MATHEMATICAL MODELING AND COMPUTING, Vol. 11, No. 3, pp. 826–834 (2024)

A RGB image encryption algorithm based on Archimedes optimizer, chaos and DNA

Bencherqui A.[1], Tahiri M. A.[1], Karmouni H.[2], Alfidi M.[1], Sayyouri M.[1], Qjidaa H.[3], Jamil M. O.[2]

[1] *Engineering, Systems and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco*

[2] *Systems and Sustainable Environment Laboratory (SED), Faculty of Engineering Sciences (FSI), Private University of Fez (UPF), Fez, Morocco*

[3] *CED-ST, STIC, Laboratory of Electronic Signals and Systems of Information LESSI, Dhar El Mahrez, Faculty of Science, Sidi Mohamed Ben Abdellah-Fez University, Fez, Morocco*

(Received 7 January 2024; Revised 13 August 2024; Accepted 15 August 2024)

This paper introduces an innovative method for encrypting images, skillfully combining a modified logistic map (MLM), deoxyribonucleic acid (DNA) and the Archimedean optimization algorithm (AO). The resulting system is divided into three essential phases, each playing a distinct role: a permutation phase using the modified logistics map, a diffusion phase using DNA, and finally, an optimization phase incorporating AO. In the optimization phase, the AO is successfully deployed to determine the optimal sequence of masks for image encryption. A notable feature of this approach is its ability to improve the quality of DNA masks, making them compatible with the complex nature of images. Simulation results and performance evaluations attest to the feasibility of the proposed system for color image encryption, underlining at the same time its high level of security. One of the most remarkable aspects of this methodology lies in its ability to enhance entropy, thus conferring increased resistance to various statistical and differential attacks. The approach has been validated through experimental results, affirming its efficacy, consolidating its position as a robust and secure solution for image encryption. This research highlights the significant contribution of the AO algorithm in the specific field of image encryption, offering a major contribution to the evolution of security techniques in this area.

Keywords: *Archimedes optimizer; encryption; modified logistic map.*

2010 MSC: 68-06 **DOI:** 10.23939/mmc2024.03.826

1. Introduction

The widespread adoption of information and communication technologies in recent years has resulted in their pervasive integration across various sectors. Voice data, images and videos are now fundamental elements, circulating freely in modern society [1]. However, with the proliferation of the Internet, the risk of piracy and fraud has intensified, as this channel becomes a breeding ground for unsecured exchanges of information. This reality has made the protection of multimedia data against unauthorized access a major challenge for the research community [2]. Encryption, as an essential bulwark, plays a crucial role in meeting this security requirement. Despite this, conventional encryption techniques such as Advanced Standard Encryption (AES) and Data Encryption Standard (DES) face notable limitations when it comes to handling image data, characterized by high redundancy and high capacity [3].

Faced with these constraints, researchers are increasingly turning to methods based on chaotic systems for image encryption [4]. These approaches, boasting increased sensitivity to initial conditions, erratic behavior, non-periodicity, ease of hardware and software implementation, as well as the possibility of combining them with other tools, are attracting growing interest. Among chaotic maps, the logistic map is emerging as a preferred option, and its modified counterpart has successfully demonstrated its effectiveness in image encryption [5, 6].

In order to design a more powerful encryption system, researchers are advocating synergy between chaotic systems and DNA, the molecule that carries genetic information essential to the development and functioning of organisms [7]. DNA's intrinsic properties, such as high information density, low energy consumption and high parallelism, make it a strategic choice. In addition, the introduction of the optimization algorithm (AO) enriches the toolbox. Based on Archimedes' law of physics, AO has distinguished itself by its remarkable efficiency in solving complex optimization problems, outperforming other classical optimization algorithms [8, 9].

In the context of this research, we suggest an optimal system designed for the encryption of color images. Our ingenious scheme combines a modified chaotic map, DNA, and the AO optimization algorithm for fast and optimized results. Simulation results attest that the combination of MLM-based permutation, DNA diffusion and AO-based optimization generates an optimized encrypted image, ready for secure transmission. This proposal seeks to transcend the limitations of conventional encryption techniques, making a substantial contribution to the advancement of multimedia data security.

The rest of our study is organized as follows: the second section outlines the fundamental components of the proposed encryption scheme, encompassing MLM, AO, and DNA. The third section delves into the encryption scheme specifically designed for color images. The fourth section showcases the simulation results. Conclusions and avenues for future work are addressed in the concluding section.

2. Preliminary

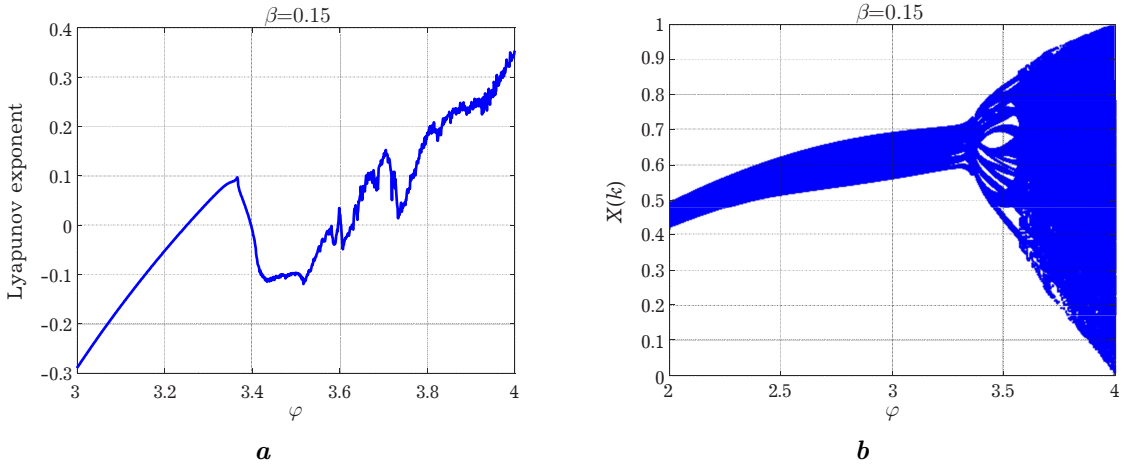
2.1. The modified logistics map (MLM)

Among the classical chaotic maps frequently used in encryption systems, the logistic map stands out for its remarkable sensitivity to initial conditions and its important randomization properties [10]. Seeking to enhance the level of security inherent in the logistic map, Daoui and colleagues [6] have formulated a proposal for its modification. This crucial update involves the introduction of a new parameter β, into the parameter space, conferring increased complexity on the associated key, making it more arduous to use. The following formula defines the modified logistic map (MLM):

$$X_{k+1} = \phi(1 - \beta|\cos(k)|)X_k(1 - X_k) \tag{1}$$

with $\beta \in [0, 0.25]$.

Figure 1 displays the bifurcation and Lyapunov diagrams of the Modified Logistic Map (MLM). This visual representation clearly demonstrates how the parameter β influences the behavior of the initial logistic map, thereby enhancing the key space level.



a ***b***

Fig. 1. (***a***) The MLM's Lyapunov exponent, (***b***) the MLM's bifurcation diagram.

The selection of the Modified Logistic Map (MLM) for the image encryption process stems from its intrinsic qualities of robustness and advanced security. As a chaotic map, MLM offers increased sensitivity to initial conditions, introducing an element of complexity that enhances the security of the encryption process.

However, in order to achieve an even higher level of security and introduce an additional layer of complexity, we decided to go beyond the isolated use of MLM. With this in mind, we chose to combine it in an innovative way with deoxyribonucleic acid (DNA), the molecule that carries essential genetic information.

This strategic combination goes beyond the traditional use of chaotic maps, offering a holistic approach that capitalizes on the advantages of each of these elements. MLM brings its intrinsic ability to generate chaotic sequences, while DNA, as a molecular carrier, adds an extra dimension of security with its high information density, low energy consumption, and high parallelism. This fusion of two robust technologies aims to create an innovative image encryption system, capable of meeting the most stringent security requirements. The details of this combination and the benefits resulting from this synergy are set out in detail in the following paragraphs.

2.2. DNA encoding and decoding

Based on the Watson–Crick complementation rule [11], a series of eight subsequent DNA coding rules unfold, as detailed in Table 1. These rules detail the specific pairings between DNA nucleotide bases, establishing the correspondences needed to reliably encode genetic information. Crucially, this coding rule can be reversed, opening up the possibility of DNA decoding. This reverse phase is of vital importance in the overall process of DNA manipulation in the context of encryption, as it enables the original information to be recovered from the previously encoded sequence. Table 2 shows the DNA_XOR operations, representing a specific facet of this inversion of the coding rule. The XOR (or exclusive) operation is meticulously applied to the bits of two DNA sequences, enabling precise, calculated manipulation to achieve the desired result in the decoding process.

Table 1. DNA coding and decoding.

Rules 2	1	2	3	4	5	6	7	8
00	A	A	T	T	C	C	G	G
01	G	C	G	C	T	A	T	A
10	C	G	C	G	A	T	A	T
11	T	T	A	A	G	G	C	C

Table 2. DNA_XOR.

XOR	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Following the introduction of the DNA that will be integrated into the encryption scheme, the next section is devoted to a detailed presentation of the Archimedes optimization algorithm.

2.3. Archimedes optimizer (AO)

Recent developments have seen the introduction of an innovative algorithm known as the Archimedean Optimization Algorithm (AO) [12]. Its modus operandi is inspired by the famous Archimedes' Law in physics, adding a unique dimension to its approach. AO is distinguished by its ability to strike a harmonious balance between two fundamental aspects of optimization: exploration, which involves seeking new solutions, and exploitation, which aims to capitalize on solutions already discovered.

The key advantage of AO lies in its ability to dynamically modulate this balance between exploration and exploitation. This feature makes it particularly well suited to solving complex optimization problems in engineering, where the search for optimal solutions requires a balanced and flexible approach.

Archimedes' optimization algorithm ingeniously emulates the principles underlying Archimedes' Law, by introducing a notion of buoyancy into the solution search space. This innovative approach makes Archimedes remarkably agile in navigating vast and often complex solution spaces. In the remainder of our talk, we will take a closer look at this new algorithm and examine how its integration into our encryption scheme enhances the system's overall efficiency.

The AO's primary steps are as follows:

Step 1: Start by defining the positions, volume (V), density (D) and acceleration (acc) of all the objects.

Step 2: Update the densities (D) and volumes (V) of an object i. When two objects first collide, they attempt to attain a stable state after some time has passed, and TF is used in the AO to do this. The

transition from exploration to operation is based on the following formula:

$$\mathrm{TF} = \exp\left(\frac{t - t_{\max}}{t_{\max}}\right). \tag{2}$$

Step 3: Similarly, the density factor d_{t+1} decreases over time, allowing one to concentrate in a favorable area:

$$d_{t+1} = \exp\left(\frac{t_{\max} - t}{t_{\max}}\right) - \frac{t}{t_{\max}}. \tag{3}$$

Step 4: Exploration phase. If TF $\leqslant 0.5$ (objects are colliding), at iteration $t+1$, adjust the object acceleration using the following formula:

$$acc_{t+1}(i) = \frac{D_{mr} + V_{mr} \times acc_{mr}}{D_{t+1}(i) \times V_{t+1}(i)}. \tag{4}$$

Step 5: Exploration phase. When TF > 0.5 (no collision between objects), at iteration $t+1$, adjust the object acceleration using the following formula:

$$acc_{t+1}(i) = \frac{D_{\text{best}} + V_{\text{best}} \times acc_{\text{best}}}{D_{t+1}(i) \times V_{t+1}(i)}. \tag{5}$$

Step 6: Normalize acceleration. The normalized acceleration is calculated using:

$$acc_{t+1}(i)_{\text{norm}} = u\frac{acc_{t+1}(i) - \min(acc)}{\max(acc) - \min(acc)} + l, \tag{6}$$

$l = 0.1$ and $u = 0.9$ are the normalization ranges.

Step 7: Update the position. The object position for $t+1$ is calculated by

$$X_{t+1}(i) = \begin{cases} X_t(i) + C_1 \times \text{rand} \times x\_acc_{t+1}(i)_{\text{norm}} \times d \times (X_{\text{rand}} - X_t(i)), & \text{if TF} \leqslant 0.5, \\ X_{\text{best}} + F \times C_2 \times \text{rand} \times x\_acc_{t+1}(i)_{\text{norm}} \times d \times (T \times X_{\text{best}} - X_t(i)), & \text{otherwise.} \end{cases} \tag{7}$$

Step 8: Evaluation. Select the object position with the best suitability value after evaluating each object. The AO flowchart is displayed in Figure 2.

The remarkable efficiency and flexibility demonstrated by the Archimedean Optimization (AO) algorithm motivated its essential integration into our encryption scheme. The intrinsic capabilities of AO have been successfully deployed to determine the optimal sequence of masks used in the image encryption process. This strategic choice is in line with our quest for high-performance, adaptive solutions to enhance the security of our system. A notable feature of this approach is the AO's ability to significantly improve the quality of DNA masks. The aim of this improvement is to make them compatible with the complex nature of images, which often present varied features and subtle structures. The AO's agility in adjusting the mask sequence to the specific requirements of the visual content thus helps to optimize the encryption process, guaranteeing enhanced integrity and security. The integration of the AO algorithm into our encryption scheme thus represents a significant step forward, exploiting its exceptional features to meet the specific challenges posed by image encryption. In the following sections, we will delve into the details of this synergy and illustrate how this innovative combination delivers optimized results, reinforcing the robustness and reliability of our encryption system.

3. The proposed color image encryption scheme

The encryption scheme is based on the following steps:

Step 1: Input original image. In this initial stage, a color image $I(M, N, 3)$ is integrated into the system, where M and N symbolize the dimensions of the original image in number of rows and columns respectively.

Step 2: MLM generates three chaotic sequences $S_x = \{x_1, x_2, \ldots, x_{M\times N}\}$, $S_y = \{y_1, y_2, \ldots, y_{M\times N}\}$ and $S_z = \{z_1, z_2, \ldots, z_{M\times N}\}$.

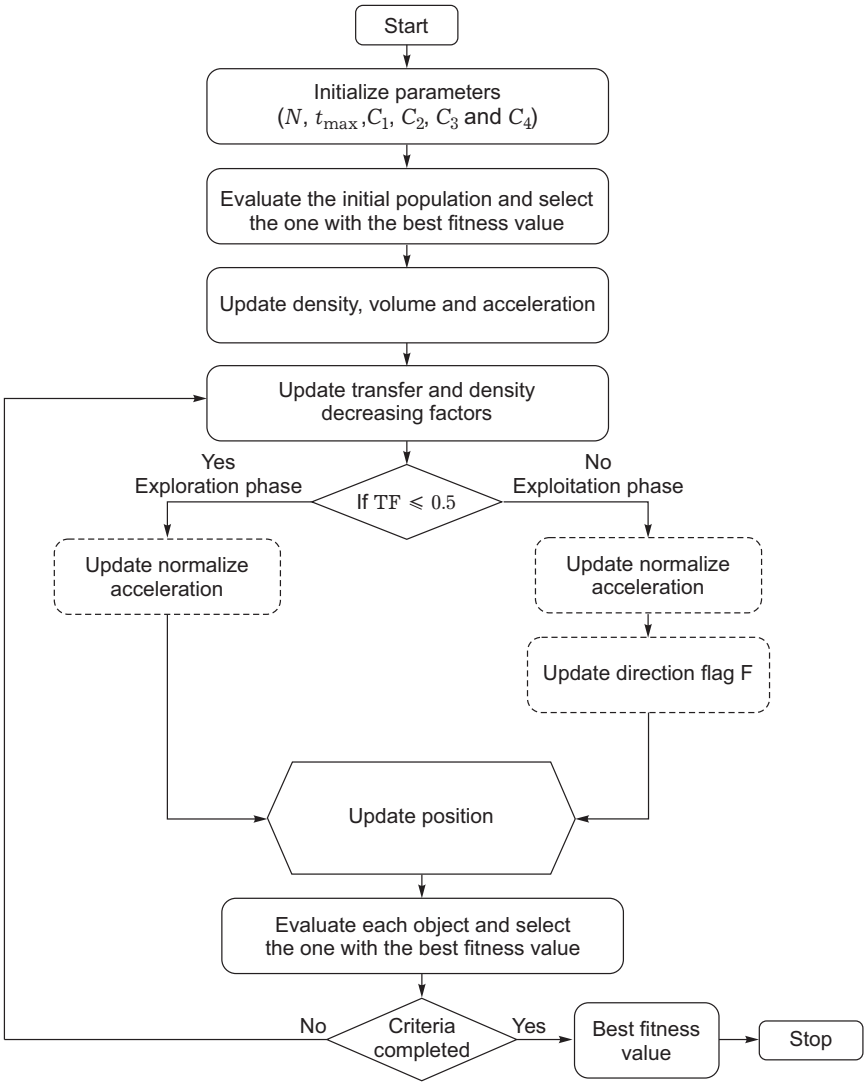


Fig. 2. AO flowchart.

The chaotic sequences crucial to the encryption process are generated using the Modified Logistic Map (MLM), in accordance with the following equations:

$$\begin{aligned} x_{i+1} &= \phi_1(1-\beta_1|\cos(i)|)x_i(1-x_i),\\ y_{i+1} &= \phi_2(1-\beta_2|\cos(i)|)y_i(1-y_i),\\ z_{i+1} &= \phi_3(1-\beta_3|\cos(i)|)z_i(1-z_i). \end{aligned} \tag{8}$$

The values of the parameters of $\{\phi_1, \phi_2, \phi_3, \beta_1, \beta_2, \beta_3, x_0, y_0, z_0\}$ are given as a security key.

Step 3: Transforming the matrices I_R, I_G, I_B and the sequences S_x, S_y, S_z into binary matrices. Next, apply the DNA coding rule to encode the binary matrices into DNA matrices, utilizing the rules specified. This process results in the generation of six transformed coding matrices.

Step 4: Using the AO algorithm to optimize the mask sequence. The next step involves applying the Archimedean Optimization (AO) algorithm to refine the mask sequence. At each iteration, each vector in the population is subjected to the optimization algorithm. In the end, the vector with the best fitness value forms the optimized mask sequence. Figure 3 displays the suggested encryption scheme.

This combined methodology, integrating MLM for chaotic sequence generation and the AO algorithm for DNA mask optimization, offers a robust and sophisticated approach to image encryption. The results obtained through this procedure promise enhanced security and optimum performance when transmitting and storing encrypted images.

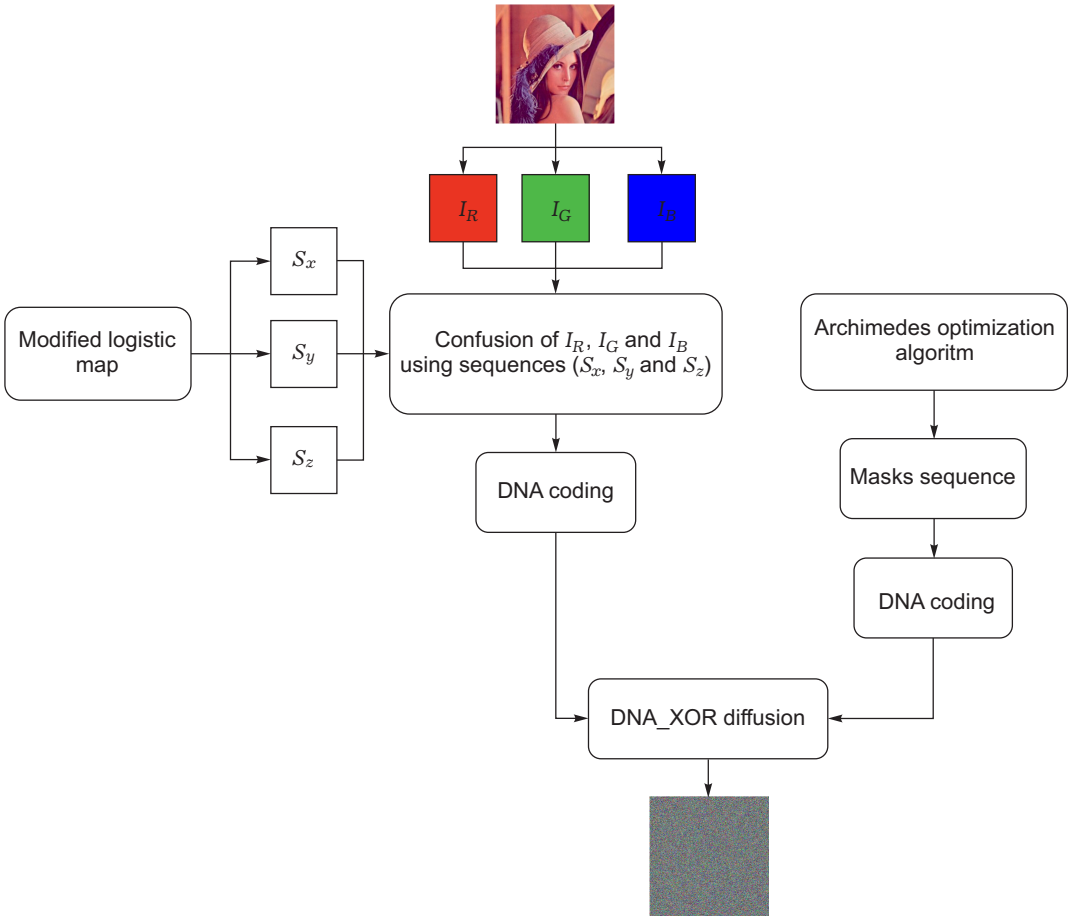
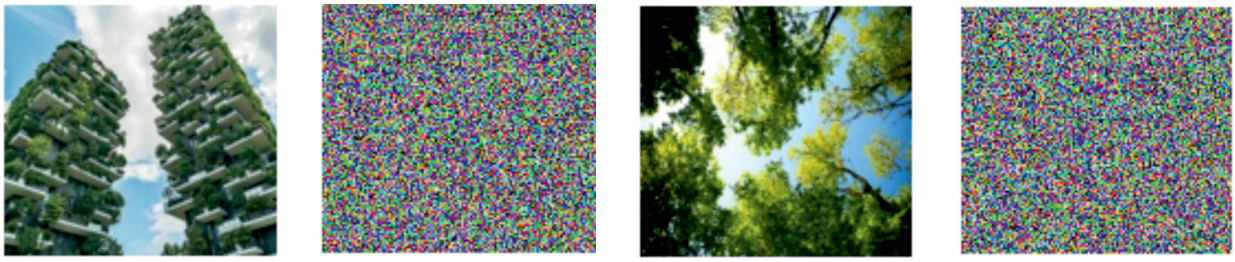


Fig. 3. Bloc diagram of the proposed encryption scheme.

4. Discussion and conclusion

This section is devoted to an in-depth analysis of the performance and detailed simulation results of the encryption technique we have developed, the initial values of the MLM are: $\phi_1 = 3.9$, $\phi_2 = 3.98$, $\phi_3 = 4$, $\beta_1 = 0.08$, $\beta_2 = 0.06$, $\beta_3 = 0.02$. To evaluate the effectiveness of our approach, we have chosen examples of color images such as "Building green cities" and "Tree". The results of this analysis are shown in Figure 4, displaying both the original image and the encrypted images. Looking closely at these images, it is immediately apparent that no discernible relationship exists Among the original and encrypted images. This lack of visual correlation reinforces the robustness of our encryption system, ensuring adequate protection against any attempt at visual analysis. Figure 5 provides an in-depth analysis, exposing the histograms of the original and encrypted images for the R, G and B channels. This graphical representation highlights the uniform distribution of pixels in the encrypted images, confirming the robustness of our system in the face of various statistical attacks. Entropy data, presented in Table 3, further reinforces the resilience of our system. The entropy values of the encrypted images exceed 7.990, approaching their theoretical value of 8 in relation to the original images. This demonstrates the superior ability of our encryption algorithm to counter attacks aimed at altering information entropy. Table 4 shows the correlation coefficients between the original and encrypted images. While the correlation coefficients of the original image are highly correlated (close to 1), those of the encrypted image show a low correlation (close to 0). This finding highlights the significant effectiveness of our encryption system in protecting images against statistical attacks. In summary, the results obtained through this performance analysis attest to the robustness, security, and efficiency of our encryption system, positioning it as a reliable solution for protecting images against various forms of attack.



a ***b*** ***c*** ***d***

Fig. 4. (***a***) Original "Green-cities" image. (***b***) Encrypted "green cities" image. (***c***) Original "Tree" image. (***d***) Encrypted "Tree" image.

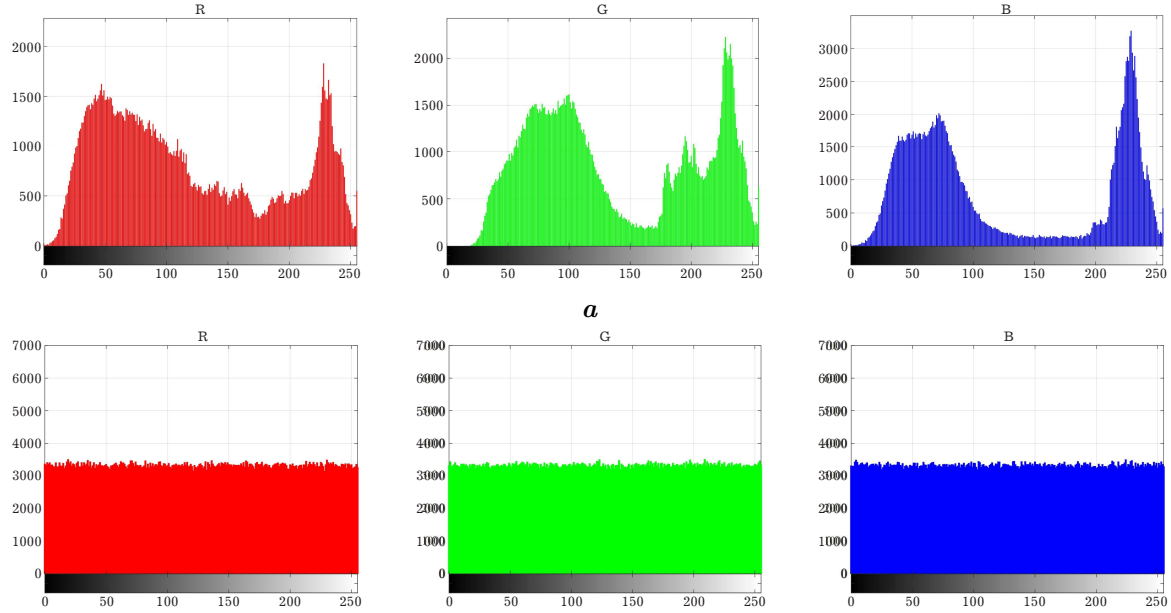


Fig. 5. (***a***) Histogram of the original image. (***b***) Histogram of the encrypted image.

Table 3. Information entropy.

	Original image			Encrypted image			Ref [4]		
H	R	G	B	R	G	B	R	G	B
	4.6511	4.5819	4.4905	7.9998	7.9998	7.9998	7.9971	7.9970	7.9966

Table 4. Correlation coefficients.

	Original image			Encrypted image		
	R	G	B	R	G	B
Horizontal	0.9990	0.9973	0.9998	0.01815	0.00342	0.00117
Vertical	0.9995	0.9991	0.9980	−0.01081	0.01249	−0.00756
Diagonal	0.9986	0.9975	0.9965	0.00533	−0.04018	0.01865

[1] Karmouni H., Yamni M., El Ogri O., Daoui A., Sayyouri M., Qjidaa H., Alami B. Fast computation of 3D discrete invariant moments based on 3D Cuboid for 3D image classification. Circuits, Systems, and Signal Processing. **40** (8), 3782–3812 (2021).

[2] Tahiri M. A., Karmouni H., Sayyouri M., Qjidaa H. 2D and 3D image localization, compression and reconstruction using new hybrid moments. Multidimensional Systems and Signal Processing. **33**, 769–806 (2022).

[3] Bencherqui A., Karmouni H., Daoui A., Alfidi M., Qjidaa H., Sayyouri M. Optimization of Jacobi moments parameters using artificial bee Colony algorithm for 3D image analysis. 2020 Fourth International Conference on Intelligent Computing in Data Sciences (ICDS). 1–7 (2020).

[4] Tahiri M. A., Karmouni H., Bencherqui A., Daoui A., Sayyouri M., Qjidaa H., Hosny K. M. New color image encryption using hybrid optimization algorithm and Krawtchouk fractional transformations. The Visual Computer. **39**, 6395–6420 (2022).

[5] Zheng J., Liu L. Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map. IET Image Processing. **14** (11), 2310–2320 (2022).

[6] Daoui A., Karmouni H., El Ogri O., Sayyouri M., Qjidaa H. Robust image encryption and zero-watermarking scheme using SCA and modified logistic map. Expert Systems with Applications. **190**, 116193 (2022).

[7] Xuejing K., Zihui G. A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. Signal Processing: Image Communication. **80**, 115670 (2020).

[8] Hashim F. A., Hussain K., Houssein E. H., Mabrouk M. S., Al-Atabany W. Archimedes optimization algorithm: a new metaheuristic algorithm for solving optimization problems. Applied Intelligence. **51**, 1531–1551 (2021).

[9] Ait Lhadj Lamin S., Raghib A., Abou El Majd B. Robust multi-objective optimization for solving the RFID network planning problem. Mathematical Modeling and Computing. **8** (4), 616–626 (2021).

[10] Zhang G., Ding W., Li L. Image encryption algorithm based on tent delay-sine cascade with logistic map. Symmetry. **12** (3), 355 (2020).

[11] Patro K. A. K., Acharya B., Nath V. Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation. IETE Technical Review. **37** (3), 223–245 (2020).

[12] Houssein E. H., Helmy B. E.-D., Rezk H., Nassef A. M. An enhanced Archimedes optimization algorithm based on Local escaping operator and Orthogonal learning for PEM fuel cell parameter identification. Engineering Applications of Artificial Intelligence. **103**, 104309 (2021).

Алгоритм шифрування RGB зображення на основі оптимізатора Архімеда, хаосу та ДНК

Бенчеркі А.[1], Тахірі М. А.[1], Кармуні Х.[2], Альфіді М.[1],
Сайюрі М.[1], Кджідаа Х.[3], Джаміль М.О.[2]

[1] *Лабораторія інженерії, систем і застосувань, Національна школа прикладних наук, Університет Сіді Мохамеда Бен Абделла, Фес, Марокко*

[2] *Лабораторія систем і стійкого навколишнього середовища (SED), Факультет інженерних наук (FSI), Приватний університет Феса (UPF), Фес, Марокко*

[3] *CED-ST, STIC, Лабораторія електронних сигналів та інформаційних систем LESSI, Дхар Ель Марез, Факультет природничих наук, Університет Сіді Мохамед Бен Абделлах-Фез, Фес, Марокко*

У цій статті представлено інноваційний метод шифрування зображень, який вдало поєднує модифіковану логістичну карту (MLM), дезоксирибонуклеїнову кислоту (ДНК) і алгоритм оптимізації Архімеда (АО). Отримана система розділена на три основні фази, кожна з яких відіграє окрему роль: фаза перестановки з використанням модифікованої логістичної карти, фаза дифузії з використанням ДНК і, нарешті, фаза оптимізації, що включає АО. На етапі оптимізації АО успішно розгортається для визначення оптимальної послідовності масок для шифрування зображення. Примітною особливістю цього підходу є його здатність покращувати якість масок ДНК, роблячи їх сумісними зі складною природою зображень. Результати моделювання та оцінки ефективності свідчать про придатність запропонованої системи для шифрування кольорових зображень, підкреслюючи в той же час її високий рівень безпеки. Один із найвидатніших аспектів цієї методології полягає в її здатності підвищувати ентропію, надаючи таким чином підвищену стійкість до різноманітних статистичних і диференціальних атак. Цей підхід підтверджено експериментальними результатами, що підтверджує його ефективність і зміцнює його позицію як надійного та безпечного рішення для шифрування зображень. Це дослідження підкреслює значний внесок алгоритму АО у конкретну область шифрування зображень, пропонуючи великий внесок у розвиток методів безпеки в цій галузі.

Ключові слова: *оптимізатор Архімеда; шифрування; модифікована логістична карта.*