0,0012	0,0523	0,0134
0,5787	-0,3118	0,0313	0,1544	0,1409	0,688	0,1848	0,1253

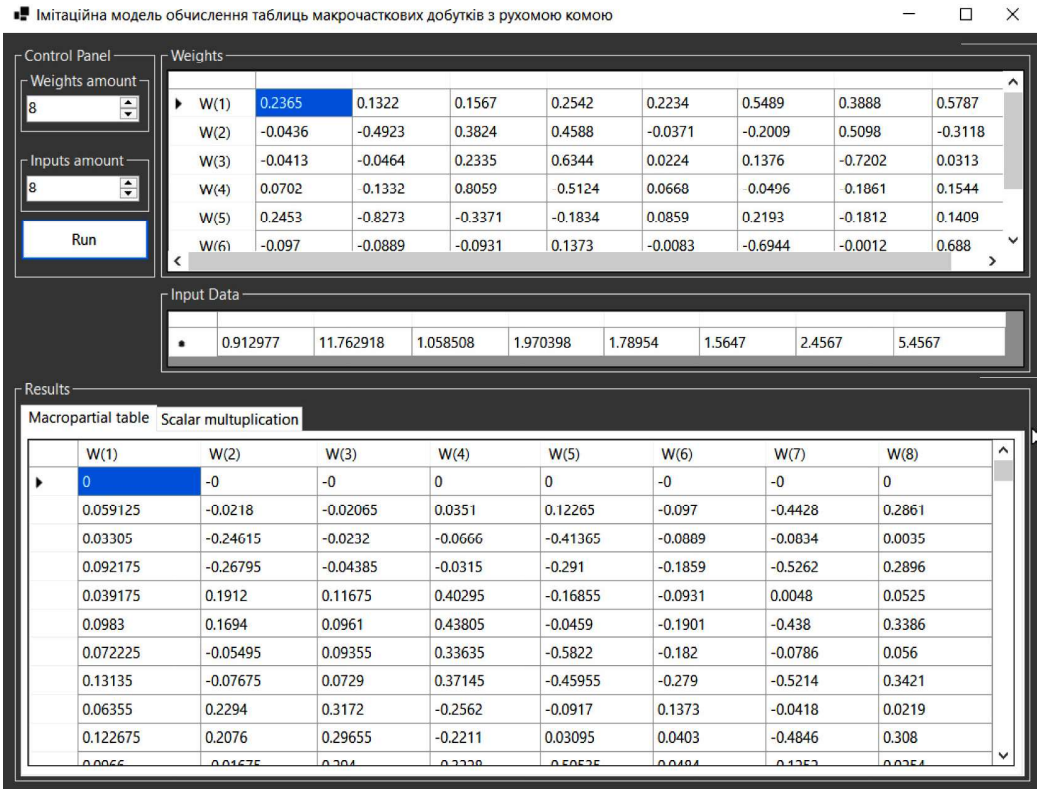

Рис. 2. Користувацький інтерфейс імітаційної моделі обчислення таблиці макрочасткових добутків / User interface of the simulation model for calculating the macroparticle product table

Розроблено користувацький інтерфейс імітаційної моделі обчислення таблиці макрочасткових добутків (див. рис. 2). Користувацький інтерфейс імітаційної моделі обчислення таблиці макрочасткових добутків забезпечує такі можливості:

1. *Control Panel* – панель керування аплікації.
2. *Weights amount* – ввід кількості вагових коефіцієнтів.
3. *Inputs amount* – ввід кількості входів.
4. *Run* – кнопка запуску розрахунку макрочасткових добутків.
5. *Weights* – таблиця відображення вхідних вагових коефіцієнтів.
6. *Input Data* – таблиця відображення вектора вхідних даних.

7. *Macropartial table* – таблиця відображення розрахованих макрочасткових добутків.
8. *Scalak multiplication* – таблиця відображення розрахованих скалярних добутків, та результат звичайного множення, а також точність розрахунку.
9. *Scalar multiplication* – кнопка розрахунку скалярного добутку за допомогою макрочасткових добутків.
10. *Multiplication* – кнопка звичайного множення вхідних даних.
11. *Result* – відображає результат дешифрування.

Розроблена імітаційна модель обчислення значень елементів таблиць макрочасткових добутків забезпечує швидке їх обчислення для різної кількості операндів при таблично-алгоритмічній реалізації скалярного добутку.

Обговорення результатів дослідження. Порівнюючи отримані результати дослідження з працями [7, 9, 14, 19], можна дійти висновку, що наша модель попередніх налаштувань додає гнучкості та швидкості під час шифрування даних.

У роботах [9, 19] автори розраховують матрицю вагових коефіцієнтів тільки для квадратних навчальних матриць. У нашій же реалізації завдяки використанню покращеного методу сингулярного розкладу матриць є змога працювати із навчальними матрицями довільної розмірності. Також наш підхід підвищує криптостійкість унаслідок складності розрахунку вагових коефіцієнтів.

Порівнюючи із роботою [7, 14], наш принцип шифрування даних дає змогу пришвидшити процес, оскільки вже є попередньо розрахована таблиця макрочасткових добутків за таблично-алгоритмічним методом, тому немає потреби виконувати складні розрахунку у реальному часі, які показано у роботі [7].

Також обидва блоки обчислення чудово працюють між собою. Оскільки вагові коефіцієнти ідуть як вхідні дані для розрахунку макрочасткових добутків. І вже під час самого шифрування достатньо просто використовувати результати роботи блоку обчислення таблиці макрочасткових добутків.

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – розроблено узагальнену модель попередніх налаштувань для реалізації нейроподібного шифрування даних, основними компонентами якої є блок формування архітектури нейроподібної мережі, блок обчислення матриць вагових коефіцієнтів і блок обчислення значень елементів таблиць макрочасткових добутків, реалізація якої забезпечує зменшення часу налаштування.

Практична значущість результатів дослідження – розроблена узагальнена модель попередніх налаштувань забезпечує підвищення безпеки та ефективності шифрування даних.

Висновки / Conclusions

Отже, розроблено узагальнену аналітичну модель для нейроподібного криптографічного шифрування даних та досліджено ефективність запропонованої моделі з використанням методики симуляцій та експериментів. Зокрема:

1. Розроблено модель попередніх налаштувань для реалізації нейроподібного шифрування/дешифрування даних, основними компонентами якої є блок формування архітектури нейроподібної мережі, блок обчислення значень елементів матриць вагових коефіцієнтів і блок обчислення таблиць макрочасткових добутків. Втілення моделі забезпечує зменшення часу налаштування.
2. Розроблено імітаційну модель та наведено користувацький інтерфейс для обчислення значень елементів матриць вагових коефіцієнтів для заданої архітектури нейроподібних мереж.
3. Розроблено імітаційну модель та наведено користувацький інтерфейс для обчислення значень елементів таблиць макрочасткових добутків для таблично-алгоритмічної реалізації скалярного добутку.
4. Використання розроблених моделей забезпечує зменшення часу налаштування нейроподібних мереж для шифрування/дешифрування даних.

References

1. Amos, R. O., Jagath, C. R. (2006). *FPGA Implementations of Neural Networks,* Springer, 363 p.
2. Arvandi, M., Wu, S., Sadeghian, A., Melek, W. W., & Woungang, I. (2006). Symmetric cipher design using recurrent neural networks. Proceedings of the IEEE *International Joint Conference on Neural Networks*, 2039–2046.
3. Chang, A. X. M., Martini, B., & Culurciello, E. (2015). *Recurrent neural networks hardware implementation on FPGA*: arXiv preprint arXiv: 1511.05552.
4. Chi Zhang, Wei Zou, Liping Ma, & Zhiqing Wang. (2020). Biologically inspired jumping robots: A comprehensive review. *Robotics and Autonomous Systems*, Vol. 124, 103362.
5. Corona-Bermúdez, E., Chimal-Eguía, J. C., & Téllez-Castillo, G. (2022). Cryptographic Services Based on Elementary and Chaotic Cellular Automata. *Electronics*, 11(4), 613. https://doi.org/10.3390/electronics11040613
6. Diamantaras, K. I., & Kung, S. Y. (1996). Principal Component Neural Networks. *Theory and Applications* (Wiley, 1996), 270 p.
7. Dong, T., & Huang., T. (2019). Neural cryptography based on complex-valued neural network. IEEE *Transactions on Neural Networks and Learning Systems*, Vol. 31, No. 11.
8. Khavalko Viktor, & Tsmots Ivan. (2019). Image classification and recognition on the base of autoassociative neural network usage. 2019 IEEE 2*nd Ukraine conference on electrical and computer engineering*, UKRCON-2019: conference proceedings (Lviv, Ukraine, July 2-6, 2019), 1118–1121.
9. Rabyk, V., Tsmots, I., Lyubun, Z., & Skorokhoda, O. (2020). Method and Means of Symmetric Real-time Neural Network Data Encryption. 2020 IEEE 15*th International Scientific and Technical Conference on Computer Sciences and Information Technologies*, CSIT 2020 – Proceedings, 1, 47–50, 9322006.
10. Riznyk, O. Ya., Tkachenko, R. O., & Kinash, Yu. E. (2019). Neural network technology for protection and real-time data transmission using noise-like codes. *Innovative technologies in the development of modern society: collection of abstracts of reports of the international scientific and practical conference* (Lviv, April 18-19, 2019), 19–23.
11. Sagar V., & Kumar, K. (2014). A Symmetric Key Cryptographic Algorithm Using Counter Propagation Network (CPN). Proceedings of the 2014 *ACM International Conference on Information and Communication Technology for Competitive Strategies*, Vol. 2, No. 9, 78–91.
12. Shihab, K. (2006). A backpropagation neural network for computer network security. *Journal of Computer Science*, Vol. 2, No. 9, 710–715.
13. Śledź, S.; Ewertowski, M. W., & Piekarczyk, J. (2021). Applications of unmanned aerial vehicle (UAV) Surveys and Structure from Motion photogrammetry in glacial and periglacial geomorphology. *Geomorphology*, 378, 107620.
14. Sooyong Jeong, Cheolhee Park, Dowon Hong, Changho Seo, Namsu Jho. (2021). Neural Cryptography Based on Generalized Tree Parity Machine for Real-Life Systems. *Security and Communication Networks*, Vol. 2, No. 3. https://doi.org/10.1155/2021/6680782

15. Tkachenko, R., & Izonin, I.. (2019). Model and Principles for the Implementation of Neural-Like Structures based on Geometric Data Transformations. *Advances in Computer Science for Engineering and Education. ICCSEEA2018.* Advances in Intelligent Systems and Computing, Vol. 754, 578–587.
16. Tsmots Ivan, Rabyk Vasyl, Skorokhoda Oleksa, & Teslyuk Taras. (2019). Neural element of parallel-stream type with preliminary formation of group partial products. *Electronics and information technologies* (ELIT-2019)*: proceedings of the XIth International scientific and practical conference*, 16-18 September, 2019, Lviv, Ukraine, 154–158.
17. Tsmots, I. G., & Skorohoda, O. V. (2011). Device for calculating the scalar product. Utility Model. *Patent of Ukraine for an invention* No. 66138, Bulletin No. 24/2011.
18. Tsmots, I. G., Lukashchuk, Yu. A., Khavalko, V. M., & Rabyk, V. G. (2019). Models of the neuro-like element of the parallel-parallel type. *Modeling and information technologies*, Vol. 86, 119–126.
19. Tsmots, I. G., Rabyk, V. G., & Lukashchuk, Yu. A. (2021). Development of mobile means of neuro-like cryptographic encryption and decryption of data in real time. *Bulletin of the Lviv Polytechnic National University. Series: Information systems and networks*, 9, 84–95.
20. Tsmots, I. G., Skorohoda, O. V., & Teslyuk, V. M. (2013). Device for calculating the scalar product. *Patent of Ukraine for an invention* No. 101922, 13.05.2013, Bulletin No. 9.
21. Tsmots, I. G., Skorokhoda, O. V., & Medikovsky, M. O. (2019). Device for calculating the scalar product. *Patent of Ukraine for an invention* No. 118596, February 11, 2019, Bulletin No. 3.
22. Tsmots, I. G., Teslyuk, V. M., Teslyuk, T. V., Medikovsky, M. O., & Tsymbal, Yu. V. (2019). A device for calculating sums of even products. *Patent of Ukraine for an invention* No. 120210, October 25, 2019, Bulletin No. 20/2019.
23. Tsmots, I., Rabyk, V., Skorokhoda, O., & Tsymbal, Yu. (2021). Neural-like real-time data protection and transmission system. *Advances in Intelligent Systems and Computing* (AISC), Vol. 1293: Advances in Intelligent Systems and Computing V. Selected papers from the International conference on computer science and information technologies.
24. Tsmots, I., Tsymbal, Yu., Khavalko, V., Skorokhoda, O., & Tesluyk, T. (2018). Neural-Like Means for Data Streams Encryption and Decryption in Real Time. Processing of the 2018 IEEE 2*nd International Conference on Data Stream Mining and Processing*, DSMP 2018, 438–443, 84788513.
25. Tsmots, I., Tsymbal, Yu., Skorokhoda, O., & Tkachenko, R. (2019). Neural-like methods and hardware structures for real-time data encryption and decryption. Computer Sciences and Information Technologies, CSIT-2019: Proceedings of the XIV *International Scientific and Technical Conference*, September 17-20, 2019, Lviv, Ukraine, 248–253.
26. Tsmots, Ivan, Skorokhoda, Oleksa, Ignatyev, Ihor, & Rabyk, Vasyl. (2017). Basic Vertical-Parallel Real Time Neural Network Components. *Proceedings of XIIth International Scientific and Technical Conference*, CSIT 2017. 5-8 September 2017. Lviv, Ukraine, 344–347.
27. Tsymbal, Yu. V. (2018). Neural network method of symmetric data encryption. Bulletin of the Lviv Polytechnic National University. Series: Information systems and networks, 901, 118–122.
28. Verma, A., & Ranga, V. (2020). Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review. IEEE *Sensors Journal*, 20, 5666–5690.
29. Volna, E., Kotyrba, M., Kocian, V., & Janosek M. (2012). Cryptography Based on Neural Network. Proceedings of the 26*th European Conference on Modeling and Simulation*, 386–391.
30. Wolfgang Kinzel, & Ido Kanter. (2002). Neural cryptography. *Proceedings of the 9th International Conference on Neural Information Processing*. ICONIP 02. https://doi.org/10.1109/ICONIP.2002.1202841

I. H. Tsmots, Yu. A. Lukashchuk

Lviv Polytechnic National University, Lviv, Ukraine

GENERALIZED ANALYTYCAL MODEL OF PRESETTING FOR NEURAL CRYPTOGRAPHIC DATA ENCRYPTION

The paper presents some results of development of a generalized analytical model of presetting for the implementation of neural data encryption. In the course of research, its main components are found to be as follows: a building block of the neural network architecture, a calculation block of weighting coefficient matrices, and a calculation block of macroparticle product tables, the implementation of which ensures reducing setup time. We have analyzed recent research and publications on the relevance of problems in the implementation of neural cryptography data encryption. This is where the generalized analytical model of presetting appears to be useful. Some rules for creation of the neural network architecture are formulated in the paper. The structure of a neural network for cryptographic data encryption is determined by the number of neural elements. A calculation block of weighting coefficient matrices has also been developed. Therefore, the method of singular value decomposition of the matrix and the Jacobi rotation method was used to find eigenvectors and eigenvalues. A simulation model was developed to demonstrate the operation of this calculation block using a 13×16 training matrix with a predefined architecture as an example. A macroparticle product calculator based on a table-algorithmic method was developed as well. A simulation model was developed based on a weighting coefficient matrix with a bit depth of 8 and a given neural network architecture. Moreover, a flexible user interface has been developed for both calculation blocks, and a detailed description of its use has been provided as well. The C# programming language and the Visual Studio 2022 development environment were chosen to implement the tasks. Windows Forms was chosen as the development technology. The Accord.Math library was used for matrix operations. The practical value is that the developed tools provide fast calculation of coefficients for the given neural network architecture. As a result, the use of such a generalized presetting model will ensure the speed and security of data encryption.

Keywords: neural network; neural elements; macroparticle products; tabular algorithmic method; method of singular value decomposition of a matrix; Jacobi rotation method; eigenvectors; eigenvalues.