УДК 004.032.26, 004.056.55

Ю. В. Цимбал
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

НЕЙРОМЕРЕЖЕВИЙ МЕТОД СИМЕТРИЧНОГО ШИФРУВАННЯ ДАНИХ

© Цимбал Ю. В., 2018

Розглянуто метод симетричного шифрування даних на основі нейронних мереж моделі геометричних перетворень (МГП). Ключ шифрування складається зі значень на входах навчальної та тестової множин мережі. Використовується властивість мереж МГП формувати гіперплощину, що проходить через точки навчальної множини. Показано можливості застосування розробленого методу для шифрування растрових зображень.

Ключові слова: нейронні мережі прямого поширення, модель геометричних перетворень.

The method of symmetric data encryption on the basis of neural networks of the geometric transformations model (GTM) has been considered. Encryption key consists of input values of the training and test sets of the network. The property of the GTM networks to form a hyperplane that passes through the points of the training set has been used. The possibilities of application of the developed method for encryption of raster images have been shown.

Key words: feed-forward neural networks, geometric transformation model.

Вступ

Із розвитком технологій зберігання і передачі даних дедалі більшого значення набувають проблеми захисту інформації, зокрема, за допомогою методів шифрування. Сучасні технології криптоаналізу, які використовують доступні ресурси для високопродуктивних обчислень, поставили під сумнів стійкість багатьох класичних алгоритмів шифрування даних і сприяли розвитку нових підходів.

Одним із сучасних напрямків розробки ефективних і стійких методів криптографічного захисту стали технології штучних нейронних мереж, які вирізняються різноманітністю архітектур та алгоритмів навчання, а також можливостями гнучкого налаштування, зокрема і для задач симетричного шифрування даних.

Огляд досліджень та публікацій

В [1–2] розглянуто застосування для побудови систем криптографічного захисту нейронних мереж прямого поширення, що навчаються за алгоритмом зворотного поширення похибки (back propagation). У [3–4] розглянуто можливості застосування рекурентних нейронних мереж, зокрема мережі Гопфілда. Також розроблені схеми криптографічного захисту на основі нейромереж зустрічного поширення (counter propagation) [5] та радіальних базисних функцій [6]. Спільною особливістю цих підходів є застосування алгоритмів ітераційного навчання, що обмежує можливості їхнього використання у системах захисту даних у реальному часі. Мета досліджень, розглянутих у цій статті, – розробити метод симетричного шифрування даних на основі нейронних мереж з неітераційним навчанням.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Метод симетричного шифрування
на основі нейронної мережі геометричних перетворень

Запропонований метод симетричного шифрування ґрунтується на застосуванні архітектури нейронної мережі прямого поширення із латеральними зв'язками між нейронами прихованого шару, що навчається на основі парадигми "модель геометричних перетворень" (МГП) [7] (рис. 1).

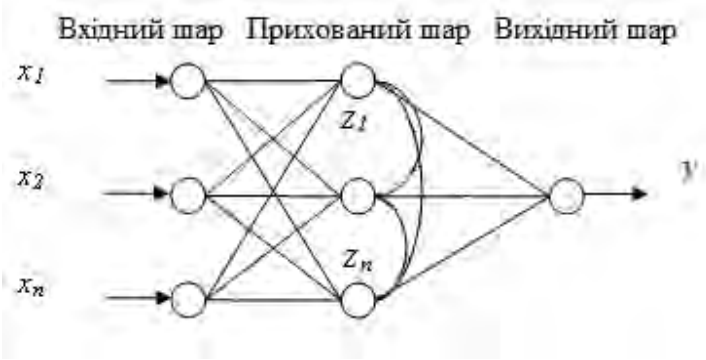


Рис. 1. Нейронна мережа із латеральними зв'язками між нейронами прихованого шару

Визначальною особливістю нейромереж МГП є побудова на прихованому шарі гіперплощини заданої розмірності у просторі вхідних даних. Ця гіперплощина наближає сукупність вхідних даних з мінімальною дисперсією (за аналогією зі статистичним методом головних компонент), використовуючи при переході до нового базису ортогоналізацію Грама-Шмідта. Якщо обрати кількість векторів навчальної множини на 1 більшою за кількість входів, то при побудові гіперплощини із розмірністю, що дорівнює кількості входів, забезпечується відсутність залишкової дисперсії (похибки перетворення).

В основі пропонованого методу симетричного шифрування є використання двох однотипних мереж МГП вказаної вище структури – нейромережі шифрування та нейромережі дешифрування. Передбачається формування симетричного ключа (*Key*), що складається з двох рівних за розміром частин. Перша частина (*Key1*) подається на вхід нейронної мережі МГП на етапі навчання. Виходом мережі на етапі навчання є сукупність даних для шифрування (*Original Data*). Друга частина (*Key2*) подається на вхід навченої мережі на етапі застосування. Між елементами *Key1* та Key2 не має бути лінійної залежності. Значення на виході при цьому утворюють сукупність зашифрованих вхідних даних (*Encrypted Data*), які належать побудованій на етапі навчання гіперплощині (рис. 2).

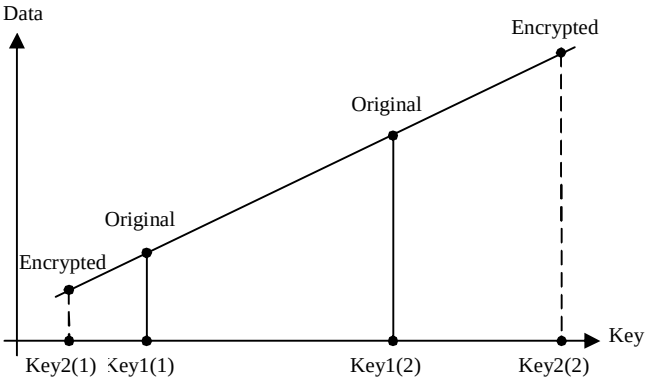


Рис. 2. Гіперплощина у нейромережі шифрування, побудована на елементах ключа Key1 і застосована для елементів ключа Key2

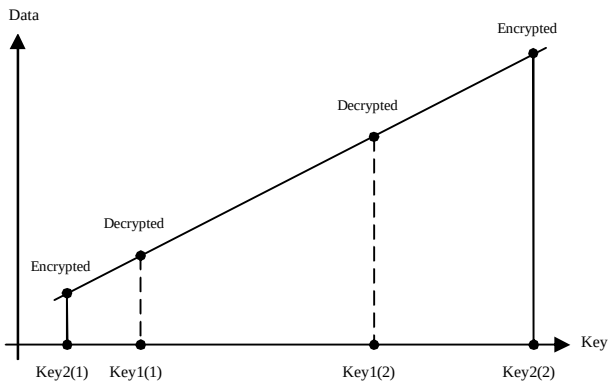


Рис. 3. Гіперплощина у нейромережі дешифрування, побудована на елементах ключа Key2 і застосована для елементів ключа Key1

При дешифруванні частина ключа *Key2* подається на вхід нейронної мережі на етапі навчання. Виходом мережі буде сукупність зашифрованих даних (*Encrypted Data*). При цьому

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

відновлюється гіперплощина, що була утворена під час шифрування. Частина ключа *Key1* подається на вхід навченої мережі на етапі застосування. Значення на виході при цьому складуть сукупність дешифрованих вхідних даних (*Decrypted Data*) (рис. 3).

Базовий алгоритм навчання та застосування нейронної мережі геометричних перетворень

Етап навчання мережі

1. Сформувати файл даних для навчання з N векторів навчальної множини $X_{i,1}, X_{i,2},..., X_{i,j},..., X_{i,n}$, $Y_{i,1}, Y_{i,2},..., Y_{i,f},..., Y_{i,F}$, де тут і надалі: $i = \overline{1,N}$ – номер вектора; $j = \overline{1,n}$ – номер j-ї вхідної компоненти вектора, $X_{i,j}$ – j-а вхідна компонента i-го вектора; $f = \overline{1,F}$ – номер f-ї вихідної компоненти вектора, $Y_{i,f}$ – f-а вихідна компонента i-го вектора. Для задачі симетричного шифрування обираємо $F = 1$.

2. Сформувати файл даних для застосування з $N1$ векторів тестової множини $X^t_{k,1}, X^t_{k,2},..., X^t_{k,j},..., X^t_{k,n}$, $Y^t_{k,1}, Y^t_{k,2},..., Y^t_{k,f},..., Y^t_{k,F}$, де тут і надалі $k = \overline{1,N1}$ – номер вектора. Вихідні компоненти векторів тестової множини можуть бути відсутні.

3. Задати кількість нейронів прихованого шару m, яка для задачі симетричного шифрування дорівнює кількості входів мережі n.

4. Для векторів навчальної множини виконати нормування входів і виходів по стовпцях до діапазону [-1; +1], відповідно:

$$x_{i,j} = X_{i,j} / X_j^{\max}\ , y_{i,f} = Y_{i,f} / Y_f^{\max},$$

де $X_j^{\max}$ – модуль максимального за модулем елемента j-го стовпця входів навчальної множини; $Y_f^{\max}$ – модуль максимального за модулем елемента f-го стовпця виходів навчальної множини.

5. Обчислити центр мас для N елементів навчальної множини $x_j^c = \left(\sum_{i=1}^{N} x_{i,j} \right) / N$;

$y_f^c = \left(\sum_{i=1}^{N} y_{i,f} \right) / N$.

6. Центрувати дані навчальної множини: $x1_{i,j} = x_{i,j} - x_j^c$, $y1_{i,f} = y_{i,f} - y_f^c$.

7. Задати початкове значення номера кроку перетворень S = 1 і повторювати п.п. 8-12, інкрементуючи значення S ($S = S + 1$), $S_{\max} = m$.

8. Для кожного нового S обрати базовий рядок (позначений як $xb_{j,S}\_yb_{f,S}$ серед усіх рядків $x1_{i,j}, s\_y1_{i,f}, s$, дотримуючись принципу вибору найвіддаленішої точки: сума квадратів вхідних компонентів початкового базового рядка $x1_{i,j}, s$ має бути найбільшою серед усіх рядків).

9. Обчислити значення головних компонент: $K1_{i,S} = \sum_{j=1}^{n} \left(x1_{i,j,S} \times xb_{j,S} \right) / \sum_{j=1}^{n} \left(xb_{j,S} \right)^2$.

10. Обчислити елементи базових рядків гіперплощини по входах $b_{j,S} = \sum_{i=1}^{N} \left(x1_{i,j,S} \times K1_{i,S} \right) / \sum_{i=1}^{N} \left(K1_{i,S} \right)^2$.

11. Обчислити елементи базових рядків гіперплощини по виходах $b_{f,S} = \sum_{i=1}^{N} \left(y1_{i,f,S} \times K1_{i,S} \right) / \sum_{i=1}^{N} \left(K1_{i,S} \right)^2$.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

12. Модифікувати елементи кожного з N рядків $x1_{i,j,S+1} = x1_{i,j,S} - K1_{i,S} \times b_{j,s}$; $y1_{i,f,S+1} = y1_{i,f,S} - K1_{i,S} \times b_{f,s}$.

14. Зберегти результати навчання (отримані значення $X_j^{\max}, Y_f^{\max}, m, x_j^c, xb_{j,S}, b_{j,S}, b_{f,S}$).

Етап застосування мережі

1. Виконати нормування всіх векторів тестової множини, кількість яких дорівнює $N1$, використовуючи значення $X_j^{\max}, Y_f^{\max}$, отримані при навчанні на даних навчальної множини:

$$x_{k,j}^t = X_{k,j}^t / X_j^{\max},\ y_{k,f}^t = Y_{k,f}^t / Y_f^{\max}.$$

2. Центрувати елементи $x1_{k,j,1}^t = x_{k,j,1}^t - x_j^c$.

3. Задати $S = 1$.

4. В циклі для $k = \overline{1, N1}$, $S = \overline{1, m}$ виконати обчислення $K1_{k,S}^t = \sum_{j=1}^{n} \left(x1_{k,j,S}^t \times xb_{j,S}\right) / \sum_{j=1}^{n} \left(xb_{j,S}\right)^2$, $x1_{k,j,S+1}^t = x1_{k,j,S}^t - K1_{k,S}^t \times b_{j,s}$, запам'ятати масив $K1_{k,S}^t$.

5. Задати $y1_{k,f,S}^t = 0$.

6. Обчислити в циклі $y1_{k,f,S+1}^t = y1_{k,f,S}^t + K1_{k,s}^t \times b_{f,s}$, для $f = \overline{1, F}$, збільшуючи значення S.

7. Отримати нормовані передбачені значення, децентруючи: $y_{k,f}^t = y1_{k,f}^t + y_f^c$.

8. Денормувати передбачені значення: $Y_{k,f}^t = y_{k,f}^t \times Y_f^{\max}$.

Застосування методу симетричного шифрування на прикладі растрових зображень

Мережа шифрування на прикладі даних-растрових зображень діє так:

1) Етап навчання.

Сформувати навчальну множину, якої містять дані про повне *початкове* зображення, або його окремий фрейм, розміром N пікселів. Кількість стовпців-входів тоді становить N-1, стовпців-виходів – 1. *Входи* – рівномірно розподілені випадкові числа із певного діапазону (або задані в інший спосіб елементи ключа *Key1*), *вихід* – значення інтенсивності для відповідного пікселя початкового зображення. Навчити лінійну мережу МГП із кількістю прихованих нейронів, що дорівнює кількості входів, за алгоритмом описаним вище.

2) Етап застосування.

Сформувати тестову множину, яка є ідентичною за розміром до навчальної. *Входи* – інші рівномірно розподілені випадкові числа із діапазону для навчальної множини (або задані в інший спосіб елементи ключа *Key2*), *вихід* – значення інтенсивності для відповідного пікселя початкового зображення (ті що і на етапі навчання). Застосувати навчену лінійну мережу МГП, отримуючи набір з N вихідних значень, які утворюють *зашифроване* зображення. Набір з 2 х N х (N-1) значень на входах навчальної та тестової множини складає дві частини ключа (*Key1* та *Key2*) для наступного дешифрування.

Мережа дешифрування навчається та застосовується так:

1) Етап навчання.

Як і для мережі шифрування сформувати навчальну множину, яка містить дані про повне *зашифроване* зображення, або його окремий фрейм, розміром N пікселів. Кількість стовпців-входів сстановить N-1, стовпців-виходів – 1. *Входи* – значення попередньо збережених елементів ключа *Key2*, *вихід* – значення інтенсивності для відповідного елемента зашифрованого зображення. Навчити лінійну мережу МГП із кількістю прихованих нейронів, рівній кількості входів.

2) Етап застосування.

Сформувати тестову множину, яка є ідентичною за розміром до навчальної. *Входи* – значення попередньо збережених випадкових чисел з ключа *Key1*. Застосувати навчену лінійну мережу МГП, отримуючи набір з N вихідних значень, які утворюють *дешифроване* зображення.

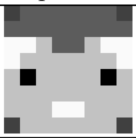
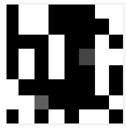
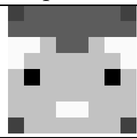
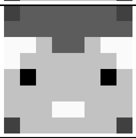
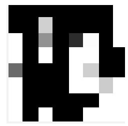
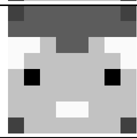
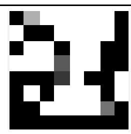
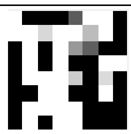
Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Результати застосування розробленого методу

У табл. 1 подано вхідні дані та результати шифрування на тестових півтонових зображеннях "Boy" та "Cat" розміром 8x8 пікселів. Як ключі обрано тестові півтонові зображення "Lena" та "Baboon" розміром 64x63 пікселів. Результати експериментів підтверджують коректність запропонованого методу та відсутність корельованості між вхідними і зашифрованими даними.

Таблиця 1

Вхідні дані та результати експериментів

Вхідне зображення	Ключ *Key1*	Ключ *Key2*	Зашифроване зображення	Дешифроване зображення
				
				
				
				

Висновки

Запропоновано метод симетричного шифрування даних на основі нейронних мереж моделі геометричних перетворень. Унаслідок використання властивості мереж МГП формувати гіперплощину, що проходить через точки навчальної множини з нульовою залишковою дисперсією, забезпечується відсутність похибки відтворення даних на виході мережі після дешифрування. Проведені експерименти показали можливості застосування розробленого методу для шифрування растрових зображень.

1. Shihab K. A backpropagation neural network for computer network security // Journal of Computer Science, Vol. 2, No. 9, 2006, pp. 710–715. 2. Volna E., Kotyrba M., Kocian V., Janosek M. Cryptography Based On Neural Network // Proceedings of the 26th European Conference on Modelling and Simulation, 2012, pp. 386–391. 3. Arvandi M., Wu S., Sadeghian A., Melek W.W., Woungang I. Symmetric cipher design using recurrent neural networks // Proceedings of the IEEE International Joint Conference on Neural Networks, 2006, pp. 2039–2046. 4. Chan C.K., Chan C.K., Lee L.P. Cheng L.M. Encryption system based on neural network // Communications and Multimedia Security Issues of the New Century, Springer, 2001, pp. 117–122. 5. Sagar V., Kumar K. 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, 2014, p. 51. 6. Zhou K., Kang Y., Huang Y., Feng E. Encrypting Algorithm Based on RBF Neural Network // Proceedings of the IEEE Third International Conference on Natural Computation, Vol. 1, 2007, pp. 765–768. 7. Tkachenko R., Tkachenko P., Izonin I., Tsymbal Y. Learning-based image scaling using neural-like structure of geometric transformation paradigm // Advances in Soft Computing and Machine Learning in Image Processing, Springer, 2018, pp. 537–565.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua