КІБЕРБЕЗПЕКА

ISSN 2707-1898 (print)
Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2022.02.045
Article received 08.10.2022 p.
Article accepted 17.10.2022 p.
UDK 004.94

Correspondence author
I. G. Tsmots
ivan.tsmots@gmail.com

І. Г. Цмоць, В. М. Теслюк, Ю. В. Опотяк, І. В. Піх
Національний університет "Львівська політехніка", м. Львів, Україна

МОДЕЛІ ТА ЗАСОБИ ВІДЛАГОДЖЕННЯ Й ТЕСТУВАННЯ МОБІЛЬНИХ СИСТЕМ ДЛЯ НЕЙРОПОДІБНОГО КРИПТОГРАФІЧНОГО ЗАХИСТУ Й ПЕРЕДАЧІ ДАНИХ

Визначено потребу забезпечення криптографічного захисту та завадостійкості при передачі даних і команд управління за допомогою мобільних робототехнічних платформ, важливість врахування обмеження щодо габаритів, енергоспоживання та продуктивності. З'ясовано, що одним із шляхів забезпечення вимог криптографічного захисту даних є використання нейроподібних мереж. Їхня особливість в можливості наперед обчислити вагові коефіцієнти, які будуть використані при шифруванні/дешифруванні даних. Запропоновано при нейроподібному шифруванні/дешифруванні даних генерувати ключ з урахуванням архітектури нейроподібної мережі (кількості нейронів, кількості входів і їх розрядності), матриці вагових коефіцієнтів і таблиці для маскування. Визначено, що нейроподібна мережа з наперед обчисленими ваговими коефіцієнтами дає змогу використати таблично-алгоритмічний метод при шифруванні/дешифруванні даних, який ґрунтується на операціях зчитування з пам'яті, додавання та зсуву. Проаналізовано обмеження щодо габаритів, енергоспоживання та продуктивності, які під час реалізації можна подолати шляхом використання універсального процесорного ядра, доповненого спеціалізованими апаратними засобами (ПЛІС), що реалізують нейроподібні елементи, а сумісне використання програмних і ПЛІС забезпечує ефективну реалізацію алгоритмів нейроподібного шифрування/дешифрування даних і команд управління. Представлено моделі та засоби для відлагодження й тестування нейроподібної криптографічної системи. Розроблено модель попередніх налаштувань системи нейроподібного шифрування даних, основними компонентами якої є формувач архітектури нейроподібної мережі, обчислювач матриць вагових коефіцієнтів і обчислювач таблиць макрочасткових добутків. Розроблено модель процесу нейроподібного шифрування з використанням таблично-алгоритмічного методу, основними компонентами якої є перетворювач повідомлення, формувач адреси зчитування з таблиць, *N* таблиць макрочасткових добутків, *N* суматорів і комутатор, реалізація якої забезпечує тестування системи криптографічного захисту й передачі даних (СКЗПД) у реальному часі. Розроблено моделі тестування та відлагодження блоків шифрування (дешифрування), кодування (декодування), маскування (демаскування) даних, які за рахунок використання еталонних значень для порівняння забезпечують підвищення якості тестування та відлагодження СКЗПД. Розроблено СКЗПД, яка внаслідок динамічної зміни типу архітектури нейроподібної мережі (НПМ) та значень вагових коефіцієнтів (ВК), кодів маски та баркероподібного коду (БПК) забезпечує підвищення криптостійкості процедури передачі даних. Запропоновано динамічну зміну архітектури НПМ (значення ВК), маски та БПК, що сприяє підвищенню криптостійкості СКЗПД загалом. Виконано тестування імітаційної моделі на прикладі передачі повідомлень для різних конфігурацій СКЗПД.

Ключові слова: таблично-алгоритмічний метод розрахунку вагових коефіцієнтів нейроподібної мережі; імітаційна модель нейроподібного шифрування/дешифрування; динамічна зміна архітектури нейроподібної мережі; обчислення таблиць макрочасткових добутків.

Вступ / Introduction

При дистанційному управлінні мобільними інтелектуальними робототехнічними платформами важливим завданням є забезпечення криптографічного захисту та завадостійкості при передачі команд і даних з урахуванням обмежень щодо габаритів, енергоспоживання, продуктивності та вартості. Одним із шляхів забезпечення таких вимог є використання автоасоціативної нейромережі прямого поширення, яка навчається на підставі методу головних компонент та баркероподібних кодів як основи для розроблення мобільної системи криптографічного захисту й передачі даних (СКЗПД).

Особливістю автоасоціативної нейромережі прямого поширення є можливість наперед обчислити вагові коефіцієнти, які будуть використані при шифруванні/дешифруванні даних, а сама мережа стає нейроподібною. Наперед обчислені вагові коефіцієнти дають змогу використати таблично-алгоритмічний метод для шифрування/дешифрування даних, який ґрунтується на операціях зчитування з пам'яті, додавання та зсуву. Ключами

при нейроподібному шифруванні та дешифруванні даних є архітектура нейроподібної мережі (кількість нейронів, кількість входів і їх розрядність), матриці вагових коефіцієнтів і таблиці для маскування.

Одним із шляхів реалізації мобільних СКЗПД є використання універсального процесорного ядра (мікроконтролера) доповненого спеціалізованими апаратними засобами (ПЛІС), які реалізують нейроподібні елементи. Сумісне використання програмних і спеціалізованих апаратних засобів забезпечує ефективну реалізацію алгоритмів нейроподібного шифрування/дешифрування команд і даних.

Вартість і тривалість проектування мобільних СКЗПД значною мірою визначають програмно-апаратні засоби відлагодження й тестування. До мобільних СКЗПД ставляться високі вимоги за надійністю та забезпеченням перевірки працездатності на робочих тактових частотах, швидкої локалізації та знешкодження неполадок. Забезпечення високої надійності та діагностики мобільних СКЗПД досягається шляхом застосування сучасної елементної бази (мікроконтролерів, ПЛІС) та апаратної й програмної надлишковості. Для забезпечення відлагодження мобільних СКЗПД вони мають володіти властивостями керованості, спостережуваності й передбачуваності. При відлагодженні мобільних СКЗПД необхідно забезпечити відповідну інтенсивність надходження команд управління рухом інтелектуальної робототехнічної платформи.

Процес відлагодження мобільних СКЗПД можна розбити на наступні етапи: підготовка тестових і еталонних масивів даних, формування масиву керуючих сигналів відповідно до режимів роботи; підготовка апаратури відлагодження (завантаження еталонних масивів даних); проведення тестування; нагромадження результатів тестування та їх опрацювання.

Отже, актуальною проблемою є розроблення моделей, засобів відлагодження й тестування системи криптографічного захисту й передачі даних (СКЗПД) на робочих тактових частотах.

Об'єкт дослідження – процеси моделювання, відлагодження й тестування СКЗПД.

Предмет дослідження – моделі, методи, алгоритми обчислень вагових коефіцієнтів, таблиць макрочасткових добутків і засоби відлагодження, тестування системи криптографічного нейроподібного захисту та передачі даних.

Мета роботи – розроблення моделей і засобів попередніх налаштувань, нейроподібного шифрування, відлагодження й тестування СКЗПД.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- вибрати засоби розроблення мобільних СКЗПД;
- розробити модель попередніх налаштувань для нейроподібного шифрування даних;
- розробити узагальнену модель нейроподібного шифрування команд управління з використанням таблично-алгоритмічного методу;
- розробити інформаційні моделі відлагодження й тестування мобільної СЗПД;
- розробити засоби обчислення вагових коефіцієнтів, макрочасткових добутків і еталонних результатів.

Аналіз останніх досліджень та публікацій. Аналіз основних тенденцій у створенні мобільних бортових систем для криптографічного захисту й передачі даних у реальному часі показує, що для виконання операцій шифрування та дешифрування у таких системах використовуються нейромережні методи [3], [6], [21], [22]. У роботі [9] зазначено, що композитним ключем шифрування в криптосистемі нейронної мережі є вагові матриці синаптичних зв'язків між нейронами та метадані про архітектуру нейронної мережі, а стохастичний характер помилки передбачення нейронної мережі забезпечує постійно мінливу пару ключ-шифртекст. Аналіз засобів для реалізації криптографічного захисту даних, які використовують нейромережні методи, показує, що така реалізація в основному виконують програмно [4], [7], [8], [10]. Зокрема, у роботі [20] описано багатоваріантні криптосистеми з відкритим ключем, засновані на розширеній нейронній мережі Хопфілда, а запропонований авторами алгоритм забезпечує практичність апаратної реалізації. Однак, основним недоліком програмної реалізації нейромережевого криптографічного захисту даних є складність забезпечення режиму реального часу та додаткових обмежень, які висуваються до СКЗПД щодо маси, габаритів, продуктивності, енергоспоживання та вартості.

У роботах [13], [17], [18] описано адаптацію автоасоціативної нейронної мережі з неітераційним навчанням для задач криптографічного шифрування та дешифрування даних. У такій нейромережі вагові коефіцієнти обчислюють наперед, а не формують внаслідок її навчання на підставі методу головних компонент. Особливістю даного методу є використання системи власних векторів, які відповідають власним значенням коваріаційної матриці вхідних даних [15]. У роботі [16] показано, що ключ у системі нейроподібного криптографічного захисту даних формується на підставі кодів маскування, архітектури нейроподібної мережі та матриці відповідних вагових коефіцієнтів. У роботі [1] описано реалізацію нейромережі невеликого розміру на мікропроцесорі RISC-V з оперативною пам'яттю лише 16 КБ. Проте, з аналізу робіт [2], [11], [14], [19] видно, що нейроподібні алгоритми криптографічного захисту даних реалізовані з використанням ПЛІС забезпечують високу продуктивність реалізованих засобів криптографічного захисту й передачі даних завдяки розпаралелюванню та конвеєризації обчислень. Однак, проведений нами аналіз показує, що невирішеною проблемою залишається розроблення моделей і відповідних засобів для відлагодження й тестування СКЗПД, реалізованих на підставі нейроподібних мереж.

Результати дослідження та їх обговорення / Research results and their discussion

Принципи розроблення мобільних систем нейроподібного криптографічного захисту й передачі даних. Розроблення мобільних систем криптографічного захисту й передачі даних СКЗПД вимагає широкого використання сучасної елементної бази, розроблення нових методів, алгоритмів і структур, орієнтованих на ефективну апаратно-програмну реалізацію нейроподібних алгоритмів шифрування та дешифрування даних. Під час розроблення таких мобільних СКЗПД виникає проблема забезпечення режиму реального часу, підвищення криптостійкості з одночасним зменшенням маси, габаритів, енергоспоживання та вартості. Для забезпечен-

ня реального часу процеси нейроподібного шифрування та дешифрування даних мають відбуватися без нагромадження затримок. Зменшення масогабаритних характеристик, енергоспоживання, підвищення надійності та швидкодії СКЗПД можна досягнути шляхом використання проблемно-орієнтованого підходу та сучасної елементної бази.

Розроблення мобільної СКЗПД у реальному часі з високими техніко-економічними характеристиками пропонуємо здійснювати з використанням інтегрованого підходу, який охоплює:

- методи та алгоритми нейроподібного шифрування/дешифрування даних;
- методи та алгоритми синтезу баркероподібних кодів;
- розроблення нових методів і структур для реалізації нейроподібних елементів;
- сучасну елементну базу та засоби автоматизованого проектування.

Розроблення мобільної СКЗПД у реальному часі пропонуємо здійснювати з використанням таких принципів:

- змінності складу обладнання (універсальне процесорне ядро доповнене змінними апаратними модулями) та орієнтації архітектури СКЗПД на нейроподібні алгоритми шифрування/дешифрування та кодування/декодування даних;
- модульності, яка передбачає реалізацію змінних апаратних засобів у вигляді функціонально завершених пристроїв з виходом на стандартний інтерфейс;
- відкритості, при якому забезпечується можливість нарощування та вдосконалення програмного забезпечення;
- спеціалізації та адаптації змінних апаратних засобів до структури алгоритмів шифрування/дешифрування та кодування/декодування даних.

Модель попередніх налаштувань для нейроподібного шифрування даних. Мобільна система криптографічного захисту й передачі даних (СКЗПД) використовує нейроподібне шифрування з симетричними ключами, у якій ключ шифрування та ключ дешифрування є однаковими або ключ дешифрування легко обчислюють з ключа шифрування. Шифрування відбувається над відкритим текстом з використанням ключа, який визначають заданою кількістю нейроподібних елементів N, матрицею вагових коефіцієнтів W_{ji} і операціями маскування.

Виконання нейроподібного криптографічного шифрування 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 має такий вигляд:

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

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 визначають через розрядність m повідомлення X та розрядність входів нейроелемента n.

Із формули (1) видно, що модель попередніх налаштувань реалізують на базі трьох компонент: перша – формувача структури нейроподібної мережі; друга – обчислення матриці вагових коефіцієнтів; третя – обчислення таблиці макрочасткових добутків.

Перша компонента забезпечує формування структури нейроподібної мережі для шифрування/дешифрування даних. Структуру нейроподібної мережі визначають кількістю нейроподібних елементів, які обчислюють за формулою:

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

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.

Друга компонента забезпечує обчислення матриці вагових коефіцієнтів для нейроподібної мережі. Для її обчислення використаємо метод сингулярного розкладу матриці SVD (англ. *Singular Value Decomposition*). SVD схожий на метод головних компонент (МГК), але є більш загальним і записується так:

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

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

Розрахунок власних значень та власних векторів виконують за методом обертання Якобі, при якому обчислення власних значень та власних векторів симетричної матриці здійснюють ітераційно. Такий процес обчислення власних векторів відомий як діагоналізація. Суть методу Якобі зводиться до того щоб, для заданої матриці $S = S^{(0)}$ побудувати послідовність ортогональних подібних матриць $S^{(1)}$, $S^{(2)}$,…, $S^{(m)}$, які сходяться до діагональної матриці, на діагоналях якої знаходяться власні значення матриці S.

Для розрахунку матриці U за методом Якобі передається результат добутку AA^{T}, а для знаходження матриці V – результат добутку $A^{\mathrm{T}}A$. 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:

$$AW = UD, \quad (4)$$

де: A – вхідна матриця розмірністю $N\times n$; W – матриця вагових коефіцієнтів розмірністю $n\times n$; матриці U та D беруться з результату роботи SVD. Обчислення матриці вагових коефіцієнтів W виконують за такою формулою:

$$W = A^{-1}UD, \quad (5)$$

де матриця A^{-1} становить:

$$A^{-1} = VD^{-1}U^{\mathrm{T}}. \quad (6)$$

Підставивши (6) у (5) отримаємо формулу для обчислення вагових коефіцієнтів, яка запишеться так:

$$W = VD^{-1}U^{\mathrm{T}}UD. \quad (7)$$

Розмірність таблиць вагових коефіцієнтів визначають кількістю нейроподібних елементів, на підставі яких синтезована нейроподібна мережа. Так, для шифрування/дешифрування команд управління використовують нейроподібні мережі з кількість нейроподібних елементів 16, 8, 4, і 2. Розмірність матриць вагових коефіцієнтів для таких нейроподібних мереж відповідно становить 16×16, 8×8, 4×4, 2×2.

Третя компонента забезпечує обчислення таблиць макрочасткових добутків. Обчислення таблиць макро-

часткових добутків для вагових коефіцієнтів з плаваючою 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 $E_{Wmax}^h = E_{Wmax} + q$.

Таблицю макрочасткових добутків обчислюють за такою формулою:

$$P_{Mi} = \begin{cases} 0, \text{ якщо } x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 0; \\ w_1^h, \text{ якщо } x_{1i} = 1, \; x_{2i} = x_{3i} = \ldots = x_{Ni} = 0; \\ w_2^h, \text{ якщо } x_{1i} = 0, x_{2i} = 1, x_{3i} = \ldots = x_{Ni} = 0; \\ w_1^h + w_2^h, \text{ якщо } x_{1i} = 1, x_{2i} = 1, x_{3i} = \ldots = x_{Ni} = 0; \\ \vdots \\ w_2^h + \ldots + w_N^h, \cdots \text{якщо } x_{1i} = 0, x_{2i} = x_{3i} = \ldots = x_{Ni} = 1; \\ w_1^h + w_2^h + \ldots + w_N^h, \text{ якщо } x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 1, \end{cases} \quad (8)$$

де: $x_{1i}, x_{2i}, x_{3i}, \ldots, x_{Ni}$ – адресні входи таблиці; w_j^h – мантиса W_j вагового коефіцієнта приведена до найбільшого спільного порядку.

Кількість таблиць макрочасткових добутків для шифрування/дешифрування команд дорівнює кількості нейроподібних елементів у мережі. Обсяг пам'яті, необхідної для зберігання таблиці макрочасткових добутків, становить:

$$Q = 2^k, \quad (9)$$

де k – кількість входів нейроподібного елемента.

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

Узагальнена модель нейроподібного шифрування команд управління з використанням таблично-алгоритмічного методу. Для нейроподібного шифрування команд управління з використанням таблично-алгоритмічного методу розроблена узагальнена аналітична модель, яка має такий вигляд:

$$y_j = f_{(N\to 1)}(f_{(y_{1i},\ldots,y_{Ni})}(f_{(P_{M1i},\ldots,P_{MNi})}(f_{(x_{1i}\ldots x_{Ni})}(f_{(P\to S)})))), \quad (10)$$

де: y_j – зашифрована j-та частина команди управління; $f_{(P\to S)} = R^m \to NR^n$ перетворення m розрядного повідомлення на N частин розрядністю n; $f_{(y_{1i},\ldots,y_{Ni})}$ – виконання N підсумовувань макрочасткових добутків P_{Mji} відповідно до формули $y_{ji} = 2^{-1} y_{j(i-1)} + P_{Mji}$, де $y_{j0} = 0$; $f_{(P_{M1i},\ldots,P_{MNi})}$ – паралельне зчитування з таблиць, обчислених за формулою (8), N макрочасткових добутків $P_{M1i},\ldots,P_{MNi}$; $f_{(x_{1i}\ldots x_{Ni})}$ – формування розрядного зрізу для N частин повідомлення, який є адресом для зчитування макрочасткових добутків $P_{M1i},\ldots,P_{MNi}$ з таблиць; $f_{(N\to 1)}$ – послідовна передача частинами зашифрованого повідомлення.

Структуру моделі нейроподібного шифрування команд управління з використанням таблично-алгоритмічного методу, яка реалізує вираз (10), подано на рис. 1. Основними компонентами даної моделі є: перетворювач m розрядного повідомлення на N частин розрядністю n, формувач адреси зчитування з таблиць, N таблиць макрочасткових добутків, N суматорів і комутатор для послідовної передачі частинами зашифрованого повідомлення. З аналізу моделі нейроподібного шифрування команд управління видно, що збільшення кількості нейроподібних елементів веде до збільшення кількості частин зашифрованого повідомлення.

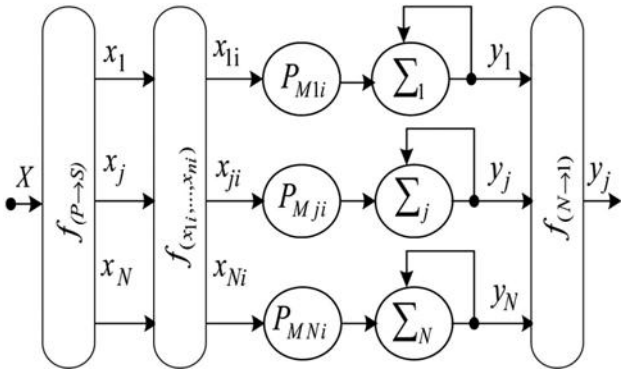

Рис. 1. Модель нейроподібного шифрування даних з використанням таблично-алгоритмічного методу / A model of neuro-like data encryption using a table-algorithmic method

Інформаційні моделі відлагодження й тестування мобільної СКЗПД. Мобільна СКЗПД апаратно відображає структуру алгоритмів нейроподібного шифрування/дешифрування, кодування/декодування даних з використанням баркереподібних кодів. Для відлагодження та аналізу функціонування мобільної СКЗПД розроблено дві інформаційні моделі:

- перша – відлагодження й тестування блоків шифрування, маскування та кодування даних;
- друга – відлагодження й тестування блоків декодування, демаскування та дешифрування даних.

Інформаційна модель відлагодження й тестування блоків шифрування, маскування та кодування даних наведена на рис. 2, де НПМ – нейроподібна мережа, ВК – вагові коефіцієнти, РТП – робототехнічна платформа, БПК – баркереподібні коди.

Основними етапами застосування моделі відлагодження й тестування блоків шифрування, маскування та кодування даних є:

- вибір архітектури нейроподібної мережі;
- задавання команди управління РТП;
- обчислення з використанням імітаційної моделі вагових коефіцієнтів для різних архітектур НПМ та запис їх у пам'ять;
- шифрування команди управління РТП з використанням емулятора та розробленого блоку і запис результатів шифрування у відповідні блоки пам'яті;
- порівняння результатів нейроподібного шифрування, отриманого за допомогою емулятора та розробленого блока;
- формування висновку на підставі порівняння результатів шифрування;
- маскування команди управління РТП з використанням кодів з блоку пам'яті;

- синтез з використанням імітаційної моделі БПК різної довжини, виду та запис їх блок пам'яті;
- кодування результатів нейроподібного шифрування за допомогою БПК, зчитаного з блоку пам'яті та запис їх у блок пам'яті;
- порівняння результатів нейроподібного шифрування після маскування та кодування, отриманих за допомогою емулятора та розробленого блока;
- формування висновку на підставі порівняння результатів маскування та кодування.

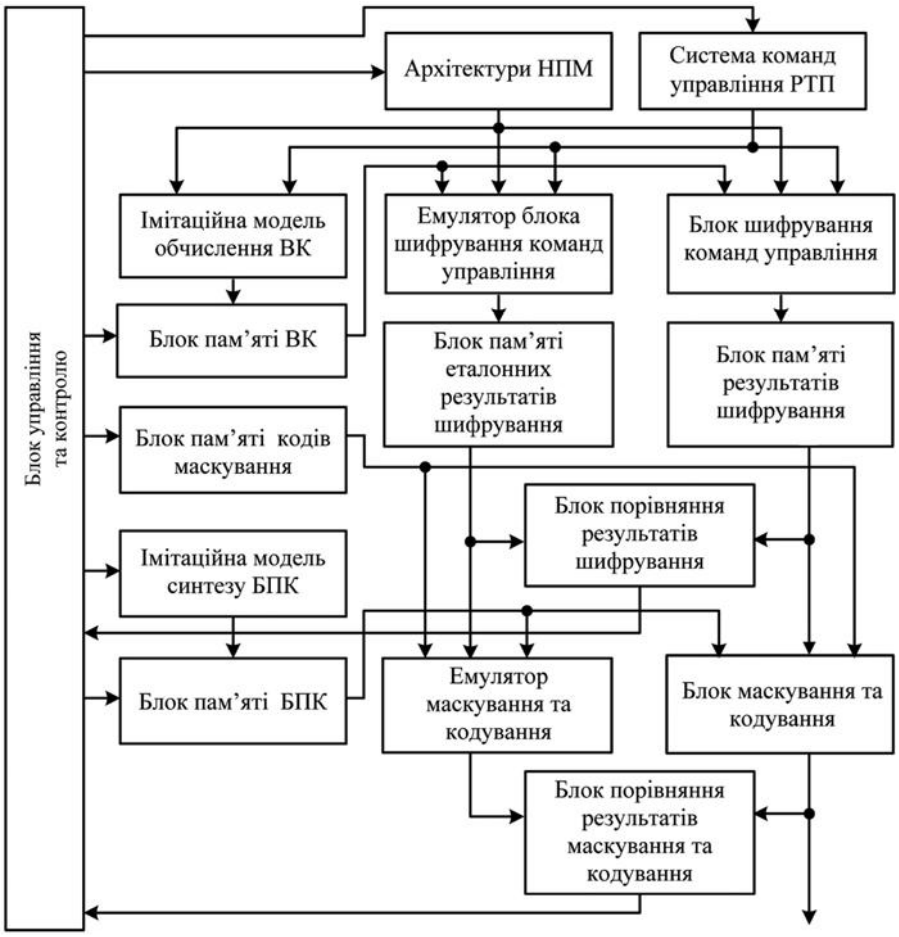

Рис. 2. Інформаційна модель відлагодження й тестування блоків шифрування, маскування та кодування даних / Information model for debugging and testing encryption, masking and data encoding blocks

Для підвищення криптостійкості пропонуємо динамічно змінювати типи архітектури НПМ (значення ВК), значення маски та БПК. Інформаційна модель відлагодження й тестування блоків декодування, демаскування та дешифрування даних наведена на рис. 3.

Основними етапами застосування моделі тестування, відлагодження блоків шифрування, маскування та кодування даних є:

- формування та запис кодів демаскування в блок пам'яті аналогічно кодам маскування;
- синтез і запис БПК для декодування команд управління в блок пам'яті аналогічно БПК для їх кодування;
- декодування та демаскування команди управління з використанням емулятора та розробленого блоку і запис результатів у відповідні блоки пам'яті;
- порівняння результатів декодування та демаскування команди управління, отриманих за допомогою емулятора та розробленого блока;
- формування висновку на підставі порівняння результатів декодування та демаскування команди управління;
- дешифрування команди управління РТП та запис результатів, отриманих за допомогою емулятора та розробленого блока у відповідні блоки пам'яті;
- порівняння результатів дешифрування команди управління, отриманих за допомогою емулятора та розробленого блока;
- обчислення за допомогою імітаційної моделі та запис у блок пам'яті ВК для дешифрування команд управління РТП;
- формування висновку на підставі порівняння результатів дешифрування команди управління РТП.

У моделі тестування, відлагодження блоків декодування, демаскування та дешифрування даних зміна типу архітектури НПМ (значення ВК для дешифрування), значення маски та БПК відбуваються динамічно. Частота зміни типу архітектури НПМ, значення маски та БПК здійснюють шляхом програмного налаштування. Реалізацію зміни типу архітектури НПМ здійснюють шляхом зчитування ВК з блоку пам'яті. Аналогічно реалізують зміну значення маски та БПК.

Для адресації блоків пам'яті ВК, маски та БПК у блоках шифрування, маскування та кодування даних і блоках декодування, демаскування та дешифрування даних використовують лічильники адреси. У блоках шифрування та дешифрування даних лічильники адреси повинні бути синхронізовані та змінювати свій стан з однаковою частотою.

Аналогічно працюють лічильники адрес у блоках маскування та кодування даних і блоках демаскування та декодування даних. Частота зміни стану лічильників адреси для блоків пам'яті маски, ВК і БПК є різною, що забезпечує підвищення криптостійкості.

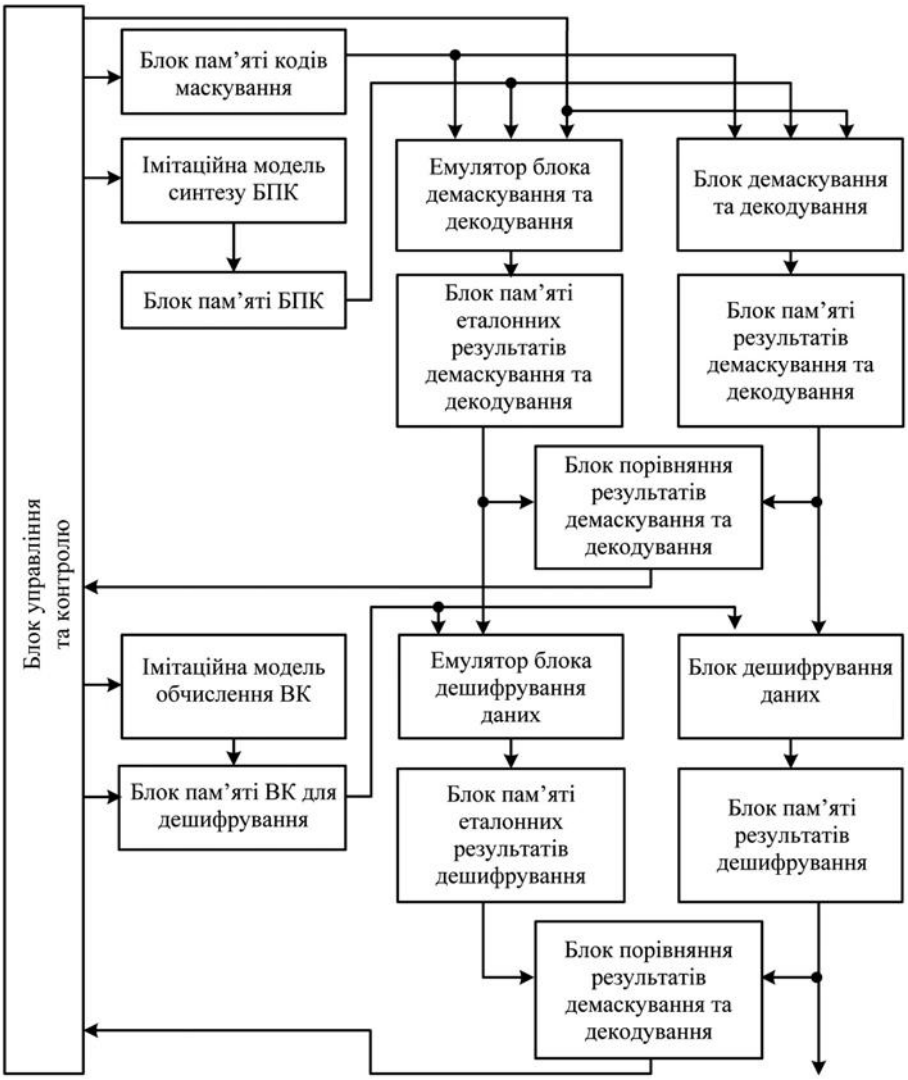

Рис. 3. Інформаційна модель відлагодження й тестування блоків декодування, демаскування та дешифрування даних / Information model for debugging and testing blocks of decoding, unmasking and decryption of data

Засоби обчислення вагових коефіцієнтів і еталонних результатів. Імітаційну модель обчислення вагових коефіцієнтів, макрочасткових добутків і еталонних результатів розроблено з використанням мови C# і середовища Visual Studio 2022. Практичною цінністю є те, що розроблена імітаційна модель забезпечує швидке обчислення коефіцієнтів для заданої архітектури нейроподібної мережі. Гнучкий користувацький інтерфейс надає змогу порівняти роботу покращеного методу SVD для знаходження коефіцієнтів із методом шифрування з симетричними ключами. До основних підготовчих етапів перед шифруванням, дешифруванням даних на підставі розробленої імітаційної моделі належать: вибір архітектури нейроподібної мережі шифрування/дешифрування даних; навчання нейронної мережі, яке містить обчислення вагових коефіцієнтів для мереж шифрування/дешифрування даних; тестування нейроподібних мереж шифрування/дешифрування даних.

Для навчання імітаційної моделі лінійного нейроподібного шифрування даних було обрано вхідне повідомлення із розрядністю 16 та розрядністю входу 2. Опираючись на ці дані, вхідна матриця буде мати розмірність 8×2. Вхідне повідомлення задає користувач. Внаслідок цього розраховують матрицю вагових коефіцієнтів розмірністю 8×8. У подальшому ця матриця буде використана при шифруванні та дешифруванні вхідного повідомлення.

Вхідними даними для програми є n – розрядність повідомлення, m – розрядність входів та навчальна матриця (рис. 4).

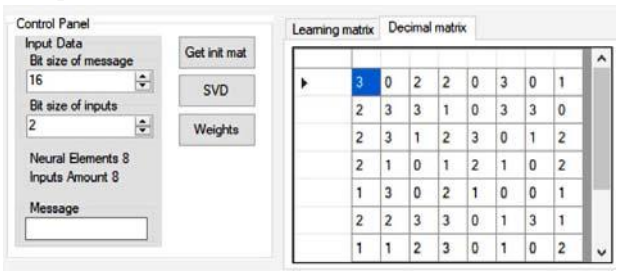

Рис. 4. Вікно формування вхідних даних для імітаційної моделі / The input data generation window for the simulation model

Для навчання нейроподібної мережі використовують матрицю вхідних даних $X[N, n\_IN]$, яку формують шляхом генерування псевдовипадкових чисел p у діапазоні $[0, max\_X=2^{k\_IN}-1]$. Перші десять навчаючих векторів зі згенерованих N=50 для X_Start=97 наведено нижче:

Size of training vectors	n = 16;
Number of training vectors	N= 50;
Size of neural networks inputs	K_IN = 2;
Number of neural networks inputs	n_IN = 8;

Number recalculations of K_i, M_j coefficients N_K_M = 4.
3 0 2 2 0 3 0 1
2 3 3 1 0 3 3 0
2 3 1 2 3 0 1 2
2 1 0 1 2 1 0 2
1 3 0 2 1 0 0 1
2 2 3 3 0 1 3 1
1 1 2 3 0 1 0 2
0 1 0 1 1 0 3 2
2 3 1 1 0 1 0 0
1 0 1 1 2 3 3 3

Після введення даних програма розраховує кількість нейроелементів та входів. Далі знаходять матриці U, V та D за допомогою алгоритму SVD, який спрацьовує при натисканні кнопки *SVD*. Для знаходження матриці U на вхід SVD подається результат добутку AA^{T}, де A – навчальна матриця, а для знаходження V – результат добутку $A^{\mathrm{T}}A$. Матриця D складається із власних значень, розміщених на головній діагоналі. Розрахунок вагових коефіцієнтів відбувається при натисканні кнопки *Weights*, а результат продемонстровано на рис. 5.

Розраховані матриці можна застосувати для налаштування нейроподібної мережі шифрування вхідного повідомлення, яке користувач може ввести у спеціальне текстове поле *Message*. Далі, перейшовши на вкладку *Encryption* і натиснувши на кнопку *Encrypt*, користувачу відобразиться зашифроване повідомлення за формулою (рис. 6).

Для роботи програми потрібно задати архітектуру нейроподібної мережі: розрядність навчаючих векторів; розрядність вхідних нейронів нейроподібної мережі; кількість нейронів вхідного шару нейроподібної мережі; вагові коефіцієнти мережі. Далі, щоб дешифрувати зашифровані дані, треба перейти на вкладку *Decryption* і натиснути на кнопку *Decrypt*, а результат дешифрування показано на рис. 7.

Користувацький інтерфейс імітаційної моделі для нейроподібного шифрування/дешифрування даних показано на рис. 8.

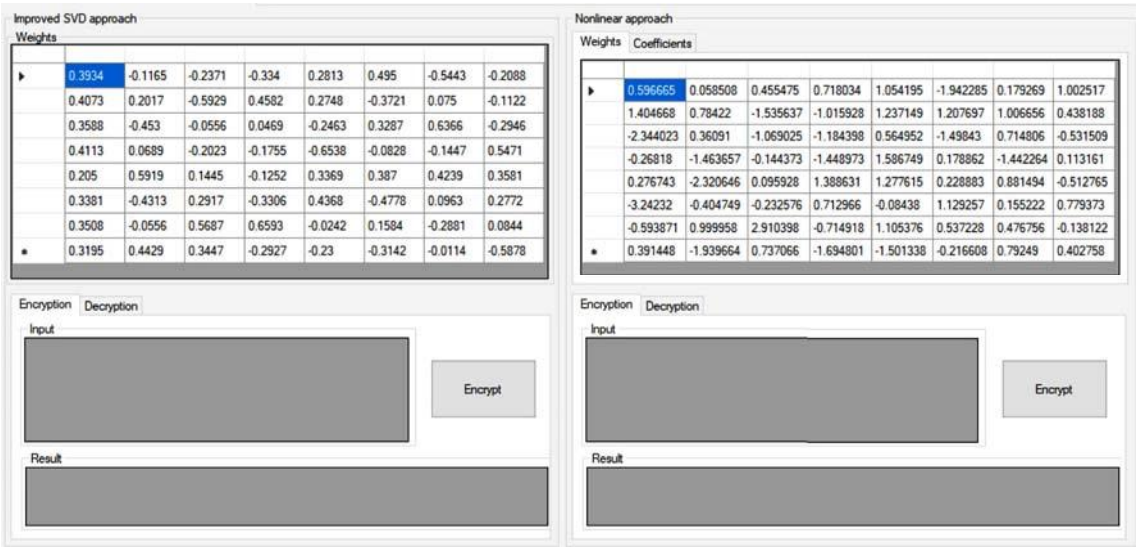

Рис. 5. Вікно з матрицею вагових коефіцієнтів / A window with a matrix of weighting coefficients

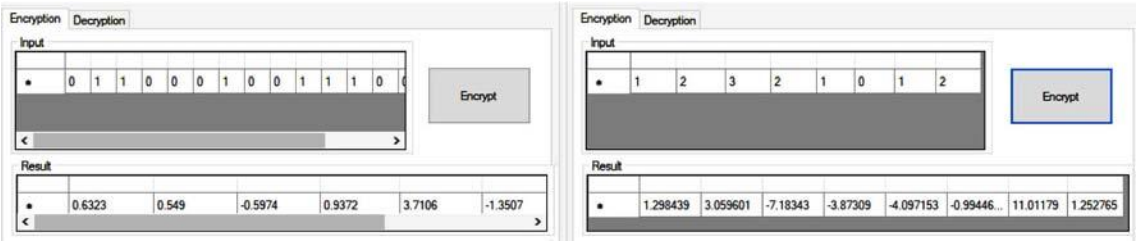

Рис. 6. Вікно імітаційної моделі нейроподібного шифрування вхідного повідомлення / Window of the simulation model of neuro-like encryption of the incoming message

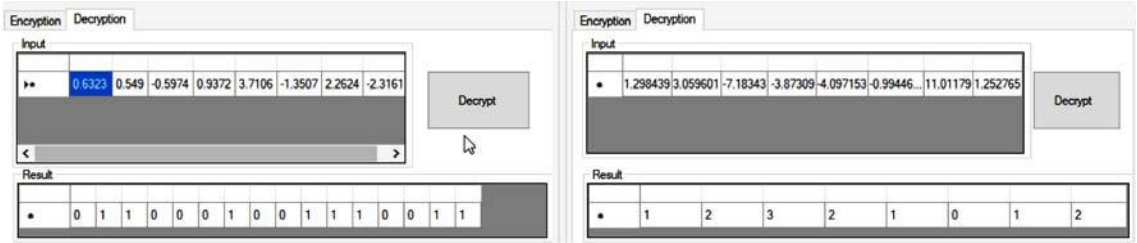

Рис. 7. Вікно імітаційної моделі нейроподібного дешифрування повідомлення / Window of the simulation model of the neuro-like decoding of the message

З використанням розроблених програмних засобів імітаційної моделі обчислено вагові коефіцієнти, які використовують для шифрування/дешифрування даних для трьох нейроподібних архітектур з параметрами:

m=2, k=8, N=8;

m=4, k=4, N=4;

m=8, k=2, N=2,

де: N – кількістю нейроподібних елементів, k – кількість входів нейроподібного елемента; m – розрядність входів нейроподібних елементів.

За допомогою розробленого програмного забезпечення імітаційної моделі обчислено матрицю вагових коефіцієнтів для нейроподібної мережі з вісьмома нейроподібними елементами (табл. 1).

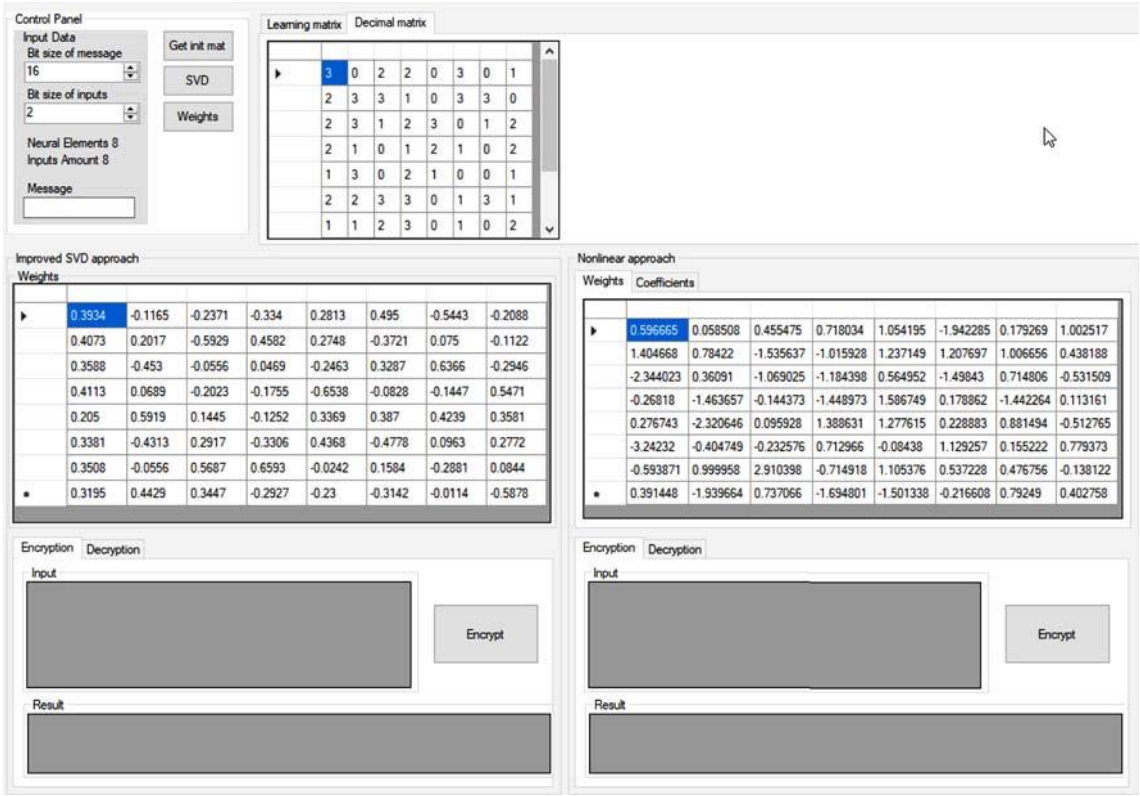

Рис. 8. Користувацький інтерфейс імітаційної моделі нейроподібного шифрування/дешифрування даних / User interface of a simulation model of neural-like encryption/decryption of data

Табл. 1. Матриця вагових коефіцієнтів для нейроподібної мережі з вісьмома нейроподібними елементами / Matrix of weight coefficients for a neural network with eight neural elements

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

Далі послідовно було обчислено матрицю вагових коефіцієнтів для нейроподібної мережі з чотирма та двома нейроподібними елементами, ваги яких вказано відповідно у табл. 2 та табл. 3.

Табл. 2. Матриця вагових коефіцієнтів для нейроподібної мережі з чотирма нейроподібними елементами / Matrix of weight coefficients for a neural network with four neural elements

-7,722469	-1,768955	-4,89013	-5,411336
7,071378	-2,227652	2,931437	-6,707074
-6,939177	1,246172	8,290145	-1,07193
-0,912977	-11,762918	1,058508	1,970398

Табл. 3. Матриця вагових коефіцієнтів для нейроподібної мережі з двома нейроподібними елементами / Matrix of weighting coefficients for a neural network with two neural elements

0,5934	0,8049
0,8048	-0,5934

Для розрахунку застосовано розроблені програмні засоби імітаційної моделі. Створена модель і відповідні програмні засоби дають змогу оцінити похибки обчислень при різних значеннях кількості значущих біт для обчислення таблиць макрочасткових добутків. Оцінювання проведено для значень розрядності 8, 16 та 24 біт. Результати зведено у табл. 4.

Табл. 4. Оцінювання похибки обчислень / Estimation of calculation error

Стандарт	Запропонований алгоритм			Похибка для розрядності:		
Стандарт	8 біт	16 біт	24 біт	8 біт	16 біт	24 біт
-43.697238	-42.632813	-43.689017	-43.697238	-1.064426	-0.008221	-0.000010
-29.860335	-29.605469	-29.858745	-29.860333	-0.254866	-0.001589	-0.000002
-105.333265	-103.335938	-105.327900	-105.333248	-1.997328	-0.005365	-0.000017
10.273581	10.393803	10.270640	10.273588	0.120222	-0.002941	-0.000007

Виконано тестування процесів шифрування/дешифрування даних з використанням розробленої моделі за допомогою макету СКЗПД. Як платформу для реалізації застосовано мікрокомп'ютер NanoPi Duo фірми FriendlyElec на підставі SoC Allwinner's Cortex-A7 H2+ з ОЗП 256 МБ під керуванням ОС Ubuntu. Моделювання

проводилося для розроблених варіантів нейроподібних мереж з застосуванням вихідного коду, перекомпільованого для платформи, та було отримано результати, наведені у табл. 5, де P_{max} – степінь поліному.

Табл. 5. Тривалість виконання операцій формування та обчислення вагових коефіцієнтів, шифрування та дешифрування для типів нейроподібної мережі / The duration of operations of formation and calculation of weight coefficients, encryption and decryption for types of neuro-like networks

Нейромережа / Модуль	Training, мс	EnCrypt, мс	DeCrypt, мс
Лінійна	200	15	10
Нелінійна P_{max}=5	710	30	35
Нелінійна P_{max}=15	2800	65	70
Нелінійна P_{max}=25	4630	92	98
Нелінійна P_{max}=35	6525	128	135

Для отримання тривалості виконання операцій формування та обчислення вагових коефіцієнтів, шифрування та дешифрування окремими модулями застосовувалася процедура clock(), яка повертає кількість тактів, що пройшли з моменту запуску програми. Вказані значення було переведено у час. Як показує аналіз результатів використання імітаційної моделі, при розрахунках звичайним методом і шляхом використання запропонованого алгоритму обчислення макрочасткових добутків отримані значення похибок для розрядності 24 біт становлять у абсолютному значенні не більше $2{,}0 \cdot 10^{-5}$, і є надзвичайно малими. Очевидно, для меншої розрядності похибка обчислення для пропонованого таблично-алгоритмічного методу обчислення скалярного добутку зростає.

Як показують результати імітаційного моделювання роботи програмних реалізацій нейромережевого шифрування/дешифрування даних на обраній платформі у різних конфігураціях нейроподібної мережі і різних значеннях поліномів P_{max} найбільш тривала операція – формування та обчислення вагових коефіцієнтів нейроподібної мережі. Тривалість її виконання на мікрокомп'ютері становить біля 200 мс для лінійної мережі та від 700 мс і більше – для нелінійної. Причому, ця тривалість сильно залежить від степеня поліному для обраної конфігурації нейроподібної мережі. Однак, вказана процедура виконується одноразово при зміні ключа шифрування, а отже, не впливає безпосередньо на тривалість процедур шифрування/дешифрування.

Тривалість виконання процедур нейромережевого криптографічного шифрування/дешифрування блоків даних при реалізації на мікрокомп'ютері становить біля відповідно 15 мс та 10 мс для лінійної нейроподібної мережі та відповідно 65 мс та 70 мс для степеня полінома P_{max}=15 для нелінійного типу мережі. Таку тривалість можна вважати прийнятною для практичного застосування. Застосування нелінійної нейроподібної мережі сприяє захищеності процесів шифрування/дешифрування від злому, а тривалість виконання операцій у такому випадку зростає у 2–3 рази і знаходиться у межах прийнятних для роботи у режимі часу, близькому до реального. Зменшення тривалості вказаних операцій можна досягнути шляхом використання процесорного ядра, доповненого спеціалізованими апаратними засобами (ПЛІС), які реалізують нейроподібні елементи.

Обговорення результатів дослідження. У роботі [9] запропоновано композитний ключ для шифрування в криптосистемі нейронної мережі з використанням вагової матриці синаптичних зв'язків між нейронами та метаданих про архітектуру нейронної мережі. Авторами запропоновано при нейроподібному шифруванні/дешифруванні даних генерувати ключ не тільки з урахуванням архітектури нейроподібної мережі (кількості нейронів, кількості входів і їх розрядності), матриці вагових коефіцієнтів, а з застосуванням таблиці для маскування та шляхом динамічної зміни типу архітектури нейроподібної мережі, чим забезпечується підвищення криптостійкості процедури передачі даних.

На відміну від описаного у роботі [1] здійснено реалізацію нейроподібної мережі з використанням мікрокомп'ютера на базі SoC, що забезпечило ширші можливості щодо налаштування та відлагодження алгоритмів. У роботі [12] запропоновано систолічну структуру для реалізації на ПЛІС, на підставі якої реалізують нейронні мережі прямого поширення, наприклад, багатошаровий персептрон, автоматичний кодер і логічна регресія. На відміну, пропоновану нейроподібну мережу можна реалізувати програмно або апаратно, що підвищує гнучкість застосування та не вимагає ітераційного навчання. Вагові коефіцієнти нейроподібної мережі для криптографічного захисту розраховують неітераційним методом, що значно пришвидшує процес навчання.

Подібно до представленого у роботі [5] підходу до побудови згорткових нейронних мереж за допомогою центральних процесорів загального призначення, DSP і GPGPU та реалізації на ПЛІС, пропоноване у роботі використання таблично-алгоритмічного методу неітераційного обчислення вагових коефіцієнтів забезпечує можливість ефективної реалізації на ПЛІС та відповідне зростання продуктивності, особливо у задачах криптографічного захисту даних при їх передачі.

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

Наукова новизна отриманих результатів дослідження – вперше розроблено модель попередніх налаштувань системи нейроподібного шифрування даних, яка окреслює вибір структури нейроподібної мережі, обчислення матриці вагових коефіцієнтів і таблиці макрочасткових добутків, реалізація якої забезпечує зменшення часу налаштування.

Розроблено модель процесу нейроподібного шифрування з використанням таблично-алгоритмічного методу, що забезпечує тестування системи криптографічного захисту й передачі даних у реальному часі.

Отримали подальший розвиток моделі тестування та відлагодження блоків шифрування (дешифрування), кодування (декодування), маскування (демаскування) даних, які за рахунок використання еталонних значень для порівняння забезпечують підвищення якості тестування та відлагодження системи криптографічного захисту.

Практична значущість результатів дослідження – розроблена система криптографічного захисту й передачі даних з використанням запропонованих моделей забезпечує підвищення криптостійкості процедури передачі даних і може застосовуватись у мобільних робототехнічних платформах внаслідок можливості досяг-

нення високих масо-габаритних показників і низького енергоспоживання при апаратній реалізації нейроподібної мережі.

Висновок / Conclusions

Розроблено моделі та засоби попередніх налаштувань, нейроподібного шифрування, відлагодження й тестування СКЗПД. За результатами виконаної роботи можна зробити такі основні висновки.

1. Представлено модель попередніх налаштувань для реалізації нейроподібного шифрування/дешифрування даних основними компонентами якої є формувач архітектури нейроподібної мережі, обчислювач матриць вагових коефіцієнтів і обчислювач таблиць макрочасткових добутків. Реалізація вказаної моделі забезпечує зменшення часу налаштування. Розроблено модель нейроподібного шифрування даних і команд управління з використанням таблично-алгоритмічного методу основними компонентами якої є перетворювач повідомлення, формувач адреси зчитування з таблиць, N таблиць макрочасткових добутків, N суматорів і комутатор, реалізація якої забезпечує тестування СКЗПД у реальному часі. Реалізовано моделі тестування та відлагодження блоків шифрування/дешифрування, кодування/декодування, маскування /демаскування даних, які за рахунок використання еталонних значень для порівняння забезпечують підвищення якості тестування та відлагодження СКЗПД.

2. Представлено СКЗПД, яка за рахунок динамічної зміни типу архітектури НПМ (значення ВК), кодів маски та БПК забезпечує підвищення криптостійкості процедури передачі даних. Запропоновано динамічно змінювати тип архітектури НПМ, значення ВК, маски та БПК синхронно кількості тактових імпульсів, які поступають на відповідні лічильники.

3. Виконано тестування імітаційної моделі на прикладі повідомлення n=16 для нейроподібної мережі. З'ясовано, що тривалість виконання процедур нейромережевого криптографічного шифрування/дешифрування блоків даних при реалізації на мікрокомп'ютері становить біля відповідно 15 мс та 10 мс для лінійної нейроподібної мережі та відповідно 65 мс та 70 мс для степені полінома P_{max}=15 для нелінійного типу мережі. Отримані значення тривалості слід вважати прийнятними для забезпечення роботи у режимі реального часу, а подальшого зменшення тривалості вказаних операцій можна досягнути шляхом реалізації запропонованих нейроподібних елементів апаратними засобами ПЛІС.

References

[1] Cai, J., Takemoto, M., & Nakajo, H. (2018). Implementation of DNN on a RISC-V Open Source Microprocessor for IoT devices. 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE), pp. 295–299. https://doi.org/10.1109/GCCE.2018.8574663

[2] Cai, L., et al. (2019). TEA-DNN: the Quest for Time-Energy-Accuracy Co-optimized Deep Neural Networks. 2019 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED), pp. 1–6. https://doi.org/10.1109/ISLPED.2019.8824934

[3] Dong, T., & Huang, T. (2020). Neural Cryptography Based on Complex-Valued Neural Network, in IEEE Transactions on Neural Networks and Learning Systems, *31*(11), 4999–5004. https://doi.org/10.1109/TNNLS.2019.2955165

[4] Forgáč, R., & Očkay, M. (2019). Contribution to Symmetric Cryptography by Convolutional Neural Networks, Communication and Information Technologies (KIT), 1–6. https://doi.org/10.23919/KIT.2019.8883490

[5] Hadnagy, Á., Fehér, B., & Kovácsházy, T. (2018). Efficient implementation of convolutional neural networks on FPGA. *2018 19th International Carpathian Control Conference* (ICCC), pp. 359-364. https://doi.org/10.1109/CarpathianCC.2018.8399656

[6] Jiang, L. (2020). The Application Analysis of Computer Network Security Data Encryption Technology. In: Abawajy, J., Choo, KK., Xu, Z., Atiquzzaman, M. (Eds). 2020 International Conference on Applications and Techniques in Cyber Intelligence. ATCI 2020. Advances in Intelligent Systems and Computing, 1244. Springer, Cham. https://doi.org/10.1007/978-3-030-53980-1_21

[7] Kotsovsky, V., Batyuk, A., & Mykoriak, I. (2020). The Computation Power and Capacity of Bithreshold Neurons. 2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020. Proceedings, 1, pp. 28-31. https://doi.org/10.1109/CSIT49958.2020.9322014

[8] Meraouche, I., Dutta, S., Tan, H., & Sakurai, K. (2021). Neural Networks-Based Cryptography: A Survey. In IEEE Access, 9, pp. 124727–124740. https://doi.org/10.1109/ACCESS.2021.3109635

[9] Peleshchak, R., Lytvyn, V., Kholodna, N., Peleshchak, I., & Vysotska, V. (2022). Two-Stage AES Encryption Method Based on Stochastic Error of a Neural Network. IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), pp. 381–385. https://doi.org/10.1109/TCSET55632.2022.9766991

[10] Saraswat, P., Garg, K., Tripathi, R., & Agarwal, A. (2019). Encryption Algorithm Based on Neural Network. 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 1–5. https://doi.org/10.1109/IoT-SIU.2019.8777637

[11] Sumayyabeevi, V. A., Poovely, J. J., Aswathy, N., & Chinnu, S. (2021). A New Hardware Architecture for FPGA Implementation of Feed Forward Neural Networks. 2021 2nd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS), pp. 107–111. https://doi.org/10.1109/ACCESS51619.2021.9563342

[12] Sumayyabeevi, V. A., Poovely, J. J., Aswathy, N., & Chinnu, S. (2021). A New Hardware Architecture for FPGA Implementation of Feed Forward Neural Networks. 2021 2nd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS), pp. 107-111. https://doi.org/10.1109/ACCESS51619.2021.9563342

[13] Tkachenko, R., Tsmots, I., Tsymbal, Y., Skorokhoda, O. (2019). Neural-like Methods and Hardware Structures for Real-time Data Encryption and Decryption. International Scientific and Technical Conference on Computer Sciences and Information Technologies, 3, 248-253. https://doi.org/10.1109/STC-CSIT.2019.8929809

[14] Tsmots, I., & Skorokhoda, O. (2010). Methods and VLSI-structures for neural element implementation. Perspective Technologies and Methods in MEMS Design, MEMSTECH2010 – Proceedings of the 6th International Conference, 135.

[15] Tsmots, I., Rabyk, V., Skorokhoda, O., & Teslyuk, T. (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, pp. 154-158. https://doi.org/10.1109/ELIT.2019.8892334

[16] Tsmots, I., Rabyk, V., Skorokhoda, O., & Tsymbal, Y. (2021). Neural-like real-time data protection and transmission

system. Advances in Intelligent Systems and Computing (AISC), 1293: Advances in Intelligent Systems and Computing V. Selected papers from the International conference on computer science and information technologies. https://doi.org/10.1007/978-3-030-63270-0_8
[17] Tsmots, I., Teslyuk, V., Lukashchuk, Y., & Opotiak, Y. (2022). Method of Training and Implementation on the Basis of Neural Networks of Cryptographic Data Protection CEUR Workshop Proceedings, 3171, 916-928.
[18] Tsmots, I., Tsymbal, Y., Khavalko, V., Skorokhoda, O., & Tesluyk, T. (2018). Neural-Like Means for Data Streams Encryption and Decryption in Real Time. Processing of the 2018. IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018, 438-443. https://doi.org/10.1109/DSMP.2018.8478513
[19] Valavi, H., Ramadge, P. J., Nestler, E., & Verma, N. (2018). A Mixed-Signal Binarized Convolutional-Neural-Network Accelerator Integrating Dense Weight Storage and Multiplication for Reduced Data Movement, 2018 IEEE Symposium on VLSI Circuits, 141–142. https://doi.org/10.1109/VLSIC.2018.8502421
[20] Wang, J., Cheng, L.-M., & Su, T. (2018). Multivariate Cryptography Based on Clipped Hopfield Neural Network, in *IEEE Transactions on Neural Networks and Learning Systems,* *29*(2), 353–363. https://doi.org/10.1109/TNNLS.2016.2626466
[21] Zhu, Y., Vargas, D. V., & Sakurai, K. (2018). Neural Cryptography Based on the Topology Evolving Neural Networks. 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), 472–478. https://doi.org/10.1109/CANDARW.2018.00091
[22] Zolfaghari, B., & Koshiba, T. (2022). The Dichotomy of Neural Networks and Cryptography: War and Peace. Appl. Syst. Innov., 5, 61. https://doi.org/10.3390/asi5040061

I. G. Tsmots, V. M. Teslyuk, Yu. V. Opotiak, I. V. Pikh

Lviv Polytechnic National University, Lviv, Ukraine

MODELS AND TOOLS FOR DEBUGGING AND TESTING MOBILE SYSTEMS FOR NEURO-LIKE CRYPTOGRAPHIC PROTECTION OF DATA TRANSMISSION

The work revealed the need for providing cryptographic protection and immunity to data transmission and control commands when using the mobile robotic platform as well as the importance of taking into account the limitations regarding dimensions, energy consumption and productivity. It was found that one of the ways to meet the requirements of cryptographic protection is the use of neuro-like networks. Their feature is the ability to pre-calculate the weight coefficients that will be used when encrypting/decrypting data. It is suggested that during neuro-like encryption/decryption of data, the key should be generated taking into account the architecture of the neuro-like network (the number of neurons, the number of inputs and their bit rate), the matrix of weight coefficients and the table for masking. It was determined that a neural network with pre-calculated weight coefficients makes it possible to use a table-algorithmic method for data encryption/decryption, which is based on the operations of reading from memory, adding and shifting. Limitations regarding dimensions, energy consumption and performance are analyzed. They can be overcome during implementation by using a universal processor core supplemented with specialized FPGA hardware for neuro-like elements. That is the combined use of software and specialized hardware ensures the effective implementation of neuro-like data encryption/decryption algorithms and management teams. Models and tools for debugging and testing a neuro-like cryptographic system are presented. A model of the preliminary settings of the neuro-like data encryption system has been developed, the main components of which are the former of the neuro-like network architecture, the calculator of weight coefficient matrices and the calculator of tables of macro-partial products. A model of the process of neuro-like encryption of control commands using a table-algorithmic method has been developed. Models for testing and debugging blocks of encryption (decryption), encoding (decoding), and masking (unmasking) of data have been developed, which, due to the use of reference values for comparison, ensure an increase in the quality of testing and debugging of the cryptographic system. A cryptographic system was developed, which, as a result of a dynamic change in the type of neuro-like network architecture and the values of weighting coefficients, mask codes and barker-like code, provides an increase in the crypto-resistance of data transmission. Testing of the simulation model was carried out on the example of message transmission for various configurations of a cryptographic system.

Keywords: tabular-algorithmic method of calculating the weight coefficients of a neuro-like network; simulation model of neuro-like encryption/decryption; dynamic change of the architecture of the neuro-like network; calculation of tables of macro-partial products.

Інформація про авторів:

Цмоць Іван Григорович, д-р техн. наук, професор, кафедра автоматизованих систем управління.
Email: ivan.g.tsmots@lpnu.ua; https://orcid.org/0000-0002-4033-8618

Теслюк Василь Миколайович, д-р техн. наук, професор, зав. кафедри автоматизованих систем управління.
Email: vasyl.m.teslyuk@lpnu.ua; https://orcid.org/0000-0002-5974-9310

Опотяк Юрій Володимирович, канд. техн. наук, доцент, кафедра автоматизованих систем управління.
Email: yurii.v.opotiak@lpnu.ua; https://orcid.org/0000-0001-9889-4177

Піх Ірина Всеволодівна, д-р техн. наук, професор, кафедра автоматизованих систем управління.
Email: iryna.v.pikh@lpnu.ua; https://orcid.org/0000-0002-9909-8444

Цитування за ДСТУ: Цмоць І. Г., Теслюк В. М., Опотяк Ю. В., Піх І. В. Моделі та засоби відлагодження й тестування мобільних систем для нейроподібного криптографічного захисту й передачі даних. *Український журнал інформаційних технологій.* 2022, т. 4, № 2. С. 45–55.

Citation APA: Tsmots, I. G., Teslyuk, V. M., Opotiak, Yu. V., & Pikh, I. V. (2022). Models and tools for debugging and testing mobile systems for neuro-like cryptographic protection of data transmission. *Ukrainian Journal of Information Technology, 4*(2), 45–55. https://doi.org/10.23939/ujit2022.02.045