7. *Uday Bondhugula* Effective Automatic Parallelization and Locality Optimization Using The Polyhedral Model. – The Ohio State University, 2010.
8. *Pouchet L.N.*, The polyhedral benchmark suite [Online]. Available: http://web.cs.ucla.edu /*pouchet/software/polybench/ 22 Sept 2016

Поступила 22.02.2018р.

УДК 004.032.26 : 004.056.55

І.Г. Цмоць, д.т.н., НУ «Львівська політехніка», Львів
Ю.В. Цимбал, к.т.н., НУ «Львівська політехніка», Львів
О.В. Скорохода, к.т.н., НУ «Львівська політехніка», Львів
В.М. Хавалко, к.т.н., НУ «Львівська політехніка», Львів
Т.В. Теслюк, НУ «Львівська політехніка», Львів

АПАРАТНА РЕАЛІЗАЦІЯ НЕЙРОМЕРЕЖЕВИХ ЗАСОБІВ ШИФРУВАННЯ-ДЕШИФРУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ ДАНИХ

Abstract. The “model of successive geometric transformations” paradigm has been adapted for the implementation of parallel-streaming neural network encryption-decryption of data in real time. A model and structure of a parallel-streaming neural-like network for the mode have been developed.

Keywords*:* intensive data stream; neural networks; geometric transformations model

Постановка проблеми

Розвиток новітніх інформаційних технологій та засобів комунікацій, забезпечують все більш широкі можливості доступу до інформаційних ресурсів і переміщення великих масивів даних на необмежені відстані. Широке впровадження інформаційних технологій робить закономірною та актуальною проблему захисту передачі інформації з використанням криптографічних методів, які забезпечують шифрування готової до передачі інформації. Зашифрована інформація передається каналом зв’язку до санкціонованого користувача, який після її отримання виконує дешифрування за допомогою зворотного перетворення. Криптографічні перетворення здійснюються шляхом використання спеціальних алгоритмів. Для шифрування та дешифрування потоків даних у реальному часі пропонується використати нейроподібні мережеві алгоритми, ключем в яких використовуються архітектура мережі, вагові коефіцієнти та коди маскування. Забезпечити реальний час шифрування та дешифрування інтенсивних потоків можна шляхом НВІС-реалізації відповідних алгоритмів. Для синтезу нейроподібних елементів і нейроподібних мереж реального часу необхідно

розробити нові паралельно-потокові нейроподібні елементи та мережі, які забезпечують просторово-часове розпаралелення алгоритмів шифрування та дешифрування.

Тому актуальною проблемою є розроблення апаратних нейроподібних мереж шифрування-дешифрування інтенсивних потоків даних в реальному часі.

Аналіз публікацій

Аналіз робіт [1-10] дозволив виділити особливості задач і архітектур нейрокомп'ютерів реального часу, а також показати, що задачі шифрування-дешифрування у реальному часі характеризуються високою інтенсивністю, постійністю вхідних потоків даних і підвищенням вимог до часу життя ключа.

В [1-6] проаналізовано існуючі нейромережі та засоби їх реалізації і показано, що переважна більшість нейромереж реалізується програмним шляхом. Такі нейромережі мають відносно невисоку продуктивність і не забезпечують опрацювання інтенсивних потоків даних у реальному часі.

З аналізу робіт [1-10] видно, що для забезпечення високої продуктивності нейромереж реального часу необхідно використовувати апаратну реалізацію та сучасну елементну базу, а також три базових принципи: паралелізм обробки; програмованість структури; регулярність (однорідність) структури. Такий підхід забезпечується поєднанням принципів конвеєризації, векторної та матричної програмно-апаратної організації обчислень на базі новітніх технологій елементної бази.

Основними компонентами апаратних нейромереж є різні моделі штучних нейроелементів. Вибір моделі штучного нейрона залежить від вимог конкретних застосувань. В [7] розглянуто моделі та НВІС-структури формального нейрона паралельно-вертикального типу [8-10], які відрізняються між собою способом надходження та опрацювання вхідних даних та вагових коефіцієнтів – з використанням мультиплексування шин, з суміщенням процесів надходження та опрацювання даних та з табличним формуванням макрочасткових результатів. Недоліком даних моделей та НВІС-структур формального нейрона є відносно невисока швидкодія.

З проведеного аналізу слідує, що синтез апаратних нейромереж для задач шифрування та дешифрування потоків даних у реальному часі вимагає розроблення нової моделі та нових НВІС-структур нейроелемента, які повинні бути орієнтовані на опрацювання інтенсивних потоків даних.

Метою роботи є адаптація моделі послідовних геометричних перетворень до задач шифрування-дешифрування даних, розроблення моделі, структури паралельно-потокового нейроподібного елемента та синтез на його базі паралельно-потокової нейроподібної мережі шифрування-дешифрування потоків даних.

Основна частина

Базова структура системи криптографічного захисту. У системах передачі інтенсивних потоків даних (системи зв'язку) із шифрування і дешифрування їх у режимі реального часу (системи криптографічного захисту) прослідковується низка аналогій, що дозволяє ототожнювати такі

системи. Зокрема, розглянувши принцип впливу завад в каналі зв'язку на інформацію та дію алгоритму шифрування на повідомлення, можна стверджувати, за Шенноном, про шифртекст як аналог спотвореного сигналу. Проте, дані системи мають ряд розбіжностей, що полягають у складності процесу шифрування, природі ключа та спеціалізованому захисті характеристик інформації.

Розглянемо структуру системи криптографічного захисту (рис.1) для обґрунтування розробленого алгоритму шифрування, що базується на поєднанні основ процесу шифрування та принципів навчання нейронної мережі. Криптографічна система визначається абстрактно як деяка множина відображень одного простору (множини можливих повідомлень) в інший простір (множину можливих шифртекстів). Кожне відображення з цієї множини відповідає способу шифрування за допомогою ключа.

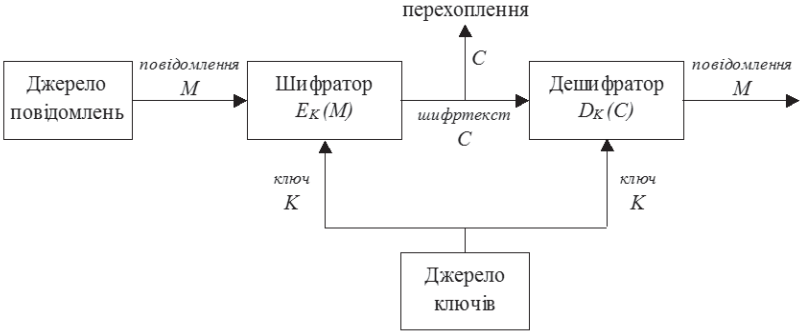

Рис. 1. Базова структура системи криптографічного захисту

Для функціонування криптографічної системи (рис. 1) обирається деякий ключ для шифратора/дешифратора. Вибір ключа визначає певне відображення з множини відображень (алгоритм шифрування), що складають систему. Вибирається повідомлення і за допомогою вибраного відображення формується відповідний шифртекст. Цей шифртекст передається по каналу зв'язку та може бути перехоплений. Після передачі за допомогою оберненого відображення з шифртексту відновлюється початкове повідомлення.

Система криптографічного захисту оперує наступними об'єктами:

1) *Алфавіт* A, в якому записуються повідомлення (відкриті тексти). Повідомлення M є словом в цьому алфавіті (яке може складатись з багатьох слів у звичайному лінгвістичному розумінні), тобто $M \in A^*$, де A^* – простір повідомлень.

2) *Алфавіт* B, в якому записуються шифртексти. Відповідно, $C \in B^*$, де C – шифртекст, B^* – простір шифртекстів.

3) *Простір ключів* K^*, що складається із слів деякого алфавіту.

4) *Шифруюче відображення* $E_K : A^* \to B^*, K \in K^*$ відбувається за

допомогою базових операцій над відкритим текстом: підстановки, перестановки, циклічного зсуву, додавання та множення за модулем, причому послідовність таких операцій становить алгоритм шифрування.

5) *Дешифруюче відображення* $D_K : B^* \to A^*, K \in K^*$ перетворює шифртекст у вихідний відкритий текст.

В системі криптографічного захисту припускається, що відображення є взаємно-однозначними для одержання єдиного результату шифрування/дешифрування.

Актуальним практичним питанням на всьому етапі розвитку криптографії було створення *абсолютно стійких* (або досконалих) шифрів. Основні вимоги, які висуваються до досконалого шифру, полягають в забезпеченні неможливості успішного криптоаналізу.

На сьогоднішній день відомим абсолютно стійким шифром можна вважати шифр Вернама (або шифр одноразового блокноту). Проте, практична реалізація цього шифру ускладнюється внаслідок ідентичності довжин ключа та відкритого тексту; відповідно із збільшенням об'єму вихідної інформації збільшується розмір ключа. Необхідно зазначити, що в основі стійкості шифру Вернама лежить принцип, який був пізніше формально доведений Шенноном.

Модель послідовних геометричних перетворень. Одним з перспективних напрямків для побудови високоефективних нейромережевих засобів шифрування і дешифрування даних у режимі реального часу є застосування парадигми «модель послідовних геометричних перетворень» (МПГП), запропонованої і розробленої Р.О. Ткаченком [11-12].

В основі цієї парадигми лежить неітераційний підхід до навчання нейроподібної мережі, який передбачає пряме обчислення вагових коефіцієнтів під час поступового зменшення розмірності простору вхідних багатовимірних даних на нейронах прихованого шару [11].

Апаратна реалізація таких нейроподібних мереж за допомогою НВІС-структур може значно спроститися за умови подання вхідних, вихідних даних та вагових коефіцієнтів мережі МПГП у форматі з фіксованою комою. Для цього передбачається попереднє масштабування вхідних даних.

Застосування парадигми МПГП в задачах шифрування-дешифрування даних. При виборі структури нейроподібної мережі для шифрування-дешифрування потоків даних у реальному часі пропонується використати архітектуру автоасоціативної мережі з одним прихованим шаром [12].

Така структура мережі є досить універсальною і може бути використана при розв'язанні різних задач, які передбачають перетворення вхідних даних з подальшим їх відновленням: кодування вхідних даних з метою їх стиснення, блочне симетричне шифрування, накладання цифрових водяних знаків (на зображення) та стеганографії. Модулі шифрування та дешифрування даних, відповідно, формують та використовують ключ, який утворюють параметри

навченої нейромережі. Для підвищення криптостійкості даних на виході прихованого шару структуру мережі можна доповнити блоком шифрування за методом одноразового блокноту (накладанням маски операцією XOR).

При кількості нейронів у прихованому шарі рівній кількості вхідних і вихідних нейронів забезпечується можливість відновлення без втрат на виході мережі захищених даних, які будуть отримані на виходах нейронів прихованого шару. Зворотні послідовні геометричні перетворення між нейронами прихованого та вихідного шару використовуються для відновлення даних на виходах мережі. Передбачена можливість послідовного з'єднання декількох блоків шифрування та наступних відповідних блоків дешифрування з утворенням каскадної багатошарової мережі.

Структура паралельно-потокової нейроподібної мережі шифрування-дешифрування даних. Структура паралельно-потокової нейроподібної мережі шифрування-дешифрування даних у реальному часі будемо синтезувати на базі моделі паралельно-потокового нейроподібного елемента [7]. Метою синтезу є отримання модульної та регулярної структури орієнтованої на НВІС-технологію. Вихідною інформацією для синтезу нейроподібної мережі шифрування-дешифрування даних у реальному часі є: алгоритми навчання та функціонування нейромережі; графове відображення нейромережі; кількість вхідних даних і нейронів; інтенсивність надходження вхідних даних; вимоги до інтерфейсу; розрядність вхідних даних, вагових коефіцієнтів і точність обчислень; техніко-економічні вимоги і обмеження.

Структура нейроподібної мережі для шифрування даних наведена на рис. 2, де де *ПЕ* – процесорний елемент, *Рг* – регістр, *ОЗП* – оперативний запам'ятовуючий пристрій, *См* – суматор, *Вд* – віднімач, $У_1$, $У_2$, $У_3$ – перший, другий і третій входи управління, *ВхD* – вхід даних, *ВихY* – вихід результату шифрування.

Шифрування потоків даних за допомогою паралельно-потокової нейроподібної мережі вимагає попереднього обчислення вагових коефіцієнтів W_j, формування макрочасткових добутків P_M та їх одночасно запису в усі $ОЗПР_M$. Особливістю розробленої структури паралельно-потокового нейроподібної мережі шифрування є те, що дані поступають послідовно одне за одним і за допомогою вхідних $РгВХ_1$,…, $РгВХ_N$ перетворюються у паралельний потік даних, які надходять на вхід першого $ПЕ_1$. Паралельно-потокова нейроподібна мережі реалізується на базі *n* однотипних ПЕ, які працюють за конвеєрним принципом. Такт роботи конвеєра такої мережі рівний такту роботи нейроподібного елемента (10). У кожному такті роботи обчислені скалярні добутки записуються в регістри $РгZ1_n$,…, $РгZN_n$, а з них у регістри $РгY_1$,…, $РгY_N$ за допомогою яких виконується паралельно-послідовне перетворення надходження скалярних добутків. На виході віднімача *Вд* формується потік зашифрованих даних.

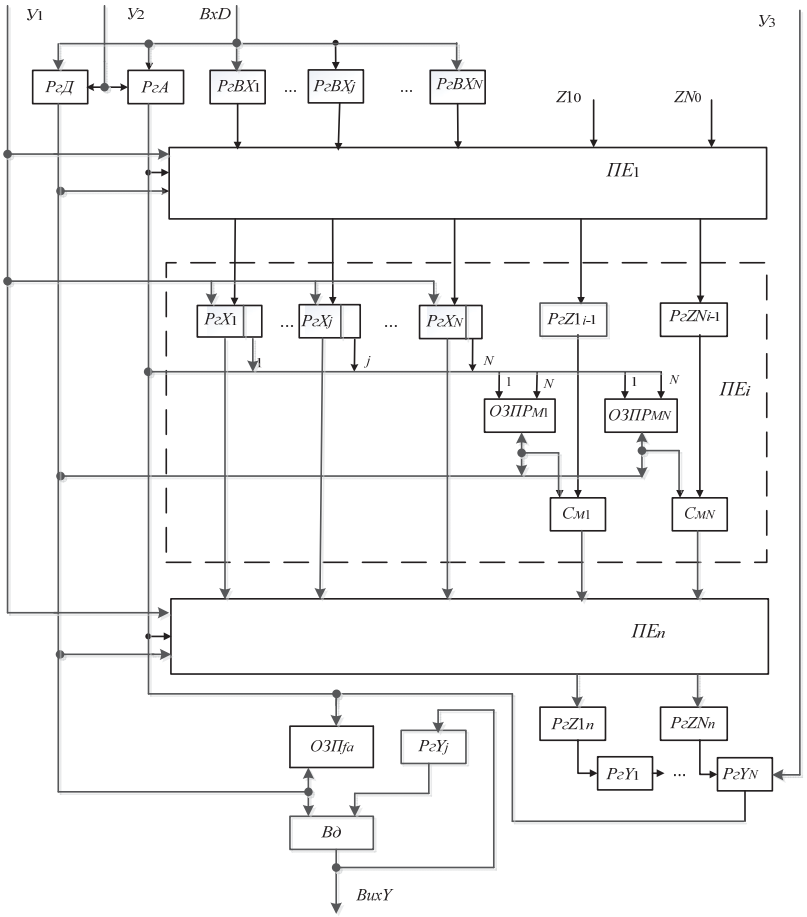

Рис. 2. Структура паралельно-потокової нейроподібної мережі шифрування потоків даних

Висновки

Адаптовано парадигму модель послідовних геометричних перетворень для реалізації паралельно-потокової нейроподібної мережі шифрування-дешифрування даних у реальному часі.

В основу розробки паралельно-потокової нейроподібної мережі шифрування та дешифрування потоків даних доцільно покласти такі принципи: конвеєризації та просторового паралелізму; однорідності та модульності структури; попереднього обчислення вагових коефіцієнтів; табличного формування макрочасткових добутків і функції активації.

1. *Палагин А.В., Яковлев Ю.С.* Системная интеграция средств компьютерной техники. – Вінниця: УНІВЕРСУМ-Вінниця, 2005. – 680 с.
2. *Грибачев В.П.* Элементная база аппаратных реализаций нейронных сетей // Компоненты и технологии. 2006. № 8.
3. *McCulloch W.S., Pitts W.* A logical calculus of the ideas immanent in nervous activity // The Bulletin of Mathematical Biophysics. – 1943. – Vol. 5, Issue 4. – pp. 115–133.
4. *Fukushima K.* Cognitron: A self-organizing multilayered neural network // Biological cybernetics. – 1975. – Vol. 20, Issue 3-4. – pp. 121–136.
5. *Hopfield J.J.* Neural networks and physical systems with emergent collective computational abilities // Proceedings of the national academy of sciences. – 1982. – Vol. 79, Issue 8. – pp. 2554–2558.
6. *Хайкин С.* Нейронные сети. – М.: Вильямс, 2006. – 1104 с.
7. *Рашкевич Ю.М., Ткаченко Р.О., Цмоць І.Г, Пелешко Д.Д.* Нейроподібні методи, алгоритми та структури обробки сигналів і зображень у реальному часі: монографія. – Львів: Видавництво Львівської політехніки, 2014. – 256 с.
8. *Цмоць І.Г., Скорохода О.В., Балич Б.І.* Модель та НВІС-структури формального нейрона паралельно-вертикального типу з використанням мультиплексування шин // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова – Львів. – 2013. – Випуск № 67. – С. 160-166.
9. *Цмоць І.Г., Скорохода О.В., Балич Б.І.*Модель та НВІС-структура формального нейрона паралельно-вертикального типу з табличним формуванням макрочасткових результатів // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова – Львів. – 2014. – Випуск № 73. – С. 133-138.
10. *Tsmots I., Skorokhoda O., Rabyk V., Ignatyev I.* Basic vertical-parallel real time neural network components // Proceedings of the XIIth International Scientific and Technical Conference “Computer Sciences and Information Technologies” (CSIT). – 2017, Lviv. – pp. 344–347.
11. *Грицик В.В., Ткаченко Р.О.* Нові підходи до навчання штучних нейромереж // Доповіді Національної академії наук України. – 2002. – № 11. – С.59-65.
12. *Tsymbal Y., Tkachenko R.* A digital watermarking scheme based on autoassociative neural networks of the geometric transformations model // Proceedings of the 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP). – 2016. – pp. 231-234.

Поступила 29.01.2018р.

УДК 004.62

В.Р.Сподарик, Національний університет «Львівська політехніка»

ПРОЕКТУВАННЯ ГЕОІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ АНАЛІЗУ РУХУ ГРОМАДСЬКОГО ТРАНСПОРТУ

Abstract. In this article analyzed available options for obtaining information about public transport traffic. Des cribed the scheme of functioning of the system for real-time information collection, the work of the system has been implemented and tested for one year with monitoring 24/7. Collected data can be used for various kinds of analytics and forecasting of possible traffic jams or road accidents.