ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - ГАБРОВО

ОТЧЕТ

НАЦИОНАЛНА ПРОГРАМА „МЛАДИ УЧЕНИ И ПОСТДОКТОРАНТИ - 2“ - ЕТАП II

Тема на проекта: Разработка и анализ на хаос-базирани криптографски алгоритми за защитено предаване на изображения в незащитени комуникационни мрежи.

Факултет: ЕЕ

Постдокторант: гл. ас. д-р инж. Христина Светославова Стойчева

Период на отчитане: Януари 2025 г. – Август 2025 г.

---

1. Актуалност на научното изследване и прилагане на нови решения или нови методически подходи:

Според статистически проучвания на Canalys, приблизително 1.94 трилиона снимки са направени през 2024 г., или 5.3 милиарда снимки дневно, като 94% от тях са заснети със смартфон, а 14 милиарда изображения се споделят ежедневно в социалните мрежи. Този впечатляващ обем генерирана дигитална информация неизбежно поставя въпроса за гарантиране на нейната защита.

Споделянето на лична дигитална информация се е превърнало в ежедневие за голяма част от населението. Но до каква степен може да бъде гарантирана цялостта на създаденото дигитално съдържание? Масово използваните платформи за споделяне на дигитално съдържание работят все по-усилено за поддържане на определени нива на защита от неоторизиран достъп. И ако в тези платформи дигиталната информация се споделя умишлено и с цел да достигне до широка аудитория, не така стои въпросът при предаването на чувствителна информация, свързана с медицински състояния, корпоративни данни, местоположение на обекти със стратегическо значение и др. Именно това е причина за засиления научен интерес в областта на защитеното предаване на данни през последните години.

Хаотичните системи предлагат привлекателни свойства за криптографията — висока чувствителност към начални условия, псевдослучайност и комплексна динамика. Поради това множество алгоритми за криптиране на изображения и хибридни криптосистеми използват хаотични карти и хаотична синхронизация. Въпреки това при пренасяне на математическите свойства в цифрово реализирани алгоритми възникват специфични уязвимости (като ограничен ключов обем, ефекти на крайна прецизност и периодичност), които налагат критичен анализ и сравнение.

Интегрирането на хаотични системи в процеса на криптиране на изображения е съвременна и ефективна стратегия, която разчита на непредсказуемостта, чувствителността

към начални условия и псевдослучайността, присъщи за хаоса. В литературата се представят разнообразни подходи за внедряване на хаос в процеса на криптиране, които обобщено могат да бъдат категоризирани както следва: използване на едномерни или многомерни хаотични функции (карти) [1,2], хаотично маскиране [3] и алгоритми, базирани на хаотична синхронизация [4,5].

Съществуват множество различни алгоритми за криптиране на изображения. Те могат основно да се разделят на: симетрични [6]; асиметрични [7]; хаотични [8]; фрактални [9]; и хибридни [10]. Част от по-разпространените алгоритми за криптиране на изображения се базират на класически подходи като OTP алгоритми [11,12], докато други разчитат на по-нестандартни методи, като внедряване на схеми за хаотична синхронизация [13–15]. През последните години особена популярност придобиват и иновативни подходи в криптирането на изображения, като внедряването на изкуствен интелект.

Изкуственият интелект навлиза бързо във всеки аспект на новите технологии. Неговото приложение е широко и разнообразно и обхваща области като автомобилостроене [16,17,18], индустриална и силова електроника [19,20,21], медицина [22–26], химия [27,28], комуникации [29–35] и др. Една от най-актуалните тенденции в областта на комуникациите е именно защитеното предаване на данни, което обуславя изследването на различни възможности за внедряване на изкуствен интелект в алгоритми за криптиране на изображения.

Критерии за оценка на хаотични алгоритми

За да се оцени обективно качеството и сигурността на хаотичните криптографски системи, се използват няколко групи показатели. От гледна точка на сигурността ключово значение има размерът на ключовото пространство, степента на чувствителност към началните условия, поведението на генерираните последователности и устойчивостта на алгоритъма към стандартни криптоаналитични атаки – ciphertext-only, known-plaintext, chosen-plaintext и chosen-ciphertext.

При алгоритмите за криптиране на изображения са утвърдени специфични количествени метрики. Сред тях най-често използвани са NPCR (Number of Pixel Change Rate) и UACI (Unified Average Changing Intensity), които измерват чувствителността на алгоритъма към малки промени в оригиналното изображение. Ентропията на криптираното изображение, корелацията между съседни пиксели и равномерността на хистограмите служат за оценка на статистическата сигурност на криптирането. Допълнително, при някои алгоритми се извършват NIST тестове за случайност, когато структурата на криптографския поток го позволява.

Освен криптографските показатели, практическата приложимост на алгоритмите се оценява чрез анализ на изчислителната сложност, възможностите за паралелизация и производителността при реални устройства, включително мобилни системи и IoT платформи. В тази връзка особено значение имат ограниченията на цифровата аритметика (finite precision), които могат да доведат до нежелана периодичност, деградация на хаотичните свойства и възможност за възстановяване на параметри.

Общи тенденции и често срещани слабости

Макар много хаотични алгоритми да демонстрират добри статистически показатели, тяхната сигурност невинаги е гарантирана. Значителна част от публикуваните решения използват хаотични функции с ограничено ключово пространство или формално дефинирани начален параметри, което ги прави уязвими към систематичен анализ. Някои подходи, макар и математически коректни, страдат от ограничената прецизност на цифровата реализация, която изменя динамиката на системата и води до периодично поведение. В допълнение, множество алгоритми не са изпитани срещу избрани-плейнтекст или избрани-шифротекст атаки, което оставя сигурността им непълно оценена.

От друга страна, хибридните подходи демонстрират най-добър баланс между сигурност и производителност. Комбинирането на хаотични карти за реализиране на пермутационната фаза с класически криптографски дифузионни механизми често води до решения, които съчетават висока статистическа сигурност с устойчивост към аналитични атаки. Тези алгоритми обаче обикновено са по-сложни за имплементация и изискват внимателно тестване върху широк набор от изображения и сценарии.

Обобщение:

Систематичният анализ на съществуващите хаотични алгоритми за криптиране на изображения показва, че хаосът представлява мощен инструмент, но ефективността му зависи силно от начина на цифрова реализация и от допълнителните криптографски механизми, с които се комбинира. Докато мнозина от описаните в литературата методи постигат висока ентропия и добри NPCR/UACI показатели, устойчивостта им към криптоаналитични атаки често остава под въпрос. Ето защо разработването на надеждни хаос-базирани криптографски системи изисква комплексен подход, включващ не само математически анализ, но и систематично експериментално тестване, което да отчита ограниченията на реалните дигитални платформи и разнообразието от практически случаи на приложение.

Литература:

1. Li, L. (2024). A novel chaotic map application in image encryption algorithm. Expert Systems with Applications, 124316.
2. Liu, H., Liu, J., & Ma, C. (2023). Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption. Multimedia Tools and Applications, 82(16), 23899-23914.
3. Zhang, B., & Liu, L. (2023). Chaos-based image encryption: Review, application, and challenges. Mathematics, 11(11), 2585.
4. Wang, X., Zhang, X., Gao, M., Tian, Y., Wang, C., & Iu, H. H. C. (2023). A color image encryption algorithm based on hash table, hilbert curve and hyper-chaotic synchronization. Mathematics, 11(3), 567.
5. Stoycheva, H., Mihalev, G., Sadinov, S., & Angelov, K. (2025). Implementation of Chaotic Synchronization and Artificial Neural Networks in Modified OTP Scheme for Image Encryption. Journal of Imaging, 11(4), 121.
6. A. Khompysh, Dyusenbayev, D., Maxmet, M., "Development and analysis of symmetric encryption algorithm.", *International Journal of Electrical and Computer Engineering* (IJECE), 2025, 15(2), pp. 1900-1911.
7. F. Lalem, Laouid, A., Kara, M., Al-Khalidi, M., Eleyan, A., "A novel digital signature scheme for advanced asymmetric encryption techniques.", *Applied Sciences*, 2023, 13(8), 5172.
8. B. Zhang, Liu, L., "Chaos-based image encryption: Review, application, and challenges.", *Mathematics*, 2023, 11(11), 2585.
9. S. Inam, Kanwal, S., Batool, M., Al-Otaibi, S., Jamjoom, M. M., "A blockchain-integrated chaotic fractal encryption scheme for secure medical imaging in industrial IoT settings.", *Scientific Reports*, 2025, 15(1), 7652.

10. M. Alanzy, Alomrani, R., Alqarni, B., Almutairi, S., "Image steganography using LSB and hybrid encryption algorithms.", *Applied Sciences*, 2023, 13(21), 11771.
11. N. N. Thorat, Singla, A., Dhaigude, T., "Sharing Secret Colour Images with Embedded Visual Cryptography Using the Stamping Algorithm and OTP Procedure.", *International Journal on Recent and Innovation Trends in Computing and Communication*, 2023, 11(6), pp. 63-70.
12. R. Konwar, Jha, D., Agrawal, R., Purkayastha, R., Banerjee, I., "A Two-Factor Authentication Mechanism Using a Novel OTP Generation Algorithm for Cloud Applications.", In 2024 14th *International Conference on Cloud Computing, Data Science & Engineering* (Confluence), IEEE, 2024, January, pp. 245-250.
13. N. A. Saeed, Saleh, H. A., Hou, L., Nasr, E. A., "A novel chaotic oscillator with a half-line of unstable equilibria: Basins of attraction, chaos control, chaos synchronization, and encryption applications.", *Modern Physics Letters B*, 2025, 39(08), 2450436.
14. Q. Shi, Zhao, Y., & Ding, Q., "Design and FPGA implementation of encrypted frame transmission scheme based on chaotic reverse synchronization.", *Nonlinear Dynamics*, 2025, 113(6), pp. 5511-5535.
15. C. H. Yang, Lee, J. D., Tam, L. M., Li, S. Y., Cheng, S. C., "FPGA Implementation of Image Encryption by Adopting New Shimizu–Morioka System-Based Chaos Synchronization.", *Electronics*, 2025, 14(4), 740.
16. P. V. Ajitha, Nagra, A., "An overview of artificial intelligence in automobile industry–a case study on Tesla cars.", *Solid State Technology*, 2021, 64(2), pp. 503-512.
17. C. R. Madhavaram, Sunkara, J. R., Kuraku, C., Galla, E. P., Gollangi, H. K., "The future of automotive manufacturing: Integrating AI, ML, and Generative AI for next-Gen Automatic Cars.", *International Multidisciplinary Research Journal Reviews-IMRJR*, 2024, 1, 010103.
18. A. K. Tyagi, Mishra, A. K., Kukreja, S., "Role of Artificial Intelligence Enabled Internet of Things (IoT) in the Automobile Industry: Opportunities and Challenges for Society.", *In International Conference on Cognitive Computing and Cyber Physical Systems,* Singapore: Springer Nature Singapore, 2023, pp. 379-397.
19. K. S. S. Liyakat, Liyakat, K. K. S., "ML in the electronics manufacturing industry.", *Journal of Switching Hub*, 2023, 8(3), pp 9-13.
20. A. V. Agrawal, Raju, K. M., Sravya, G., Chandrashekhar, A., Ramya, J., "AI-Driven Test and Measurement Automation in Electronics Manufacturing.", In 2024 *Ninth International Conference on Science Technology Engineering and Mathematics* (ICONSTEM), 2024, April, pp. 1-6.
21. K. Vasudevan, "Applications of artificial intelligence in power electronics and drives systems: A comprehensive review.", *Journal of Power Electronics* (JPE), 2023, 1(1).
22. P. Zhang, Kamel Boulos, M. N., "Generative AI in medicine and healthcare: promises, opportunities and challenges.", *Future Internet*, 2023, 15(9), 286.
23. A. L. Beam, Drazen, J. M., Kohane, I. S., Leong, T. Y., Manrai, A. K., Rubin, E. J. "Artificial intelligence in medicine.", *New England Journal of Medicine*, 2023, 388(13), pp. 1220-1221.
24. M. A. Al-Antari, "Artificial intelligence for medical diagnostics—existing and future AI technology!", *Diagnostics*, 2023, 13(4), 688.
25. M. Yip, Salcudean, S., Goldberg, K., Althoefer, K., Menciassi, A., Opfermann, J. D., Lee, I. C., "Artificial intelligence meets medical robotics.", *Science*, 2023, 381(6654), pp. 141-146.
26. A. M. DiGiorgio, Ehrenfeld, J. M., "Artificial intelligence in medicine & ChatGPT: de-tether the physician.", *Journal of Medical Systems*, 2023, 47(1), 32.
27. E. Waisberg, Ong, J., Masalkhi, M., Kamran, S. A., Zaman, N., Sarker, P., Tavakkoli, A., "GPT-4: a new era of artificial intelligence in medicine.", *Irish Journal of Medical Science* (1971-), 2023, 192(6), pp. 3197-3200.
28. R. C. Rial, "AI in analytical chemistry: Advancements, challenges, and future directions.", *Talanta*, 2024, 125949.
29. R. Han, Yoon, H., Kim, G., Lee, H., Lee, Y. "Revolutionizing medicinal chemistry: the application of artificial intelligence (AI) in early drug discovery.", *Pharmaceuticals*, 2023, 16(9), 1259.
30. Z. Qin, Liang, L., Wang, Z., Jin, S., Tao, X., Tong, W., Li, G. Y. "AI empowered wireless communications: From bits to semantics.", *Proceedings of the IEEE,* 2024.
31. F. Xu, Hussain, T., Ahmed, M., Ali, K., Mirza, M. A., Khan, W. U., Han, Z., "The state of ai-empowered backscatter communications: A comprehensive survey.", *IEEE Internet of Things Journal*, 2023, 10(24), pp. 21763-21786.
32. Y. Zuo, Guo, J., Gao, N., Zhu, Y., Jin, S., Li, X., "A survey of blockchain and artificial intelligence for 6G wireless communications.", *IEEE Communications Surveys & Tutorials*, 2023, 25(4), pp. 2494-2528.

33. E. Malthouse, Copulsky, J. "Artificial intelligence ecosystems for marketing communications.", *International Journal of Advertising*, 2023, 42(1), pp. 128-140.
34. T. B. Ahammed, Patgiri, R., Nayak, S., "A vision on the artificial intelligence for 6G communication.", *Ict Express*, 2023, 9(2), pp. 197-210.
35. M. E. E. Alahi, Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., Mukhopadhyay, S. C. "Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends.", *Sensors*, 2023, 23(11), 5206.
36. A. J. G. De Azambuja, Plesker, C., Schützer, K., Anderl, R., Schleich, B., Almeida, V. R., "Artificial intelligence-based cyber security in the context of industry 4.0—a survey.", *Electronics*, 2023, 12(8), 1920.

2. Изпълнение на поставените цели и задачи:

Целта на проекта бе да се изследва и разработи иновативна хаос-базирана криптографска система за сигурно криптиране и предаване на изображения в комуникационни мрежи.

Основни задачи:

1. **Анализ на съществуващите хаотични алгоритми и криптографски системи. –** Анализирани са множество различни криптиращи алгоритми базирани на хаос. Техните силни и слаби страни в приложението им към криптиране на изображения, както и идентифициране на области за подобрение в сигурността и производителността, са взети в предвид при разработването на нови техни модификации.
2. **Разработване на програмни системи и модули в среда MATLAB/Simulink** –
   - Разработен е програмен модул за криптиране на изображения комбиниращ хаос и матрица на Фибоначи чрез интегриране на изкуствен интелект чрез Generative Pre-trained Transformer;
   - Разработена е симулационна система за криптиране на изображения, базирана на нова хиперхаотична система от пети ред, реализирана в средата MATLAB/Simulink.
3. **Разработване на алгоритми за хаос-базирано криптиране на изображения,**
   - Разработена е модификация на алгоритъм за криптиране на изображения комбиниращ хаос и матрица на Фибоначи чрез интегриране на изкуствен интелект чрез Generative Pre-trained Transformer (GPT).
   - Разработен е алгоритъм за криптиране на изображения, базиран на нова хиперхаотична система от пети ред, реализирана в средата MATLAB. Предлаганата система проявява хиперхаотично поведение с повече от един положителен Lyapunov експонент, което я прави особено подходяща за генериране на криптографски ключове с висока непредсказуемост и ентропия. Алгоритъмът прилага еднократна XOR операция между оригиналното изображение и ключ, генериран чрез хаотична динамика, комбиниран с втори статичен ключ за повишена сигурност.
4. **Проучване и оптимизация на алгоритми за обработка на изображения** – Анализиран е базов алгоритъм, който използва хаотична система на Лоренц от трети ред и включва основни процедури като пермутация и дифузия. Въз основа на изведените графични резултати, илюстриращи вариацията на ентропията на

изображението във връзка с промяната на параметрите на системата се разкрива ясно определен регион в пространството на параметрите, в който ентропията достига най-високите си стойности. На база тези наблюдения се формулира критерий за оптималност, дефиниращ целева функция, която улавя чувствителността на ентропията към два ключови параметъра на системата, включително параметъра на бифуркация. Изведена е комплексна целева функция, а проблемът за оптимизация се решава с помощта на модифицирана версия на алгоритъма на Price, обогатена с техники на изкуствения интелект.

5. **Тестване на предложените криптографски алгоритми -** Тестването е извършено с помощта на тестови изображения от специализирани бази данни. Този тип тестване подпомага оцени качествените показатели на криптиращите алгоритми в условия на различни типове изображения – с различна структура, хетерогенност и динамичен диапазон на яркостта.
6. **Анализ на резултатите и оценка на ефективността на разработените алгоритми** по отношение на сигурност, сложност и устойчивост на смущения в комуникационния канал, са извършени на база ефективността на метода, чрез визуални и статистически анализи, включително хистограми, коефициенти на корелация, информационна ентропия и устойчивост на диференциални атаки, измерена чрез метриките NPCR и UACI. Резултатите потвърждават способността на алгоритмите да постигат високо ниво на объркване и дифузия, което ги прави обещаващо решение за сигурна защита на изображения в комуникационни среди, изискващи висока конфиденциалност на данните.

3. Извършена научно-изследователска и експериментална работа:

Разработена е модификация на алгоритъм за криптиране на изображения базиран на матрица на Фибоначи и хаос.

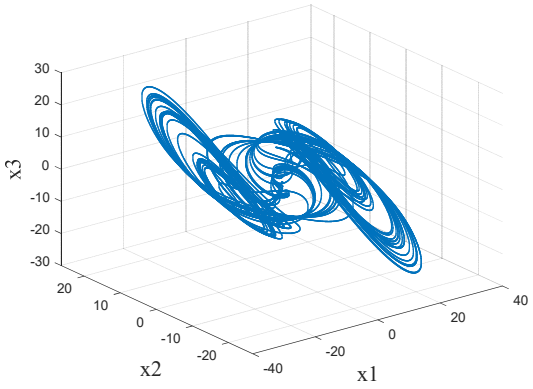
1. Математически основи

1.1 Хаотичен модел

През 2024 г. Shukur и съавт. предлагат модел на треторазмерна хаотична система със специфична нелинейност [33]:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = x_3 \\ \dot{x}_3 = ax_1 - bx_2 - cx_3 - dx_1|x_1| \end{cases}$$

където стойностите на параметрите на системата са: $a = 1{,}8,\ b = 1{,}4,\ c = 0.43$ and $d = 0{,}1$. Графичното представяне на хаотичния атрактор на системата е симулирано при следните произволно избрани начални условия $\mathbf{x}_0 = [0 \quad 0 \quad -1]^T$.



Фигура 1. Триизмерна проекция на хаотичния атрактор на модела на Shukur.

1.2 Фибоначи Q матрица

В математиката редицата на Фибоначи представлява числова последователност, в която всеки елемент е равен на сумата от двата предходни. Тази последователност е тясно свързана със златното сечение и в продължение на стотици години е широко проучвана в различни научни области.

Матрицата **Q на Фибоначи** се дефинира като:

$$Q = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

където F_n е число на Фибоначи. Тогава:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix},$$

Обратната матрица $Q^{(-n)}$ има следния вид:

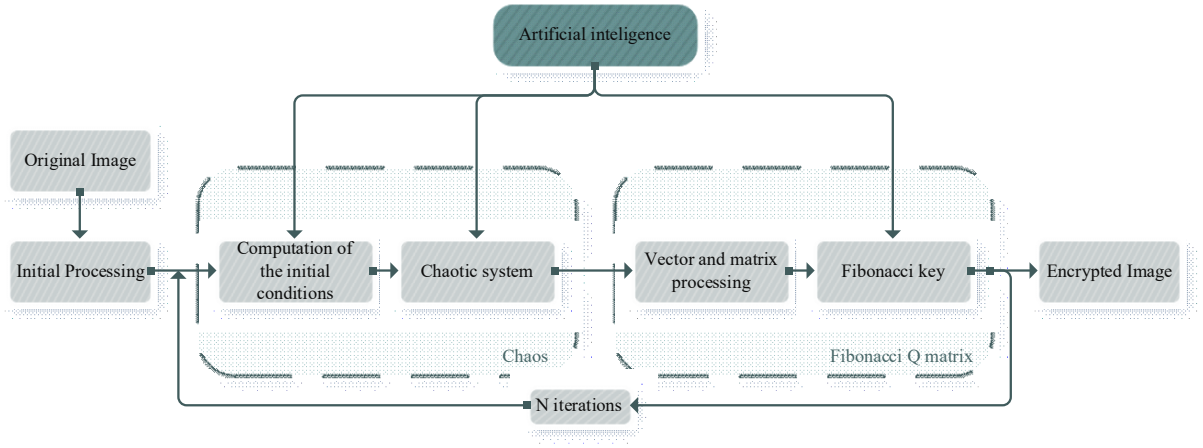
$$Q^{-n} = \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix}.$$

2. Модификация на алгоритъм за криптиране на изображения.

Алгоритмите от този тип предлагат високо ниво на сигурност, но имат и определени недостатъци, основно свързани с генерирането на криптографския ключ. Използването на изкуствен интелект ще подобри качествата на разглежданата кодираща схема, като я направи по-гъвкава и по-ефективна при работа с цветни изображения.

Модификацията на алгоритъма включва използването на изкуствен интелект при определянето на параметрите на хаотичната система, нейните начални условия и матрицата на Фибоначи, въз основа на свойствата на кодираното изображение. Това придава динамичен характер на тези стъпки от процеса на кодиране. Освен внедряването на изкуствен интелект, алгоритъмът е модифициран и чрез включването на хаотична система от трети ред, която беше описана и анализирана в предходния раздел.

Фигура 2 представя блоковата диаграма на модифицирания алгоритъм.



Фигура 2. Блокова диаграма на модифицирания алгоритъм, използващ изкуствен интелект и тримерната хаотична система на Shukur.

Algorithm 1: Image Encryption and Decryption Workflow

Input: Color image (from a .jpg file)
Output: Encrypted and decrypted image, MSE and PSNR values

Prompt user to select an image file via file dialog
$api\_key \leftarrow$ OpenAI API key
$I \leftarrow$ `imread`(selected file)
$[M, N, nc] \leftarrow$ image dimensions
`// Ensure even dimensions`
if M *or* N *is odd* **then**
  Increase M and/or N by 1
end
Resize I to $[M, N]$
Display I with title "Original Image"
$rounds \leftarrow 2$
`// Encrypt each color channel`
for $i \leftarrow 1$ **to** nc **do**
  $[I_{enc}(:,:,i), SX_i] \leftarrow Encrypt(I(:,:,i), rounds, params)$
end
Display I_{enc} with title "Encrypted Image"
`// Decrypt each color channel`
for $i \leftarrow 1$ **to** nc **do**
  $I_{dec}(:,:,i) \leftarrow Decrypt(I_{enc}(:,:,i), SX_i)$
end
Display I_{dec} with title "Decrypted Image"

Фигура 3. Псевдо код на модифицираният алгоритъм.

Algorithm 1: Image Encryption Algorithm

Input: Image I, Rounds r, Parameters *params*
Output: Encrypted image I_{enc}, Sequence SS

if I *is missing* **then**
  error("Image required")
end
if r *is missing* **then**
  $r \leftarrow 2$; `// Default rounds`
end
$r \leftarrow \lceil r \rceil$; **if** $r < 1$ **then**
  error("Invalid round count")
end
Adjust size of I to even dimensions by padding with zeros
$(M, N) \leftarrow$ size(I); $MN \leftarrow M \cdot N$
for $k \leftarrow 1$ **to** r **do**
  Flatten I to vector P (double precision)
  Initialize x from P and MN using chaotic formula
  Define system $L(t, x)$ using parameters a, b, c, d, e, r from *params*
  Solve ODE: $Y \leftarrow$ `ode45`$(L, [t_0, t_f], x)$
  Extract and sort values from Y to get index sequence S
  $SS[k] \leftarrow S$
  Permute P with S, reshape into matrix R' of size $M \times N$
  Define matrix A
  Apply 2×2 block matrix multiplication: $C \leftarrow R' \cdot A$
  $I \leftarrow C \bmod 256$
end
$I_{enc} \leftarrow$ `uint8`(I)

Фигура 4. Псевдо код на кодиращата функция.

Изследвана е оптимизация, базирана на ентропия, в хаотични алгоритми за криптиране на изображения с внедряване на изкуствен интелект.

1. Методи и материали

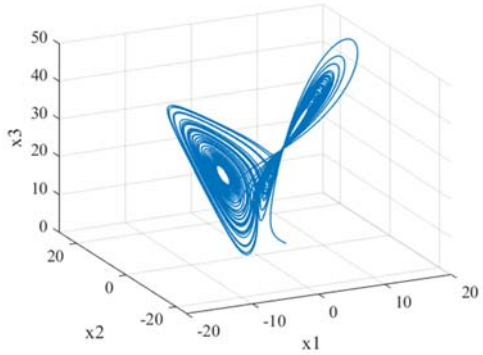
1.1.Хаотична система на Лоренц

За най-известна и най-рано математически формулирана хаотична система се счита опростения модел на уравненията за топлинна конвекция, предложен от Eduard Lorenz през 1963г. Той доказва, че предложеният от него тримерен модел с голяма степен на точност може да бъде използван за изследване на реалния модел на топлинна конвекция. Топлинната конвекция е явление в атмосферата, което се наблюдава при движението на въздушни маси вследствие на разлики в температурата.

Математичният модел на системата на Lorenz е:

$$\dot{x}_1 = -\sigma x_1 + \sigma x_2$$
$$\dot{x}_2 = -x_1 x_3 + r x_1 - x_2$$
$$\dot{x}_3 = x_1 x_2 - b x_3$$

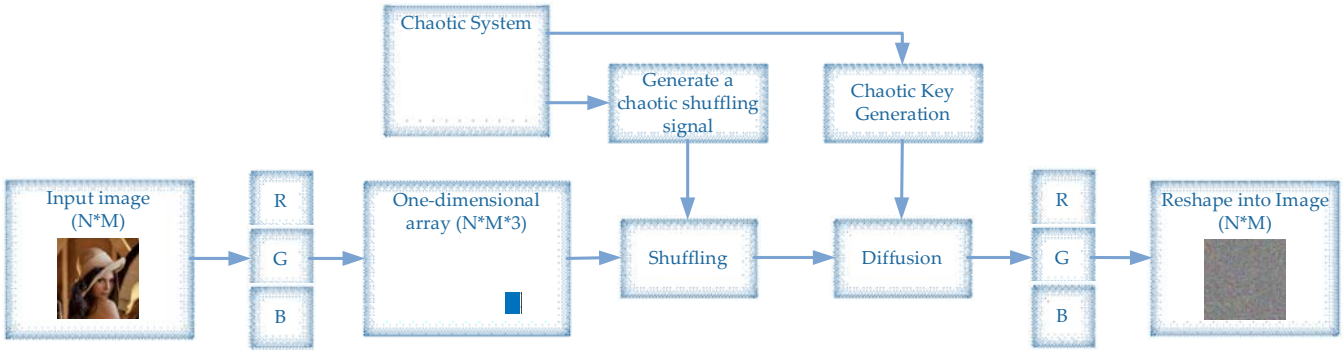
където x_1 е скоростта на флуида в кръга, x_2 и x_3 са съответно вертикалната и хоризонталната температурни разлики, σ е константата на Prandtl, b - пространствена константа и r- числото на Rayleigh, което е пропорционално на приложената топлина и може да се разглежда като вход на системата.



Фигура 5. Хаотичен атрактор на Лоренц

1.2. Хаос базирани алгоритми за криптиране

Разглежда се базова версия на алгоритъм за криптиране, използващ хаотичен сигнал. В почти всички алгоритми за криптиране на изображения, базирани на хаотични системи, сигналът, генериран от системата, се използва поне на два етапа и на няколко нива. Фигура 6 показва блоковата диаграма на базов алгоритъм за криптиране на изображения, базиран на хаос.



Фигура 6. Блок диаграма на базов алгоритъм за криптиране на изображения базиран на хаос

Първоначално се въвежда изображението, което ще бъде криптирано, и се извършва предварителна обработка. В стъпката за предварителна обработка изображението се

преобразува в сивотоново (ако алгоритъмът ще работи само с такива изображения) или се разделя на три отделни изображения, едно за всеки цветови канал. След това изображенията се трансформират от матрична форма в едномерни масиви и се комбинират, като се получава числова последователност с размер N×M×3.

След предварителната обработка се извършват стъпките на разбъркване (shuffling) и дифузия. Алгоритмите се различават по това коя от тези операции се изпълнява първо. Процесът на разбъркване включва основно работа с индексите на едномерния масив, получен от сигнала, генериран от хаотичната система. Размерността е същата като тази на масива, извлечен от изображението. След това масивът се сортира или се прилага друг алгоритъм за объркване на стойностите на елементите. Използвайки индексите, стойностите на пикселите от изображението се пренареждат, като по този начин се създава ново изображение с разбъркани пиксели.

За процеса на дифузия се генерира т.нар. хаотичен ключ. Този ключ може да бъде споделен, или ако не е, е необходима хаотична синхронизация. Методът за получаване на хаотичния ключ може да варира значително, използвайки различни математически принципи. Основно се разчита на псевдослучайната природа на избраната хаотична система, комбинирана с функционална нормализация на стойностите. Полученият ключ след това се комбинира с изображението чрез побитова XOR операция.

Комбинацията от разбъркване и дифузия може да се прилага многократно и на няколко нива, както на ниво пиксел, така и на ниво бит. След завършване на тези основни процеси изображението се реконструира на нивото на пикселите чрез формиране на три изображения за трите цветови канала, които след това се комбинират.

2. Оптимизация, базирана на ентропия, чрез прилагане на метода на Price и изкуствен интелект

2.1. Информационна ентропия

Ентропия е физична величина, която представлява мярка за безпорядък. Информационната ентропия, първоначално предложена от Шенон, е една от ключовите мерки за количествено определяне на степента на несигурност (случайност) на дадена система по отношение на информацията [5026]. Тя може да се прилага за измерване на случайността в системата за криптиране на изображения. Като се има предвид 8-битово ниво на сивата скала, което има 256 възможни пикселни стойности, т.е. $0, 1, \dots 255$, информационната ентропия – H, може да бъде формулирана като следното уравнение:

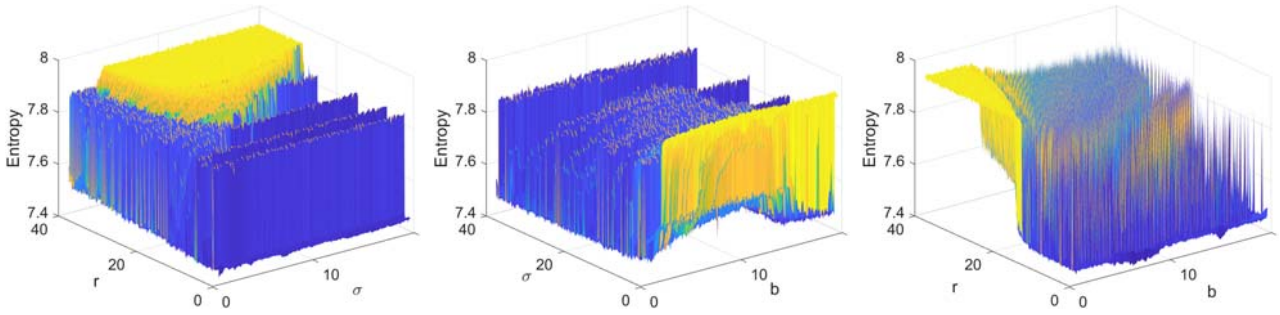
$$H(x) = -\sum_{i=0}^{255} p(x_i) \log_2 p(x_i) \qquad (5.2.7)$$

където $p(x_i)$ е вероятността с която i-тата сива стойност x_i се появява в изображение x. За криптирано изображение, когато всяка стойност на сивото x_i се появява с еднаква вероятност, т.е. $\frac{1}{256}$, информационната ентропия получава максимума - 8. Следователно, идеалният подход за криптиране на изображения трябва да има информационната ентропия близка до 8.

За настоящия алгоритъм целта не е да се постигне възможно най-високата стойност на ентропията, а да се намери оптималната. Хаотичната система има три параметъра, а

ентропията се изчислява за три потенциални целеви функции, при които се променят само два от параметрите, докато третият остава константен (избира се номиналната стойност).

Фигура 8 представя триизмерни графики на ентропията на тестово изображение при прилагането на разглеждания алгоритъм за криптиране. Ентропията се изчислява за изображение с размери 50×50 със стъпка $\Delta x = 0.01$. Промените на параметрите са в диапазона, в който хаотичната система може да бъде решена, и са регулирани съобразно приемливо време за изчисление, а именно $r = 0 \div 40$, $\sigma = 0 \div 20$ и $b = 0 \div 20$.



(**a**) (**b**) (**c**)

Фигура 7. Триизмерни графики на ентропията на тестово изображение, криптирано с разглеждания алгоритъм и системата на Лоренц: (a) При промяна на параметрите **r** и **σ**, **b = 8/3**; (b) При промяна на параметрите **σ** и **b**, **r = 25**; (c) При промяна на параметрите **r** и **b**, **σ = 10**.

Получените графики показват, че разглежданата целева функция е сложна функция с множество екстремуми и форми. Такъв тип сложни функции са трудни за диференциране и идентифициране аналитично. За да се намери екстремумът, се решава оптимизационен проблем с неизвестна целева функция, тъй като времето за изчисление дори за по-малки $\Delta \mathbf{x}$ е изключително голямо и формата на функцията на ентропията не може да бъде получена в разумно време с оглед на настоящите изчислителни възможности.

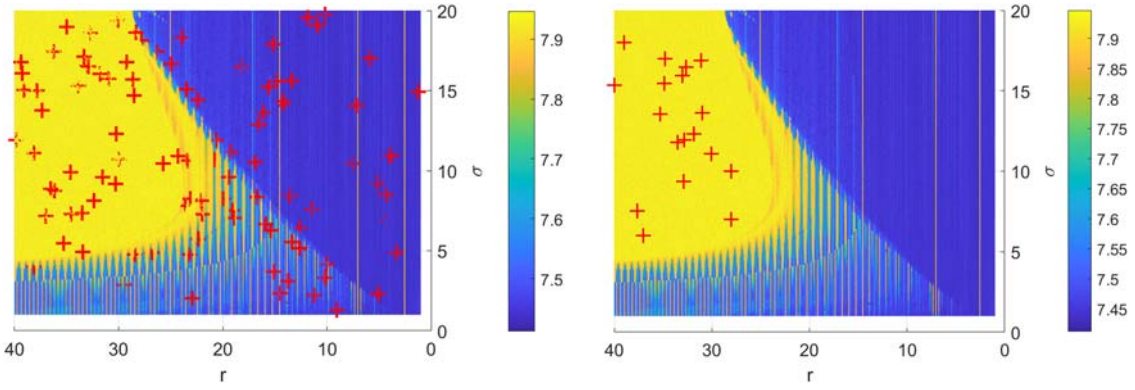
2.2. Модифициран метод на Прайс за намиране на глобален екстремум

Методът на Price използва елементи от кластерен анализ. Първоначално се генерира набор от M равномерно разпределени точки, наричани още агенти, в рамките на допустимото пространство. Всеки агент изчислява стойността на целевата функция. Случайно се избират групи от по 3 агента. Изчислява се аритметичната средна стойност на целевите функции на тези агенти и се създава нов агент. Ако стойността, предоставена от новия агент, е по-добра от най-лошата в текущата популация, новият агент замества този с най-лошия резултат; в противен случай новият агент се отхвърля. Алгоритъмът е организиран така, че групата агенти да се конвергира около текущия екстремум с продължаването на итерациите. С увеличаването на прага за най-лошия резултат, агентите се концентрират около областта на глобалния екстремум. Броят на агентите в метода не е строго дефиниран, но за 2 до 3 контролни параметъра M се избира да бъде между 10 и 100.

Чрез използване на знанието на GPT модела за хаотичната система и свойствата на изображението, координатите на точките се разполагат основно в областта, където най-вероятно се намира глобалният екстремум. Може да се каже, че генерираните агенти са „умни“ и са концентрирани около екстремума, което позволява алгоритъмът да се конвергира към него много по-бързо, без излишно лутане, което повишава продуктивността. Използвани са M = 20

агенти, отново с 1000 итерации, и е намерен екстремум с стойност 7.9498 за σ = 10.97 и r = 32.62.

Въпреки драстично по-малкия брой агенти, модификацията дава по-добри резултати при решаването на оптимизационния проблем.



а) б)

Фигура 8. Първоначално разпределение на агенти в а) класически Прайс метод, б) Модифициран Прайс метод

Изследване на алгоритъм за криптиране на изображения базиран на нова хиперхаотична система в среда на Matlab

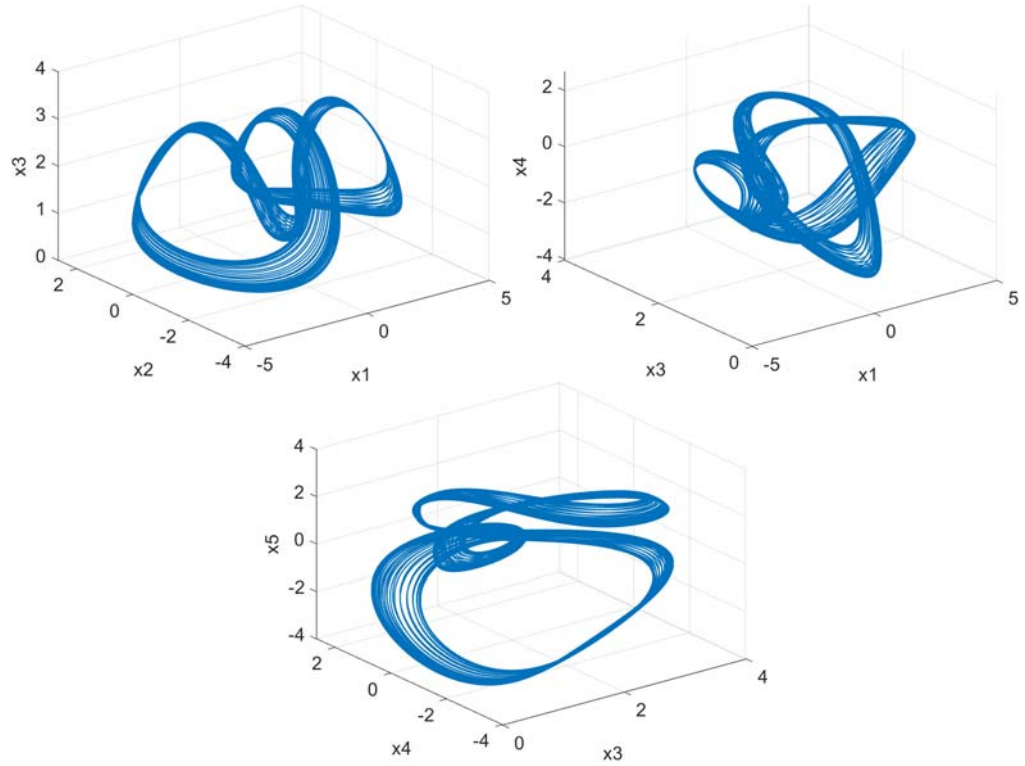
1. Хиперхаотична система

През 2024 г. е предложен нов математичен модел на хиперхаотична система от пети ред, чиято динамика са описва със следната система от уравнения [12]:

$$\begin{cases} \dot{x}_1 = x_1 x_2 + b x_1 + a x_5 \\ \dot{x}_2 = -x_1^2 + x_3^2 \\ \dot{x}_3 = -x_2 x_3 + x_3 x_4 \\ \dot{x}_4 = -x_3^2 + x_5^2 \\ \dot{x}_5 = -x_4 x_5 - a x_1 - b x_5 \end{cases}$$

За стойности на параметрите $a = 1, b = 1$ и следните произволно избрани начални условия: $\mathbf{x} = [2\ 1\ 1\ 1\ 2]^T$, системата има хиперхаотично поведение.

Хаотичният атрактор на петмерна хиперхаотична система се намира в 5D пространството. Не съществува способ за единно графично представяне на толкова сложна проекция. Прието в практиката е да се използват тримерни проекции в пространство на състоянието. За представяне на една хиперхаотична система от пери ред са необходими десет тримерни проекции. Три от тях са представени на фиг. 9.



Фиг. 9. *Тримерни проекции на хаотичен атрактор*

2. Алгоритъм за криптиране на изображения базиран на хиперхаотична система

Представеният алгоритъм реализира криптиране и декриптиране на изображения с използване на комбинация от хаотично генерирани ключове и еднократно прилагане на битова операция XOR. Псевдо-код на програмата е представен на фиг. 10.

Algorithm 1: Псевдокод за криптиране и декриптиране на изображение с хаотичен OTP ключ

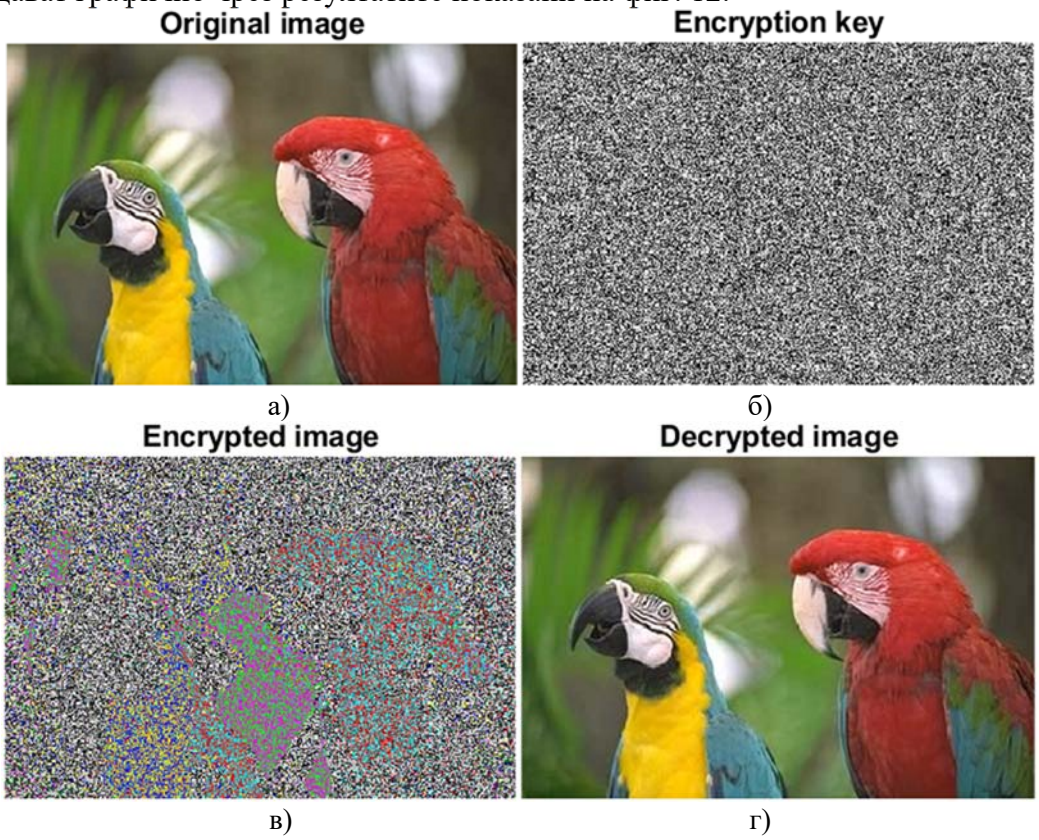
Input: Изображение I
Output: Криптирано изображение $EncI$, декриптирано изображение $DecI$

1. Зареждане на изображението:
$I \leftarrow$ `imread(път)`
2. Генериране на хаотични ключове:
Извличане на променливи x_1, x_2, x_3, x_4, x_5 от система
Генериране на бинарен хаотичен поток чрез итерации
Изграждане на ключ key_1 от хаотичния поток
Генериране на статичен ключ key_2
Комбиниране: $key \leftarrow key_1 \oplus key_2$
3. Криптиране:
$EncI \leftarrow$ `imageProcess`(I, key)
4. Декриптиране:
Повторно генериране на key със същите начални условия
$DecI \leftarrow$ `imageProcess`$(EncI, key)$
5. Визуализация:
Показване на I, $EncI$, $DecI$ с помощта на `imshow`

Фиг. 10. *Псевдо-код за криптиране и декриптиране на изображение с хиперхаотичен ключ*

Алгоритъмът започва със зареждане на изображение (фиг. 11 а)) и извличане на пет стойности от предварително изчислената хиперхаотична система. Въз основа на тези стойности се създава бинарен поток чрез итеративна формула, чиито стойности се преобразуват в ключ. Успоредно с това се генерира втори, статичен ключ. Полученият криптиращ ключ (фиг. 11 б)) е резултат от XOR между двата ключа, което повишава сигурността чрез допълнителна ентропия. С помощта на този ключ оригиналното изображение се кодира (фиг. 11 в)). За декриптиране се повтаря процесът по генериране на ключ, при същите начални условия, и полученият ключ се използва за възстановяване на изображението

(фиг. 11 г)). Алгоритъмът демонстрира висока ефективност и сигурност, които се потвърждават графично чрез резултатите показани на фиг. 12.



Фиг. 12. *Резултати от процеса по криптиране и декриптиране*

4. Получени крайни резултати:

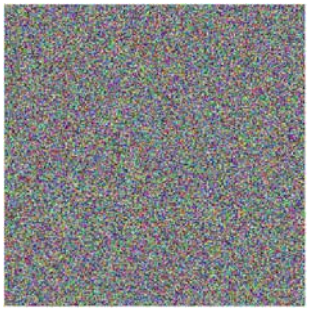
1. *Резултати от модифицираният алгоритъм за криптиране на изображения базиран на матрица на Фибоначи и хаос.*

За тестване на модифицирания алгоритъм са използвани различни стандартни цветни изображения от свободно достъпни бази данни. За оценка на качеството и нивото на криптиране на изображенията са приложени няколко широко използвани статистически и числени анализа, а именно: хистограми, корелационни функции, информационна ентропия, NPCR и UACI.

1.1. Основни резултати

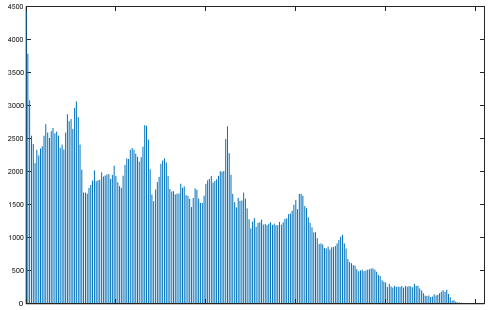
Основното тестово изображение, избрано за анализа, е „Lena“. Оригиналното, криптираното и декриптираното изображение са представени на Фиг. 12 а), б) и в), след което са показани графично представените хистограми (г) и д)) и корелации (е) и ж)) на оригиналното и криптираното изображение.

(а) original

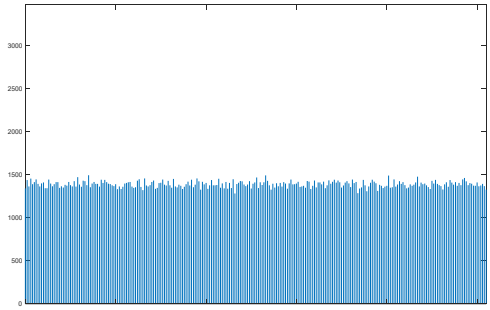


(б) encrypted

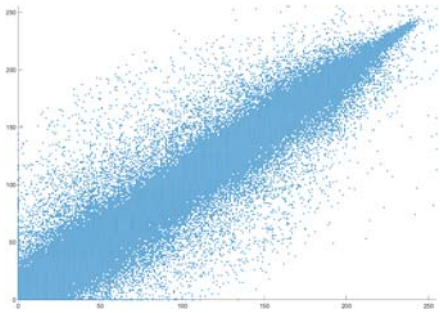
(в) decrypted



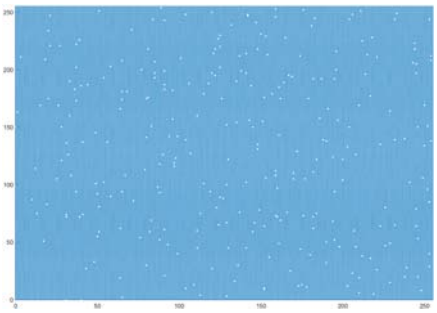
(г) Histogram of the OI



(д) Histogram of the EI



(е) Correlations of the OI



(ж) Correlations of the EI

Фигура 12. Оригинално изображение (а), криптирано (б) и декриптирано (в), заедно с графично представените им хистограми (г – Оригинално изображение; д – Криптирано изображение) и корелации (е – Оригинално изображение; ж – Криптирано изображение).

Хистограмата на криптираното изображение е стабилна, гладка и равномерно разпределена, което демонстрира високо ниво на криптиране на изображението. Това показва, че полученият криптиран образ не предоставя никаква статистическа информация за съответното входно изображение. По отношение на анализа на корелационния модел, степента на корелация между оригиналното и криптираното изображение е изключително ниска, което допълнително потвърждава високото ниво на постигнато криптиране.

Таблица 1 представя числените резултати за информационната ентропия, както и коефициентите NPCR и UACI.

Таблица 1. Числови резултати

	Entropy	**Correlation**	**NPCR**	**UACI**
Input image	7,3283	0,9864	-	-
Encrypted image	7,9995	0,0037	99,6217	33,4463

Представените числени резултати показват, че стойностите на информационната ентропия и NPCR са близки до теоретичния максимум, докато коефициентът на корелация е значително по-нисък в сравнение с този на оригиналното изображение.

Таблица 2 представя сравнение между оригиналния алгоритъм, базиран на хиперхаотична система от 6-ти ред и Q-матрицата на Фибоначи [32], и представената модификация. Сравнението е направено въз основа на цифровите резултати, получени при криптиране на сивотоновото изображение Lena.

Таблица 2. Сравнителен анализ за черно-бяло изображение Lena

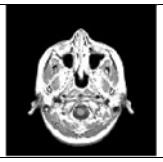
	Entropy	**Correlation**	**NPCR**	**UACI**
Input image	7,3283	0,9864	-	-
Original method [32]	7,9993	0,0069	99,6174	33,4226
Modified	7,9995	0,0037	99,6217	33,4463

От представените данни може да се заключи, че въведените модификации на алгоритъма повишават информационната ентропия и коефициентите NPCR, както и значително подобряват коефициента на корелация.

1.2. Допълнителни резултати

Освен това, модифицираният алгоритъм, базиран на хаос, GPT и Q-матрицата на Фибоначи, беше тестван с четири допълнителни стандартни тестови изображения. Получените резултати са представени в таблицата по-долу.

Таблица 3. Числени резултати за допълнителните изображения

					
Entropy	OI	3.6779	7.6288	7.8471	7.7563
	EI	7.9707	7.9992	7.9993	7.9994
Correlation	OI	0.9365	0.9747	0.9394	0.9829
	EI	0.0172	0.0012	-0.0014	-0.0018

Получените резултати за набора от допълнителни тестови изображения потвърждават изводите от предишния раздел. Коефициентите на корелация и информационна ентропия имат стойности, близки до теоретичния максимум, което демонстрира устойчивостта на алгоритъма срещу атаки чрез brute-force.

1.2.1. Диференциална атака

Едно от характерните свойства на криптографските алгоритми, устойчиви на диференциални атаки, е тяхната изключителна чувствителност дори към минимални промени в кодираното изображение. Способността на алгоритъма за криптиране да устоява на диференциални атаки може да се оцени чрез анализа на представянето на алгоритъма с помощта на тестовете Number of Pixels Change Rate (NPCR) и Unified Average Changing Intensity (UACI).

Таблица 4 представя стойностите на коефициентите NPCR и UACI за набора от тестови изображения.

Таблица 4. Числени резултати за диференциална атака

	Lena	**MRI**	**Parrots**	**Koala**	**Flower**
NPCR	99.6217	98.7732	99.6005	99.6180	99.5985
UACI	33.4463	34.9041	32.9957	33.2955	33.2622

Постигнатото високо ниво на устойчивост към диференциални атаки се потвърждава от изключително високите стойности на коефициентите NPCR и UACI.

1.2.2. Атаки чрез brute force

Ключовото пространство представлява пълния набор от възможни комбинации на ключове, които криптографският алгоритъм може да използва. Достатъчно голямото ключово пространство — обикновено по-голямо от 2^{100} - е от съществено значение за предотвратяване на brute-force атаки.

При разглеждания алгоритъм ключовото пространство зависи от началните условия на променливите на хаотичната система x_1, x_2 и x_3 както и от параметрите на системата a,b,c и d, в комбинация със стойностите на Q-матрицата. Приемайки, че само параметрите на системата и началното състояние $\mathbf{x}_0$ се използват като споделен таен ключ — което е честа практика при алгоритми за криптиране, базирани на хаос — полученото ключово пространство е минимум равно на $\mathbf{x}_0 \times 2^{212}$. Тази стойност значително надвишава прага, необходим за устойчивост срещу brute-force атаки, като по този начин се осигурява висока степен на сигурност.

1.2.3. Устойчивост на шум и загуба на данни

За оценка на устойчивостта на алгоритъма към шумови атаки към криптираното изображение се добавя шум „Salt and Pepper“ с различна плътност. След това засегнатите изображения трябва да бъдат успешно декриптирани. Освен това е необходимо да се оцени способността на алгоритъма да декриптира криптирано изображение, от което липсват сегменти с различни размери. За количествено определяне на качеството на криптиране при декриптиране на повредено изображение се използва метриката PSNR (Peak Signal-to-Noise Ratio).

Таблица 5. PSNR за „Salt and Pepper“ шум и загуба на данни

	Lena	**MRI**	**Parrots**	**Koala**	**Flower**
S&P noise level 0.002	22.6550	20.7806	23.6613	23.4391	22.8415
S&P noise level 0.005	18.9475	16.7527	19.6873	19.6417	19.0693
Data cut – 6%	16.8817	14.9539	17.7199	17.5721	17.0821
Data cut – 12%	11.6756	10.2426	12.4800	12.3592	11.7835

Таблица 5 представя резултатите за коефициента PSNR при шум „Salt and Pepper“ с плътности 0.002 и 0.005, както и при нарушения на целостта на изображението с загуби от 6% и 12% за целия набор от тестови изображения.

1.2.4. Анализ на времето за изпълнение

При оценката на изчислителната сложност на алгоритъма с използване на нотация O(…) става ясно, че общата сложност зависи основно от размера на входното изображение. С други думи, алгоритъмът има сложност O(N×M). Въпреки това, по-практична представа за изчислителните разходи и времето за изпълнение може да се получи чрез използване на Run-Time Profiler в MATLAB, тъй като алгоритъмът е реализиран и тестван в MATLAB среда.

За оценка на времето за изпълнение основната програма записва времето, необходимо за изпращане и получаване на отговори от AI модела, както и времето за криптиране и декриптиране. Резултатите за изображения с размери 256×256 и 512×512 са обобщени в Таблица 6.

Таблица 6. MATLAB Run-time performance резултати

Image size	Using AI	Encrypt	Decrypt	Total time
256×256	1.615 s	0.721 s	0.066 s	4.7415 s
512×512	2.062 s	2.395 s	0.252 s	7.584 s

Получените резултати ясно показват, че методът за изпращане на заявката към GPT модела не е определящ фактор. Вместо това, времето за изпълнение зависи основно от пропускателната способност на мрежата, латентността, натоварването на крайния сървър и евентуалните ограничения на скоростта, приложени на крайния пункт.

Що се отнася до процеса на криптиране, по-голямата част от времето се изразходва за подпрограмата, която решава системата от диференциални уравнения на хаотичната система. Например, това изчисление отнема приблизително 0.663 секунди за изображение с размер 256×256 и около 2.137 секунди за изображение с размер 512×512, което представлява приблизително 90% от общото време за криптиране.

Процесът на декриптиране, от друга страна, е значително по-бърз, тъй като диференциалната система не трябва да се решава отново. Общото време за изпълнение включва също множество допълнителни операции, като създаване и манипулиране на фигури, визуализация на изображения, работа с файлове и други. Когато се изключат продължителностите на тези допълнителни процеси, може да се заключи, че теоретичната изчислителна сложност, изразена с нотация O(…), действително се потвърждава.

2. *Резултати от прилагането на алгоритъма на Price с изкуствен интелект за определяне на оптималните параметри на хаотичната система*

Оптимизацията на предложената схема за криптиране на изображения се базира на целевата функция, представена в предишния раздел, която отразява ентропията на изображението във връзка с вариациите на параметрите на хаотичната система σ и r, докато параметърът b остава на номиналната си стойност. Представените резултати имат за цел да идентифицират стойностите на параметрите, които дават най-висока ентропия, без да се твърди, че алгоритъмът осигурява изключително високо ниво на сигурност. Този тип оптимизация, реализирана по описания начин, може да бъде приложена към всеки алгоритъм за криптиране на изображения, базиран на хаотични системи.

Таблица 7 представя числените резултати за ентропията на кодираното изображение при номиналните стойности на параметрите на хаотичната система, както и стойностите, получени чрез стандартния алгоритъм на Price и неговата модификация с изкуствен интелект.

Тестовите изображения са избрани от предварително подбрани бази данни и имат резолюция 256×256 пиксела. Избрани са както цветни, така и сивотонови изображения, за да се гарантира изчерпателността на изследването.

Таблица 7. Числените резултати за ентропията

	Entropy of the original image	With Nominal Parameters of the Chaotic System	With Standard Price Optimization Method	With AI-Enhanced Price Optimization Method
	7.3283	7.9975	7.9978 σ = 11.5682 r = 28.8351	7.9979 σ = 12.5817 r = 31.1784
	7.6968	7.9971	7.9978 σ = 11.3439 r = 29.1481	7.9981 σ = 11.8787 r = 29.1722
	7.7211	7.9976	7.9978 σ = 10.0268 r = 28.8655	7.9979 σ = 11.4699 r = 31.1835
	7.0839	7.9972	7.9976 σ = 10.6537 r = 28.4883	7.9979 σ = 11.9907 r = 28.7076
	7.4868	7.9961	7.9972 σ = 11.8724 r = 30.9686	7.9974 σ = 12.0712 r = 31.0978

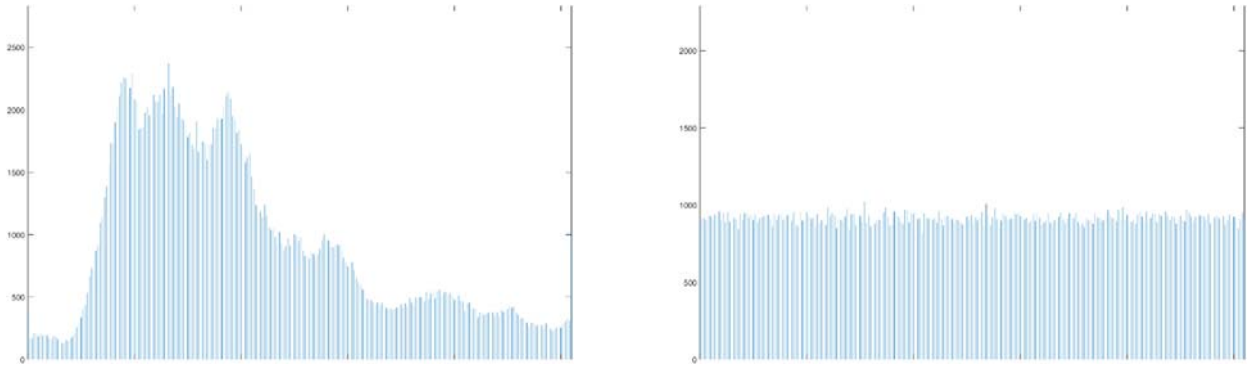
Последният набор от резултати показва, че процесът на криптиране действително може да бъде подобрен чрез формулиране и решаване на оптимизационен проблем. Максимизирането на ентропията беше извършено както чрез стандартния алгоритъм на Price, така и чрез модификация на алгоритъма на Price с изкуствен интелект. Модифицираният метод постигна по-добра стойност на екстремума в сравнение със стандартния, като разликата варира от приблизително 0.001 до 0.0002 — значително подобрение в контекста на криптиране на изображения. Превъзходните резултати се дължат основно на предположението, че AI има предварителни знания за хаотичната система и нейния бифуркационен параметър. В резултат на това началните координати на агентите са по-добре подбрани. Идентифицираните екстремуми се намират в т.нар. плато на целевата функция и могат да се считат за глобални, въпреки че алгоритъмът на Price не гарантира откриването на абсолютния глобален оптимум.

3. *Оценка на качеството на кодиране и устойчивостта срещу диференциални атаки при алгоритъм за криптиране на изображения базиран на хиперхаотична система*

От техническа гледна точка, крайната оценка за това дали даденото изображение е с висока степен на кодиране или с добро качество след възстановяването, се базира на

субективната преценка на човека. Поради тази причина анализа на резултатите от процеса по декриптиране се осъществява на база два основни метода, широкоразпространени в публикациите по тематиката, а именно хистограми и корелации.

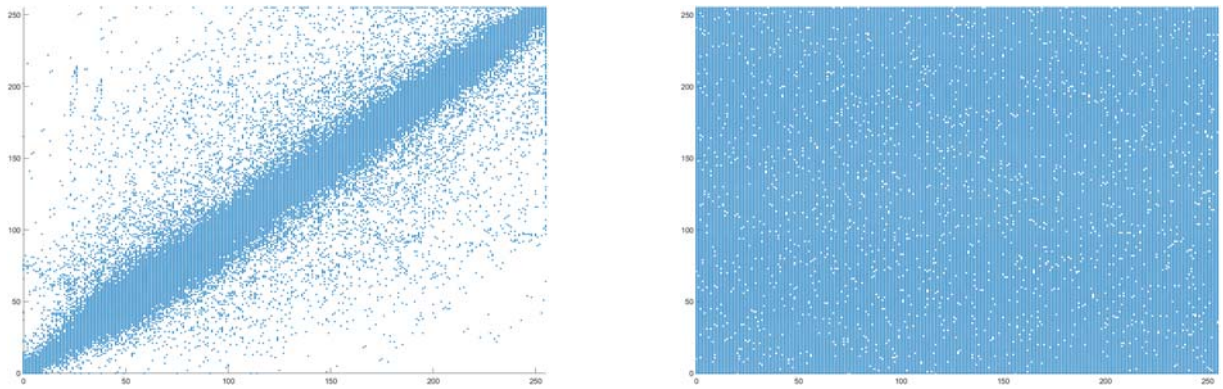
Хистограма - Хистограмата измерва качеството на криптиране по отношение на това как увеличава максимално отклонението между оригиналното и криптираното изображения. Хистограмите получени при изследване на предложеният алгоритъм са представени на фиг. 13.



а) б)

Фиг. 13. *Хистограми на а) оригинално изображение, б) криптирано изображение*

Корелация - Корелационният анализ е метод за обработка на статистически данни използвани за изучаване на коефициенти (корелации) между променливи. При анализа се сравняват коефициентите на корелацията между една или повече двойки променливи, за да се установят статистически взаимозависимости между тях. Полезен показател за оценка на качеството на криптиране на дадено изображение е коефициентът на корелация между пикселите при едни и същи индекси в оригиналните и криптираните изображения.



а) б)

Фиг. 14. *Графично представяне на корелация - а) оригинално изображение, б) криптирано изображение*

Освен чрез графично представяне (фиг. 14), коефициентът на корелация между оригиналното изображение и неговото криптирано изображение може да се изчисли, като неговата идеална стойност се намира около нулата. Получените стойности за коефициент на ко-релация при изследване на предложеният алгоритъм са представени в Таблица 8.

Информационната ентропия е статистически тест, който оценява неопределеността и случайността в комуникационните системи. При криптирането на изображения ентропията се използва за измерване на случайността на разпределението на пикселите в шифрованото изображение. Високата стойност на ентропията показва по-добра объркаост и липса на

какъвто и да е различим модел в криптираното изображение. Теоретично максималната стойност на информационна ентропия е 8. Получените стойности за коефициент на информационна ентропия при изследване на предложеният алгоритъм са представени в Таблица 8.

Таблица 8. Числови резултати

	Корелация	Ентропия	NPCR	UACI
Оригинално изображение	1.000	7.4122	99.5806	30.4716
Криптирано изображение	0.0029	7.9977		

Диференциални атаки се използват от криптоаналитиците с цел, да се открие връзката между оригинално и криптира-но изображение, като се внасят малки изменения в оригиналното изображение и в последствие то се криптира със същия ключ. Алгоритъмът за криптиране трябва да има отлични характеристики на дифузия, при които промяната на един пиксел в оригиналното изображение би трябвало да генерира напълно различно шифровано изображение. Способността на алгоритъма за криптиране да устои на диференциални атаки може да бъде оценена чрез анализ на производителността на алгоритъма, използвайки тестовете за NPCR и UACI.

Честота на промяна на пикселите -Метриката NPCR (Number of Pixels Change Rate) измерва процента на разликите между две шифровани изображения, получени чрез криптиране на две изображения, които се различават само по един пиксел, а всички останали пик-сели в двете изображения са еднакви. По-високата стойност на NPCR показва по-голяма реакция на алгоритъма към промени в изображението или ключа и по този начин по-добра устойчивост на диференциални атаки. Идеалната стойност на NPCR е ≥99,6094%. Получената стойност за NPCR при изследване на предложеният алгоритъм са представени в Таблица 8.

Средна степен на изменение на интензитета – UACI (Unified Average Changing Intensity) е друг показател, който се използва за оценка на способността на алгоритъм за криптиране да устои на диференциални атаки чрез измерване на средния интензитет на промяната между две шифровани изображения, получени чрез криптиране на две еднакви изображения, различаващи се само по един пиксел. Подобно на NPCR, по-високата стойност на UACI показва по-добра устойчивост на диференциал-ни атаки. Идеалната стойност за UACI е ≥ 33,4635%. Получената стойност за UACI при изследване на предложеният алгоритъм са представени в Таблица 8.

5. Използване и разпространение/внедряване на научните резултати (прилагат се към отчета):

- публикации, реферирани в Scopus и Web of Science
  - Stoycheva, H., Sadinov, S., Angelov, K., Kogias, P., & Malamatoudis, M., “Implementing Artificial Intelligence in Chaos-Based Image Encryption Algorithms”, Engineering Proceedings, 2025, 104(1), 20.

  - Stoycheva, H., Mihalev, G., “Entropy-based optimization in chaotic image encryption algorithms with implementation of artificial intelligence”, Engineering Proceedings, 2025, 104(1), 16.
  - H. Stoycheva, “Secure communication scheme based on chaotic switching between non-identical systems”, International Conference Automatics and Informatics 2025 (ICAI'25) 09-11.10.2025, Varna Bulgaria, 2025, (Scopus) (in print)
- други публикации
  - Х. Стойчева, „Изследване на алгоритъм за криптиране на изображения базиран на нова хиперхаотична система в среда на MATLAB“, Сборник доклади от научна конференция TechCo – Lovech 202 Сборник доклади: IX Национална научна конференция с международно участие ТК Ловеч „TechCo 2025”, 27 юни 2025, гр. Ловеч, ISSN 2535-079X, с. 133-138.
  - Х. Стойчева, „Архитектура и анализ на производителността при криптиране на изображения с изкуствени невронни мрежи в MATLAB“, Сборник доклади от научна конференция TechCo – Lovech 202 Сборник доклади: IX Национална научна конференция с международно участие ТК Ловеч „TechCo 2025”, 27 юни 2025, гр. Ловеч, ISSN 2535-079X, с. 128-132.
  - Х. Стойчева, „Имплементиране на хиперхаотична синхронизационна схема в алгоритъм за криптиране на изображения базиран на фрактално тромино“, Сборник доклади: Международна научна конференция UNITECH 2025, 20-21Ноември 2025, Габрово, България, ISSN: 2603-378X, стр. 1-7.

Дата: 09.12.2025 г. Изготвил: …….

/гл. ас. д-р инж. Христина Стойчева/