Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп’ютерних наук

Дипломна робота
магістра

з теми: «ДОСЛІДЖЕННЯ ПЕРСПЕКТИВНИХ ПІДХОДІВ ДО КОДУВАННЯ МУЛЬТИМЕДІЙНИХ ДАНИХ»

Виконав: студент групи KN1-M22
спеціальності 122 Комп’ютерні науки
Коваль Олексій Олександрович

Керівник: **Смалько Олена Аркадіївна,**
доцент кафедри комп’ютерних наук,
кандидат педагогічних наук, доцент.

Рецензент: **Шелепало Галина Василівна,**
доцент кафедри захисту інформації Вінницького національного технічного університету,
кандидат фізико-математичних наук, доцент

Кам’янець-Подільський – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КА – клітинний автомати (cellular automata).

КЛХК – кусково–лінійна хаотична карта.

ЛПКА – лінійна пам’ять клітинних автоматів (LMCA – linear memory cellular automata).

ТХ – теорія хаосу (theory of chaos).

ХС – хаотична система.

ВСТУП

Експоненціальне зростання мультимедійних даних за останні роки породило потребу в більш ефективних і безпечних способах кодування та обробки цих даних. Обсяг цифрового мультимедійного контенту станом на тепер продовжує динамічно зростати, збільшуються також проблеми стосовно забезпечення надійного зберігання величезної кількості інформації, ефективного її опрацювання та безпечного передавання мережами. Для вирішення цих проблем, зокрема, розробляються нові підходи до кодування мультимедійних даних. При цьому досить перспективними напрямками досліджень є використання клітинних автоматів і динамічних систем з хаотичною поведінкою. Дана кваліфікаційна робота присвячена дослідженню саме таких підходів.

Об'єктом дослідження є кодування мультимедійних даних.

Предметом дослідження є застосування клітинних автоматів та хаотичних систем для шифрування даних.

Метою кваліфікаційної роботи є дослідження, ґрунтовний аналіз та практична реалізація двох перспективних у наш час підходів до кодування мультимедійних даних, зокрема з використанням клітинних автоматів та динамічних систем, що демонструють хаотичну динаміку.

Завдання дослідження:

1) аналіз сучасної термінології та концепцій сфери шифрування даних;
2) дослідження перспективних методів та підходів до кодування мультимедійних даних, що спираються на використання динамічних хаотичних систем теорії хаосу та клітинних автоматів;
3) опис деяких підходів до шифрування цифрових даних за допомогою динамічних та хаотичних систем, клітинних автоматів і фрактальних функцій, які вбачаються найбільш релевантними;
4) оцінювання ефективності алгоритмів, що реалізовують описані підходи, та їх порівняльний аналіз за кількома ознаками;

5) виконання прикладного завдання по реалізації мовою Python алгоритму шифрування графічних даних з використанням системи нелінійних диференціальних рівнянь Росслера, кривої Гільберта та H-фракталу.

Впродовж виконання кваліфікаційної роботи використовувались наступні методи дослідження: аналіз літератури, тематичні дослідження, логіко-аналітичні та експериментальні дослідження, формалізація, моделювання, візуальні методи, аргументація та порівняння отриманих результатів.

Дана робота має теоретичне та практичне значення, зокрема одержані внаслідок її виконання результати дають змогу покращити свої знання у сфері криптографії. Зокрема надають глибоку та ґрунтовну інформацію, щодо використання хаотичних систем та клітинних автоматів для шифрування мультимедійних даних. Проведений аналіз та порівняння дозволяє наочно оцінити, використовувані методи та доцільність їх використання. Написаний код доцільно використовувати при вирішенні прикладних задач з шифрування.

Деякі отримані результати вдалося апробувати у вигляді статті *Метод використання динамічних перетворень для стиснення, захисту та приховування відеоінформаційних ресурсів в інфокомунікаційних системах. Сучасна спеціальна техніка* [1] (видання категорії **Б**), статті опублікованої на платформі IEEE – *Research of prospective encoding methods for multimedia content. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)* (видання категорії **А**) [29], тез – *Дослідження перспективних підходів до кодування мультимедійних даних* у збірнику матеріалів наукової конференції здобувачів вищої освіти фізико-математичного факультету Кам’янець-Подільського національного університету імені Івана Огієнка [2].

Робота складається із робота складається із переліку умовних позначень, вступу, трьох розділів, висновків до розділів 1 та 2, загальних висновків, списку використаних джерел та додатку. У вступі описано актуальність теми, об’єкт, предмет, мета та завдання дослідження. У першому розділі подано аналіз сучасної

термінології та концепцій сфери шифрування даних. Другий розділ присвячений конкретним прикладам алгоритмів шифрування за допомогою клітинних автоматів та хаотичних систем. У третьому розділі ми розглянули власне алгоритми шифрування, прикладів, що були описані у розділі 2, детально проаналізували їх та провели порівняльний аналіз алгоритмів з хаотичною системою та клітинними автоматами. У висновках для розділів 1 та 2, підбито підсумки за кожним розділом. У загального висновку підведено підсумки, щодо досягнутої мети, виконаних завдань, практичного та теоретичного значень даного дослідження. У списку використаних джерел, зібрано інформацію, статті, публікації, журнали, що використовувались під час виконання роботи та публікації, за якими апробувалась робота. У додатку поданий програмний код на мові Python алгоритму шифрування на основі хаотичної системи Росслера та рисунок із результатом роботи алгоритму.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було досягнено поставленої мети і виконані всі завдання.

Першим етапом під час написання роботи став аналіз сучасної термінології та концепцій сфери шифрування даних аналіз понять, що є необхідними для розуміння теми. Було описано, як вже доволі старі методи та підходи до шифрування даних, наприклад стенографія, асиметричне та симетричне шифрування, блочне шифрування. Так і перспективні, це такі методи як: квантова криптографія, використання хеш-функцій, застосування КА та ХС, що використовуються, як сучасні підходи в криптографії для підвищення безпеки даних і шифрування, пропонують унікальні перспективи та методи генерації безпечних криптографічних ключів і розробки алгоритмів шифрування.

Останні два привернули змогли привернути нашу увагу та стали темою наступних розділів. Були обрані саме вони, оскільки ХС і КА, які відомі своєю високою складністю і непередбачуваністю, що може зробити криптографічні методи, засновані на них, дуже стійкими до атак інженерного методу та атак грубою силою. А відсутність статистичних закономірностей, є дуже важливою якістю, оскільки такі закономірності можуть використовуватися для криптоаналізу. ХС та КА дають змогу створювати криптосистеми, в яких важко передбачити або визначити розподіл даних, що робить їх ефективними для захисту інформації. Можливість паралельної обробки клітинними автоматами дозволяють розглядати багато поточні обчислення, що може бути корисним для ефективної роботи великих обчислювальних систем.

Дослідивши основи кодування, шифрування, знаючи необхідні поняття та терміни, певні традиційні та новітні підходи та методи в криптографії стало зрозуміло, що особливого розгляду варта саме криптографія за використання саме хаотичних систем та клітинних автоматів.

У 2 розділі було досліджено й описано перспективні підходи до шифрування мультимедійних даних, що спираються на використання математичних структур ТХ та окремих КА. Було детально описано конкретні

алгоритми шифрування за допомогою КА із застосуванням блочного шифрування та двостороніх правил. ХС із фрактальними та іншими математичними функціями, що хоч і роблять алгоритм обчислювально важким, але забезпечують належний рівень захисту.

Також в рамках використання даних алгоритмів, було згадано про можливість шифрування відео. Оскільки цифрове відео, як відомо, містить послідовність ортогональних растрових цифрових зображень (кадрів), що відображаються з постійною швидкістю.

В розділі 3 було описано власне схеми алгоритмів шифрування та необхідних для цього кроків. Наступним кроком став їх аналіз. Спочатку загальний, КА та ХС окремо, під час якого було визначено, що кожний з підходів, як КА так і ХС має свої недоліки та переваги. А згодом і порівняльний аналіз представлених алгоритмів.

В результаті такого аналізу було визначено, що наведений алгоритм за використанням КА є кращим, ніж представлений алгоритм з ХС, хоч і не набагато. Оскільки різниця не значна, можна зробити висновок, що кожен з алгоритмів та підходів вартий уваги, й може знайти собі прикладне використання при правильно підібраних для нього задачах та наявних ресурсів.

В кінці була реалізовано практичну задачу із написання алгоритму шифрування за допомогою ХС на мові Python, що дає змогу для його застосування на практиці.

Дана робота надає детальний аналіз та пропонує можливості використання перспективних методів шифрування, що досі досліджуються та мають на меті покращити стан безпеки персональних даних. Викладений матеріал буде цікавий для усіх науковців, що працюють в сфері безпеки даних, а саме криптографії. Проте особливо корисною праця буде для молодих науковців, що лише починають своє знайомство з криптографією, оскільки вона дає необхідні теоретичні знання в сферах ХС та КА, а також практичну реалізацію одного з алгоритму шифрування, що дає змогу для випробування одного з представлених алгоритмів, його можливої зміни та простору для експериментів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безрук В. М., Смалько О. А., Коваль О. О., Макаренко М. В. Метод використання динамічних перетворень для стиснення, захисту та приховування відеоінформаційних ресурсів в інфокомунікаційних системах. Сучасна спеціальна техніка. 2023. № 3.
2. Коваль О. Дослідження перспективних підходів до кодування мультимедійних даних. Збірник матеріалів наукової конференції здобувачів вищої освіти фізико-математичного факультету Кам'янець-Подільського національного університету імені Івана Огієнка. 1 листопада 2023 року. Кам'янець-Подільський: Кам'янець=Подільський національний університет імені Івана Огієнка, 2023. С.36. URL: http://elar.kpnu.edu.ua/xmlui/handle/123456789/7648
3. Математичні методи криптології навчальний посібник / А. Кожухівський та ін. Київ, 2021, 244 с.
4. Основи криптографії. навчальний посібник. Чернівці, 2008, 188 с.
5. Швець О. Детермінований хаос. Київ, 2010, 93 с
6. A chaos-based image encryption technique utilizing hilbert curves and h-fractals / X. Zhang et al. IEEE access. 2019. Vol. 7. P. 74734–74746. URL: https://doi.org/10.1109/access
7. AES 256 hardware encryption - safe and secure encryption. ZyberSafe. URL: https://zybersafe.com/aes256hardwareencryption/
8. Al-Musawi W. A., Wali W. A., Ali Al-Ibadi M. A. Field-programmable gate array design of image encryption and decryption using Chua's chaotic masking. International journal of electrical and computer engineering (IJECE). 2022. Vol. 12, no. 3. P. 2414. URL: https://doi.org/10.11591/ijece.v12i3.pp2414-2424
9. A.Mokhtar et al. Gliwice. A new chaos advanced encryption standard (AES) algorithm for data security, 2010.
10. Arabnezhad H., Babak S. An Evaluation and Enhancement of Seredynski-Bouvry CA-based Encryption Scheme, 2021.

11. Carmen P.-L., Ricardo L.-R. Notions of chaotic cryptography: sketch of a chaos based cryptosystem. Applied cryptography and network security. 2012. URL: https://doi.org/10.5772/36419
12. Chaos theory and the logistic map. Geoff Boeing. URL: https://geoffboeing.com/2015/03/chaos-theory-logistic-map/
13. Corona-Bermúdez E., Chimal-Eguía J. C., Téllez-Castillo G. Cryptographic services based on elementary and chaotic cellular automata. Electronics. 2022. Vol. 11, no. 4. P. 613. URL: https://doi.org/10.3390/electronics11040613.
14. Dictionary.com. URL: https://www.dictionary.com/
15. Grzybowski J. M. V., Rafikov M., Balthazar J. M. Synchronization of the unified chaotic system and application in secure communication. Communications in nonlinear science and numerical simulation. 2009. Vol. 14, no. 6. P. 2793–2806. URL: https://doi.org/10.1016/j.cnsns.2008.09.028 (date of access: 24.11.2023).
16. Boguta, K,. Sensitivity To Peturbation in Elementary Cellular Automata, from the Wolfram Demonstrations Project, 2011. URL: http://demonstrations.wolfram.com/SensitivityToPeturbationInElementaryCellularAutomata/
17. Chand S., Aggarwal R., Dubey E. A review of image encryption using chaos based techniques. International journal of science and research, 2015.
18. Eslami Z., Kabirirad S. A block-based image encryption scheme using cellular automata with authentication capability. Third international conference of mathematical sciences (icms 2019), Istanbul, Turkey. 2019. URL: https://doi.org/10.1063/1.5136195
19. Falconer K. Fractal geometry: mathematical foundations and applications. Hoboken, NJ, USA: Wiley, 1990.
20. Legal Definitions Dictionary. URL: https://www.lawinsider.com/dictionary
21. Mankar V. H., Mishra M. Review on chaotic sequences based cryptography and cryptanalysis. International journal of electronics engineering, 2011. P. 189–194.

22. Mao Y., Chen G. Chaos-Based image encryption. Handbook of geometric computing. Berlin/Heidelberg. P. 231–265. URL: https://doi.org/10.1007/3-540-28247-5_8.
23. Mahieu, E,.Ikeda Attractor, from the Wolfram Demonstrations Project, 2011. http://demonstrations.wolfram.com/IkedaAttractor/
24. Ilachinski A. Cellular automata – A discrete universe. Kybernetes. 2003. Vol. 32, no. 4. URL: https://doi.org/10.1108/k.2003.06732dae.007
25. Kaur M., Kumar V. Efficient image encryption method based on improved Lorenz chaotic system. Electronics letters. 2018. Vol. 54, no. 9. P. 562–564. URL: https://doi.org/10.1049/el.2017.4426
26. Kocarev L., Lian S. Chaos-based cryptography: theory, algorithms and applications. Springer, 2011. 408 p.
27. Krapež A. An application of quasigroups in cryptology. Researchgate. 2010
28. Petroc T. Volume of data information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025.
29. Pylypiuk T., Smalko O., Koval O. Research of prospective encoding methods for multimedia content. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT). DOI: 10.1109/ATIT58178.2022.10024229
30. Robinson, C. (1995). Dynamical systems. 2nd ed. New York : CRC Press, 1995.
31. Steinmetz R. Multimedia systems. New York : Springer-Verlag, 2004. 466 p.
32. Suneja K., Dua S., Dua M. A review of chaos based image encryption. 2019 3rd international conference on computing methodologies and communication (ICCMC), Erode, India, 27–29 March 2019. 2019. URL: https://doi.org/10.1109/iccmc.2019.8819860
33. Teh J. S., Alawida M., Sii Y. C. Implementation and practical problems of chaos-based cryptography revisited. Journal of information security and applications. 2020. Vol. 50. P. 102421. URL: https://doi.org/10.1016/j.jisa.2019.102421

34. Zolfaghari B., Koshiba T. Chaotic image encryption: state-of-the-art, ecosystem, and future roadmap. Applied system innovation. 2022. Vol. 5, no. 3. P. 57. URL: https://doi.org/10.3390/asi5030057
35. What is group theory and how does it relate to cryptography?. Quora. URL: https://www.quora.com/What-is-group-theory-and-how-does-it-relate-to-cryptography.
36. What is elliptic curve cryptography? Definition & faqs | avi networks. Avi Networks. URL: https://avinetworks.com/glossary/elliptic-curve-cryptography/