DOI 10.31891/2307-5732-2025-347-9
УДК 004: 089

БУРЦЬО АНДРІЙ
Національний Університет "Львівська Політехніка"
https://orcid.org/0009-0006-1928-5554
email: andrii.y.burtso@edu.lpnu.ua
МАРІКУЦА УЛЯНА
Національний Університет "Львівська Політехніка"
https://orcid.org/0000-0002-9514-7413
email: Uliana.B.Marikutsa@lpnu.ua

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ У КРИПТОАНАЛІЗІ: СУЧАСНІ ПІДХОДИ ТА ПЕРСПЕКТИВИ

Метою цієї публікації є проведення аналізу сучасних підходів до використання нейронних мереж у криптоаналізі, визначення актуальних шляхів дослідження та перспектив розвитку цієї галузі. У статті розглядаються сучасні методи криптоаналітичних атак, заснованих на нейронних мережах, включаючи хаотичні нейронні мережі для дешифрування, машинне навчання для виявлення криптографічних вразливостей та використання штучних нейронних мереж для зламу складних шифрувальних систем. Результати досліджень вказують на те, що нейронні мережі можуть суттєво підвищити ефективність криптоаналізу, зокрема в аспектах розпізнавання патернів і точності дешифрування. Однак, перед галуззю стоять виклики, зокрема в масштабованості підходів до більш складних криптографічних систем.

Ключові слова: нейронні мережі, криптоаналіз, криптографія, машинне навчання, хаотичні системи, дешифрування.

BURTSO ANDRII, MARIKUTSA ULIANA
Lviv Polytechnic National University

APPLICATION OF NEURAL NETWORKS IN CRYPTANALYSIS: MODERN APPROACHES AND PROSPECTS

In today's world, the proliferation of digital technologies has revolutionized numerous aspects of modern life, fundamentally reshaping how individuals, organizations, and societies interact and function. However, alongside the numerous benefits brought by this digital transformation, a growing threat has emerged—cybersecurity breaches. As the digital landscape expands and evolves, so do the tactics and capabilities of malicious actors seeking to exploit vulnerabilities for criminal purposes. Consequently, protecting digital assets and infrastructure from cyber threats has become a necessity for individuals, businesses, and governments alike. Addressing the multifaceted challenges posed by cyber threats requires innovative and adaptive approaches that can keep pace with the dynamic nature of digital risks. In this context, artificial intelligence (AI) has emerged as a pivotal technology, offering unprecedented capabilities to enhance cybersecurity defenses. AI encompasses a range of advanced methods and algorithms enabling machines to simulate human intelligence, including learning from data, making predictions, and adapting to new information. The application of AI in cybersecurity holds the promise of significantly improving threat detection, strengthening defenses, and mitigating risks in the digital domain. This article aims to explore the critical role of AI in cybersecurity by examining its applications across various areas, such as threat detection, vulnerability assessment, incident response, and predictive analysis. Leveraging machine learning algorithms and advanced data analytics, AI-driven solutions can analyze vast amounts of data in real time, identifying anomalous patterns indicative of potential security breaches. Furthermore, AI enables organizations to implement proactive defense mechanisms, allowing them to anticipate and mitigate emerging threats before they fully manifest. However, integrating AI into cybersecurity frameworks is not without challenges and complexities. Ethical considerations, privacy concerns, and potential algorithmic biases require a nuanced approach to implementing AI-driven cybersecurity solutions. Thus, this article seeks to critically evaluate the advantages, limitations, and ethical implications of AI in cybersecurity, emphasizing the need to balance innovation with ethical responsibility. At its core, the rise of AI represents a paradigm shift in cybersecurity, offering unprecedented opportunities to strengthen defenses and combat cyber threats in the digital age. Through a comprehensive analysis of AI's role in cybersecurity, this article seeks to elucidate the transformative potential of AI-based technologies in safeguarding digital assets and preserving the integrity of cyberspace.

Keywords: neural networks, cryptanalysis, cryptography, machine learning, chaotic systems, decryption.

Постановка проблеми

Сучасні криптографічні системи стають дедалі складнішими, що значно ускладнює їхній аналіз за допомогою традиційних методів криптоаналізу. Багато алгоритмів, зокрема ті, що використовують нелінійні та хаотичні системи, мають високу стійкість до методів повного перебору, що вимагає значних обчислювальних ресурсів і часу для їхнього зламу. Водночас нейронні мережі пропонують можливість автоматизації процесу криптоаналізу, використовуючи потужності машинного навчання для виявлення прихованих патернів у зашифрованих даних. Це дає змогу не лише скоротити час, необхідний для зламу криптографічних ключів, але й підвищити ефективність процесу дешифрування.

Застосування нейронних мереж для криптоаналізу вимагає розробки нових підходів, здатних вирішувати проблему масштабованості та ефективності при роботі зі складними криптографічними алгоритмами. У той час, як традиційні методи стають менш ефективними у сучасних умовах, штучні нейронні мережі мають великий потенціал для підвищення точності криптоаналітичних атак.

Огляд літератури

У попередніх дослідженнях нейронні мережі були розглянуті як перспективний інструмент для криптоаналізу. У роботі "Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate

array" дослідники акцентують увагу на тому, як нейронні мережі можуть використовуватися для дешифрування зображень, зашифрованих хаотичними системами. Важливим аспектом є використання програмованих вентильних матриць (FPGA), які дозволяють нейронним мережам працювати в реальному часі, дешифруючи складні криптографічні системи з високою точністю.

Дослідження, представлене в "A novel image encryption/decryption scheme based on chaotic neural networks", описує застосування хаотичних нейронних мереж для дешифрування, яке показує високу ефективність у зламі шифрованих зображень. Завдяки здатності нейронних мереж розпізнавати складні патерни, вони можуть експлуатувати навіть незначні неточності або слабкі місця в хаотичних системах шифрування.

У дослідженні "Applications of Artificial Intelligence to Cryptography" підкреслюється, як нейронні мережі можуть бути поєднані з традиційними методами криптоаналізу для покращення точності дешифрування. Зокрема, нейронні мережі добре підходять для апроксимації складних математичних функцій, які використовуються в криптографії, що дозволяє швидше ідентифікувати криптографічні ключі або виявляти вразливості в алгоритмах шифрування.

Методологія

Основним підходом у криптоаналізі, заснованому на нейронних мережах, є використання контрольованого навчання. Це передбачає навчання нейронної мережі на відомих парах зашифрованих і розшифрованих даних, що дозволяє їй зрозуміти механізм шифрування. Після навчання мережа може застосовувати ці знання до невідомих зашифрованих даних, намагаючись передбачити відповідний відкритий текст або криптографічний ключ.

У дослідженні "A novel image encryption/decryption scheme based on chaotic neural networks" нейронна мережа використовувалася для навчання на хаотичних патернах шифрування, що дозволило моделі зворотно дешифрувати зашифровані дані. Це дозволяє швидко та ефективно розшифровувати інформацію навіть у випадках, коли використовуються складні хаотичні алгоритми шифрування. Використання програмованих вентильних матриць (FPGA), як зазначено в "Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate array", дозволяє здійснювати обчислення в реальному часі, що робить методологію ефективною при великих обсягах зашифрованих даних.

Інтеграція алгоритмів машинного навчання, як зазначено в "The Benefits of Artificial Intelligence in Cybersecurity", також є ключовим елементом у сучасних підходах до криптоаналізу. Машинне навчання допомагає нейронним мережам швидше ідентифікувати слабкі місця в алгоритмах шифрування, дозволяючи фокусувати ресурси на найбільш вразливих ділянках.

Результати

Використання нейронних мереж у криптоаналізі призвело до кількох важливих результатів:

- Підвищення швидкості дешифрування: Як показано в "A novel image encryption/decryption scheme based on chaotic neural networks", нейронні мережі значно скоротили час дешифрування, демонструючи високу точність при розшифруванні зображень, зашифрованих хаотичними системами. Це свідчить про те, що нейронні мережі можуть бути ефективними для інших типів даних.
- Адаптивність: Нейронні мережі продемонстрували здатність адаптуватися до різних криптографічних схем. У "Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate array" мережа успішно дешифрувала зображення, зашифровані за допомогою хаотичних систем, що підкреслює універсальність цього підходу.
- Підвищена точність: Поєднання нейронних мереж із алгоритмами машинного навчання призвело до підвищення точності криптоаналітичних атак. У "Applications of Artificial Intelligence to Cryptography" зазначається, що мережі здатні виявляти приховані патерни в криптографічних ключах, що недоступно для традиційних методів.

Обговорення

Попри значні досягнення, криптоаналіз на основі нейронних мереж стикається з кількома викликами. По-перше, для ефективного навчання нейронні мережі потребують великих обсягів даних, що не завжди доступно в криптографічних додатках. По-друге, хоча нейронні мережі добре працюють із виявленням патернів, вони можуть мати труднощі з більш складними шифрувальними системами, які використовують нелінійні перетворення або квантово-стійкі алгоритми.

Ще однією важливою проблемою є безпека самої нейронної мережі. Якщо мережа або її навчальний процес буде скомпрометовано, це може призвести до провалу криптоаналітичної атаки. У "The Benefits of Artificial Intelligence in Cybersecurity" підкреслюється необхідність розробки більш захищених архітектур нейронних мереж для їхнього використання в криптоаналізі.

Майбутні дослідження мають зосереджуватися на розширенні масштабів нейронних мереж для більш складних криптографічних систем, а також на інтеграції нейронних мереж із іншими методами криптоаналізу, зокрема квантовими обчисленнями.

Висновок

У цій публікації було проведено аналіз сучасних підходів до застосування нейронних мереж у криптоаналізі. Ми виявили, що нейронні мережі здатні значно підвищити ефективність дешифрування

завдяки швидшому розпізнаванню патернів та вищій точності атак на криптографічні системи. Незважаючи на це, існують суттєві виклики, пов'язані з масштабуванням нейронних мереж для складних криптографічних схем і забезпеченням їхньої безпеки.

Досягнення цієї роботи полягає в тому, що було визначено актуальні шляхи для подальших досліджень, зокрема у напрямку підвищення масштабованості нейронних мереж та їх інтеграції з квантовим криптоаналізом. Майбутні дослідження також мають зосереджуватися на розробці захищених архітектур для запобігання компрометації нейронних мереж у процесі криптоаналізу.

Література

1. Al-Musawi, W. A., Al-Ibadi, M. A. A., & Wali, W. A. (2023). Artificial intelligence techniques for encrypting images based on the chaotic system implemented on field-programmable gate array at the University of Basrah. *International Journal of Artificial Intelligence, 12*(1), 347–356. https://doi.org/10.11591/ijai.v12.i1.pp347-356
2. Bigdeli, N., Farid, Y., & Afshar, K. (2012). A novel image encryption/decryption scheme based on chaotic neural networks. *Engineering Applications of Artificial Intelligence, 25*(6), 753–765. https://doi.org/10.1016/j.engappai.2012.01.011
3. Blackledge, J., & Mosola, N. (2020). Applications of artificial intelligence to cryptography. *Transactions on Engineering and Computing Sciences, 8*(3), 21–60. https://doi.org/10.14738/tmlai.83.8219
4. Calderon, R. Continuous Steckel Mill Improvements. *La Salle University*. Retrieved from https://digitalcommons.lasalle.edu/cgi/viewcontent.cgi?article=1035&context=ecf_capstones
5. Botmart, T., & Niamsup, P. (2007). Adaptive control and synchronization of the perturbed Chua's system. *Mathematics and Computers in Simulation, 75*(1–2), 37–55. https://doi.org/10.1016/j.matcom.2006.07.003
6. Bennett, C. H., Bernstein, E., Brassard, G., & Vazirani, U. (1997). The strengths and weaknesses of quantum computation. *SIAM Journal on Computing, 26*(5), 1510–1523.
7. Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals, 21*, 749–761. https://doi.org/10.1016/j.chaos.2003.12.022
8. Chan, C., & Cheng, L. (2001). The convergence properties of a clipped Hopfield network and its application in the design of key-stream generator. *IEEE Transactions on Neural Networks, 12*(2), 340–348.
9. Ferguson, N., & Schneier, B. (2003). *Practical Cryptography.* John Wiley & Sons.
10. Hongjun, L., & Xingyuan, W. (2010). Color image encryption based on one-time keys and robust chaotic maps. *Computers & Mathematics with Applications, 59*, 3320–3327.
11. Joshi, M., Shakher, C., & Singh, K. (2009). Logarithms-based RGB image encryption in the fractional Fourier domain: A non-linear approach. *Optics and Lasers in Engineering, 47*(6), 721–727.
12. Karras, D. A., & Zorkadis, V. (2003). On neural network techniques in the secure management of communication systems through improving and quality assessing pseudorandom stream generators. *Neural Networks, 16*(5–6), 899–905.
13. Lian, S. (2009). A block cipher based on chaotic neural networks. *Neurocomputing, 72*, 1296–1301.
14. Lian, S. G., Chen, G. R., Cheung, A., & Wang, Z. Q. (2004). A chaotic-neural-network-based encryption algorithm for JPEG2000 encoded images. *Proceedings of the IEEE Symposium on Neural Networks (ISNN 2004), Lecture Notes in Computer Science, 3174*, 627–632.
15. Pourasad, Y., Ranjbarzadeh, R., & Mardani, A. (n.d.). A new algorithm for digital image encryption based on chaos theory. *Entropy*.
16. Copeland, B. J. (2020). Artificial intelligence. *Encyclopedia Britannica.*
17. Turing, A. M. (1950). Computing machinery and intelligence. *Mind, 49*, 433–460.
18. Wikibooks. (2020). Artificial Neural Networks/Neural Network Basics. Retrieved from https://en.wikibooks.org/wiki/Artificial_Neural_Networks/Neural_Network_Basics
19. Kostadinov, S. (2019). Understanding the Back-Propagation Algorithm. *Towards Data Science*. Retrieved from https://towardsdatascience.com
20. Blackledge, J. M., Bezobrasov, S., Tobin, P., & Zamora, F. (2013). Cryptography using evolutionary computing. *Proceedings of the IET ISSC2013, Letterkenny, Ireland, June 20–21*.
21. Stamp, M. (2018). *Introduction to Machine Learning with Applications in Information Security.* Chapman & Hall/CRC. ISBN: 978-1138626782
22. Kovalchuk, A., & Lotoshynska, N. (2018). Elements of RSA algorithm and extra noising in binary linear-quadratic transformations during encryption and decryption of images. *Proceedings of the 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*, 542–544.
23. Zhang, L., & Chen, J. (2018). U.S. Patent No. 9,992,669. *U.S. Patent and Trademark Office.*
24. Xu, S., Yang, G., & Mu, Y. (2019). Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. *Information Sciences, 479*, 116–134.
25. Zhang, Y., & Tang, Y. (2018). A plaintext-related image encryption algorithm based on chaos. *Multimedia Tools and Applications, 77*(6), 6647–6669.

26. Sun, C., Su, S., Gao, Z., Liu, H., Wu, H., Shen, X., & Bi, W. (2019). Stimuli-responsive inks based on perovskite quantum dots for advanced full-color information encryption and decryption. *ACS Applied Materials & Interfaces, 11*(8), 8210–8216.

27. Irviani, R., & Muslihudin, M. (2018). Nur algorithm on data encryption and decryption. *International Journal of Engineering & Technology, 7*(2.26), 109–118.

References

1. Al-Ibadi M. Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate array at University of Basrah / Wisal Adnan Al-Musawi, Mohammed Abd Ali Al-Ibadi, Wasan A. Wali – DOI:10.11591/ijai.v12.i1.pp347-356

2. Otavio L. A novel image encryption/decryption scheme based on chaotic neural networks/ Nooshin Bigdeli, Yousef Farid, Karim Afshar // N. Bigdeli et al. / Engineering Applications of Artificial Intelligence 25 (2012) 753–765 – https://www.sciencedirect.com/science/article/abs/pii/S0952197612000115?via%3Dihub.

3. Blackledge, J. ., & Mosola, N. . (2020). Applications of Artificial Intelligence to Cryptography. Transactions on Engineering and Computing Sciences, 8(3), 21–60. https://doi.org/10.14738/tmlai.83.8219.

4. Ricardo Calderon Continuous Steckel Mill Improvements at La Salle University– : https://digitalcommons.lasalle.edu/cgi/viewcontent.cgi?article=1035&context=ecf_capstones.

5. Botmart, T., & Niamsup, P. (2007). Adaptive control and synchronization of the perturbed Chua's system. *Math. Comput. Simulation*, 75(1–2), 37–55.

6. Bennett, C.H., Bernstein, E., Brassard, G., & Vazirani, U. (1997). The strengths and weaknesses of quantum computation. *SIAM J. Comput.*, 26(5), 1510–1523.

7. Chen, G., Mao, Y., & Chui, C.K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals*, 21, 749–761.

8. Chan, C., & Cheng, L. (2001). The convergence properties of a clipped Hopfield network and its application in the design of key-stream generator. *IEEE Trans. Neural Networks*, 12(2), 340–348.

9. Ferguson, N., & Schneier, B. (2003). *Practical Cryptography*. John Wiley and Sons.

10. Hongjun, L., & Xingyuan, W. (2010). Color image encryption based on one-time keys and robust chaotic maps. *Comput. Math. Appl.*, 59, 3320–3327.

11. Joshi, M., Shakher, C., & Singh, K. (2009). Logarithms-based RGB image encryption in the fractional Fourier domain: a non-linear approach. *Opt. Lasers Eng.*, 47(6), 721–727.

12. Karras, D.A., & Zorkadis, V. (2003). On neural network techniques in the secure management of communication systems through improving and quality assessing pseudorandom stream generators. *Neural Networks*, 16(5–6), 899–905.

13. Lian, S. (2009). A block cipher based on chaotic neural networks. *Neurocomputing*, 72, 1296–1301.

14. Lain, S.G., Chen, G.R., Cheung, A., & Wang, Z.Q. (2004). A chaotic-Neural-Network-based encryption algorithm for JPEG2000 encoded images. In *Proceedings of the 2004 IEEE Symposium on Neural Networks (ISNN2004)*, Dalian, China, Lecture Notes in Computer Science, Springer, Berlin, 3174, pp. 627–632.

15. Y. Pourasad, R. Ranjbarzadeh, & A. Mardani. (Year not specified). A new algorithm for digital image encryption based on chaos theory. *Entropy*.

16. Various simulation tests and FPGA hardware co-simulation tests were also cited, but detailed reference information is not provided.

17. Copeland, B. J. (2020). *Artificial intelligence*. Encyclopedia Britannica.

18. Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind*, 49, 433–460.

19. Wikibooks. (2020). *Artificial Neural Networks/Neural Network Basics*. - https://en.wikibooks.org/wiki/Artificial_Neural_Networks/Neural_Network_Basics.

20. Kostadinov, S. (2019). Understanding the Back-Propagation Algorithm. *Towards Data Science*. - https://towardsdatascience.com.

21. Blackledge, J. M., Bezobrasov, S., Tobin, P., & Zamora, F. (2013). Cryptography using Evolutionary Computing. *Proc. IET ISSC2013*, Letterkenny, Co Donegal, Ireland, June 20-21.

22. Stamp, M. (2018). *Introduction to Machine Learning with Applications in Information Security*. Chapman & Hall/CRC Machine Learning & Pattern Recognition. ISBN-13: 978-1138626782.

23. Kovalchuk, A., & Lotoshynska, N. (2018). Elements of RSA algorithm and extra noising in binary linear-quadratic transformations during encryption and decryption of images. In *2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*, pp. 542-544. IEEE.

24. Zhang, L., & Chen, J. (2018). U.S. Patent No. 9,992,669. Washington, DC: U.S. Patent and Trademark Office.

25. Xu, S., Yang, G., & Mu, Y. (2019). Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. *Information Sciences*, 479, 116-134.

26. Zhang, Y., & Tang, Y. (2018). A plaintext-related image encryption algorithm based on chaos. *Multimedia Tools and Applications*, 77(6), 6647-6669.

27. Sun, C., Su, S., Gao, Z., Liu, H., Wu, H., Shen, X., & Bi, W. (2019). Stimuli-responsive inks based on perovskite quantum dots for advanced full-color information encryption and decryption. *ACS Applied Materials & Interfaces*, 11(8), 8210-8216.

28. Irviani, R., & Muslihudin, M. (2018). Nur algorithm on data encryption and decryption. *International Journal of Engineering & Technology*, 7(2.26), 109-118