

# Searchable encryption based on a chaotic system and AES algorithm

Fairouz Sherali<sup>1</sup>, Falah Sarhan<sup>2</sup>

<sup>1</sup>Department of Computer Science, College of Education for Girls, Kufa University, Kufa, Iraq

<sup>2</sup>Department of Mathematics, College of Education for Girls Kufa University, Kufa, Iraq

## Article Info

### Article history:

Received Nov 14, 2024

Revised May 18, 2025

Accepted Jun 8, 2025

### Keywords:

Advanced encryption standard

Chaotic maps

Cloud computing

Hénon map

Searchable encryption

## ABSTRACT

Cloud computing provides on-demand access to computing resources, such as storage and processing power. This technology allows businesses to scale efficiently while reducing infrastructure costs. However, protecting the security and privacy of data has grown to be a top priority. This is where enhancing cloud security with searchable encryption (SE) is crucial. SE effectively secures users' sensitive data while preserving searchability on the cloud server side. It enables the cloud server to search via encrypted data without disclosing information in plaintext data. SE uses different encryption methods to encrypt data before uploading it to servers. The advanced encryption standard (AES) is a common algorithm for encrypting this data. In this paper, a novel SE method has been presented. The technique exploits the properties of the chaotic map to generate an AES key, which makes the AES algorithm more secure for encrypting the searchable index and uploaded files. We implement and test our method with real data from files. The experimental results show that the proposed method can significantly satisfy a higher level of security as compared to other schemes.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Fairouz Sherali

Department of Computer Science, College of Education for Girls, Kufa University

Kufa, Najaf 00964, Iraq

Email: fairouz.m.jaafar@uokufa.edu.iq

## 1. INTRODUCTION

Cloud computing offers a centralized repository of computing resources that can be quickly and elastically accessed based on users' demand. This technology is rapidly developing and being widely used because of its many benefits [1]. To guarantee security for data stored on the cloud, it is crucial to efficiently and securely store and access the uploaded data. One of the important ways to protect such data is to encrypt it before uploading [2]. Today, Indexing and searching cloud-encrypted data has become interesting [3], [4]. The cryptographic primitive that provides this feature is widely known as searchable encryption (SE) [5].

Encryption includes applying an asymmetric or symmetric algorithm to encrypt the data. Symmetric encryption uses one key for encryption and decryption operations, while asymmetric encryption uses a pair of different keys (public and private keys). There are various symmetric key encryption schemes like advanced encryption standard (AES) [6], [7], data encryption standard (DES), 3DES [8], and Blowfish [9]. In contemporary cryptography, the security of cryptographic systems depends on hard mathematical problems like the finite field discrete logarithm problem (DLP), integer factorization problem (IFP), and elliptic-curve DLP (ECDLP) [10]. Numerous cryptographic methods have been suggested for these problems, such as El-Gamal, Rivest–Shamir–Adleman (RSA), and elliptic curve cryptography (ECC) [11].

Chaotic schemes [12]–[14] offer a higher level of security and strong performance for real-time encryption, where chaos has unique attributes strongly related to the concepts of confusion and diffusion in

cryptography. Examples of these qualities include good pseudo-randomness and sensitivity to its control parameters. Furthermore, these systems are deterministic, meaning no random factors are involved, and their settings entirely determine their future behavior. However, because the chaotic signal is pseudorandom, unauthorized users can mistake it for noise. For these reasons, they satisfy the needs of real-time applications more than AES and DES.

Contemporary research has exhibited the possibility of using chaotic methods in cryptography. For instance, many attempts have successfully integrated chaotic maps into lightweight encryption algorithms to enhance security. Combining chaotic systems enhanced classical encryption algorithms' confusion and diffusion characteristics, increasing their robustness against cryptanalysis [15].

In the same context, several studies applied chaos-based key generation methods to enhance the AES algorithm. There are several issues with studies that use the logistic map for cryptography applications. The choice of parameters greatly influences its chaotic behavior, and when it is not within the optimal range, security is diminished since it becomes predictable. Periodicity can result from digital systems' finite accuracy problems and limited key space, leaving the system open to statistical and brute-force attacks. Furthermore, the system may become less safe and deterministic if the parameters are chosen incorrectly, losing its chaotic characteristics [16].

Notwithstanding the advantages of cloud computing, there are still problems and difficulties in guaranteeing uploaded data's security, confidentiality, integrity, and availability (CIA). To solve these problems, users encrypt their files before uploading them to the cloud. AES is one of the most widely used symmetric encryption algorithms due to its effectiveness and resilience. However, considering the increasing processing power and evolving security risks, fortifying its defences against cryptographic attacks is imperative. In certain sophisticated assault scenarios, the static substitution and permutation processes that form the basis of conventional AES might be predictable. Chaotic systems, such as the Hénon map, exhibit dynamic and surprising behavior, which makes them appealing choices for improving cryptographic techniques. Encryption procedures could become more unpredictable by integrating the Hénon chaotic system, enhancing AES's security and robustness.

The main contributions to this work are: developing a new image encryption algorithm while maintaining the algorithm's efficacy and utility poses challenges to implementation and evaluation. Investigate whether using Hénon chaotic systems is better than using the logistic map to improve AES while maintaining a balance between increased security and computing efficiency. Finally, assess the proposed image encryption method with many evaluation metrics, such as the visibility test, information entropy analysis, peak signal-to-noise ratio (PSNR), number of pixel change rate (NPCR), unified average changing (UACI), and correlation coefficient. The evaluation results of the proposed algorithm are compared with the classical AES encryption algorithm.

The rest of the article is organized as follows. Section 2 reviews the literature that employs chaotic maps in image encryption algorithms. Section 3 explains the research methodology used in this paper to achieve the study's objectives. Section 4 describes the proposed image encryption approach, detailing its structure, workflow, and key features. Section 5 evaluates the performance of the proposed method, examining its efficiency, security, and robustness through various metrics. Finally, section 5 summarizes the key findings of this work, discussing the strengths and potential improvements of the proposed method.

Qiao *et al.* [17] proposed a secure, robust cryptosystem that uses the AES substitution-boxes (S-Box) and chaotic components. It includes a block cipher, a global diffusion, and an effective pseudo-chaotic number generator (PCNG). When chaotic maps formed over real numbers are numerically applied, the PCNG defined on a finite field reduces the possibility of security degradation originating from the dynamical degradation.

To encrypt data, the study [18] proposes a unique and efficient approach that applies interlaced value-location scrambling to create a chaotic structure. Permutation and diffusion were handled as independent operations in the previous research; one was started after the other was finished. Using known-text attacks, this method enables the discovery of the transformation matrix. The suggested method, however, combines the two distinct processes into a single interwoven iteration.

In their study, Çavuşoğlu *et al.* [19] created a novel chaos-based random number generator (RNG). They developed an S-Box generation algorithm and realized the performance tests of the S-Box. The proposed hybrid CS-AES methods are used to encrypt images. Examining the proposed CS-AES algorithm proved that this algorithm has higher security than AES and chaos.

Artuğer and Özkaynak [20] presented two algorithms to enhance the problem of nonlinearity values of chaos-based S-Box structures. The first proposed post-processing algorithm can improve nonlinearity values up to 111.5. Then, the second algorithm takes the S-Box optimized by the first algorithm as input, and the elements are replaced sequentially.

Logistic maps are the foundation of the algorithm that Arif *et al.* [21] suggested. Using the plaintext picture, the suggested approach creates a hash. This hash is then split into four parts, each of which serves as an initial parameter input for the logistic maps, which produce four arrays of pseudorandom numbers. The first and second keys are then used by the method to execute row and column permutations, respectively. The third key is used to conduct an exclusive or (XOR) operation on the resultant image. The final step is to use the fourth produced key to do a substitution on the image using either AES S-Box or AES reverse S-Box. Nevertheless, Arif *et al.* [21] suggested approach is ineffective in terms of encryption time.

Hua *et al.* [22] developed an image encryption scheme based on a 2D chaotic map. They created two matrices using a 2D sine-logistic map. The suggested approach randomly shuffles the image pixel positions using one of the created matrices by joining pixels in various rows and columns into circles and moving them within the circles. The technique then uses the pixel values of the resultant permuted image to perform row and column substitutions. The second matrix is used to repeat the diffusion and confusion steps.

Shariatzadeh *et al.* [23] suggested a new image encryption method dubbed dynamic AES, which combines the AES with the logistic chaotic map. The logistic map is used to generate the encryption key, which is then combined with the encryption data at different points in time. A customized variant of AES is used to utilize the processing power of Galois Field 28. The suggested approach outperforms many of the current image encryption techniques, according to experimental results, especially when it comes to defending against statistical and differential attacks. The ideal NPCR value, near-optimal UACI and entropy values, histogram analysis, and correlation of neighboring pixels validate the effectiveness and resilience of the suggested approach.

Alanezi *et al.* [24] offer an approach that involves using two chaotic maps: the plaintext picture is permuted using a logistic-sine map, and the permuted image is then substituted using a logistic-Chebyshev map. The algorithm creates the cypher image by performing an XOR operation on the replaced picture using a cascade of the two maps. Sherali [7] suggested an enhanced technique for data encryption and decryption. Since key sharing was a major issue with the symmetric technique, the author used ECC to produce the key and use it to encrypt and decode data using the AES. The proposed method is more secure than AES because it avoids the key-sharing problem that besets AES. It is also simpler than ECC and is only used for key generation, not data encryption or decryption.

## 2. THEORETICAL FRAMEWORK

### 2.1. Searchable encryption

SE is an innovative method that helps users search for encrypted data without revealing it. This method ensures the confidentiality of sensitive data, making it an important method in modern information security. SE combines the benefits of encryption with efficient searchability, without the need to decrypt the entire data for a query, this technique enables users to perform direct searches on encrypted information using algorithms designed exclusively for this purpose, this ensures that neither the owner of the information nor unauthorized persons can guess the underlying content or queries, Figure 1 illustrates the general structure of a SE system, it consists of three main entities: the data owner, the data user, and the cloud server. Data owner: the person who encrypts and indexes the data before sending it to the cloud server. Data user: the person who creates the trapdoor to allow the server to search through the encrypted data. Cloud server: the server stores the encrypted data and performs searches on the cloud using the trapdoor [25], [26].

SE techniques can be broadly divided into two categories: i) Symmetric searchable encryption (SSE): this method is typically used in scenarios where the data owner and the searcher are the same or share a high level of trust. It relies on symmetric keys, offering efficiency and simplicity for smaller-scale applications [5], [27]; and ii) Public-key encryption with keyword search (PEKS): PEKS is designed for scenarios where the data owner and searcher are distinct entities. It uses public-key infrastructure, allowing secure searches in environments where trust is limited [28], [29].

### 2.2. Overview of advanced encryption standard algorithm

The AES algorithm implements encryption and decryption processes on a 128-bit key length and uses the same key for both processes. AES performs 10, 12, and 14 rounds for 128, 192, and 256-bit keys, respectively. 128-bit block data are arranged in the array with size 4×4, also called a state. The AES transformations are explained as follows [30]–[32]: i) SubBytes transformation: an S-Box is used to replace each data block byte with another block according to a lookup table; ii) Shift transformation of rows: a transposition step where each row of the state matrix is given a cyclic shift by a certain number of steps; iii) Mix transformation of columns: a mixing multiplication process that is performed on the columns of the state matrix, combining the four bytes in each column; iv) Add round key transformation: XOR operation is performed between the new state matrix and the round key one; and v) Add round key transformation: each

byte of the state matrix is XORed with the round key. Using a key schedule, each round key is obtained from the cipher key. The final round consists of SubBytes, ShiftRows, and AddRoundKey.

### 2.3. Chaotic maps

The logistic map was first proposed by biologist Robert May in 1976, namely, a simple nonlinear polynomial mapping equation with degree 2. It is largely a discrete-time demographic model similar to the logistic equation first discovered by Pierre Francois Verhulst [33]–[35]. The following presents various types of chaotic maps.

#### 2.3.1. 1D logistic map

The logistic map is an effective and easy 1D chaotic map that has complicated chaotic behavior, and it can be defined by (1).

$$x_{n+1} = rx_n(1 - x_n) \quad (1)$$

Where  $x$  represents the current population's ratio to the greatest existing population, with a range  $[0, 1]$ , and  $r$  stands for a control parameter that has a range of  $[0, 4]$ . Only when  $r$  falls between  $[3.57, 4.0]$  can the logistic map exhibit chaotic behaviors; if  $r$  is greater than the range, the logistic map cannot exhibit chaotic behaviors [33]. The state and the area of a map's chaotic behavior can be objectively reflected in the bifurcation diagram. Figure 2 shows the logistic map's bifurcation diagram.

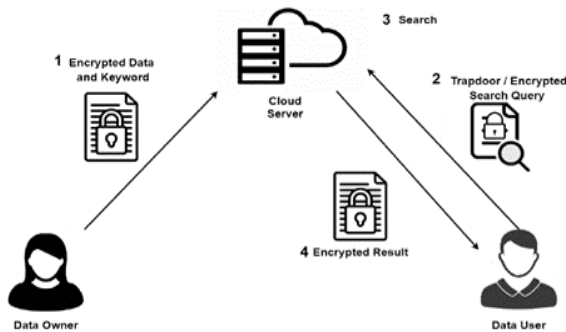


Figure 1. General structure of a searchable encryption scheme

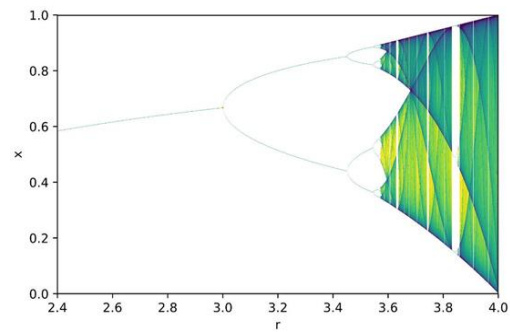


Figure 2. Bifurcation diagram

The 1D logistic map involves a single greatest Lyapunov exponent (LE), which establishes whether or not a map is chaotic. The map can be regarded as chaotic if the LE value is greater than zero and vice versa. As the LE value increases, the map's complexity rises as well. In (2) shows the LE for the 1D maps.

$$LM = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \quad (2)$$

Where  $f(x)$  denotes a 1D chaotic map and  $f'(x)$  denotes the derivative function of the function  $f(x)$ . The number of iterations of the chaotic map is  $n$ .

#### 2.3.2. Hénon map

Hénon [36] introduced the Hénon map, a 2D iterated map with chaotic solutions, as a simplified version of the Poincaré map for the Lorenz model [36]–[39]. The searchers use the 2D Hénon chaotic system as the secret key generation source because the 1D chaotic system is simple to break, and the high-dimensional chaotic system is extremely complicated and ineffective. Its definition is shown in (3) and (4).

$$x_{n+1} = 1 + y_n - ax_n^2 \quad (3)$$

$$y_{n+1} = bx_n \quad (4)$$

Where  $n=0, 1, 2, \dots$ , and  $a$  and  $b$  are bifurcation parameters for the classical Hénon map, have values of  $a=1.4$  and  $b=0.3$ . The Hénon map is the most general 2D quadratic map with the characteristic that the contraction is independent of  $x$  and  $y$ . The parameter  $b$  represents the rate of area contraction. For the Hénon map, there are bounded solutions over a range of  $a$  and  $b$ ; some lead to chaotic solutions [40].

### 3. METHOD

This section presents the procedure of the proposed data encryption algorithm to modify the AES algorithm using a chaotic map. The chaos method is utilized in the data encryption algorithm using the Hénon map to generate the AES key. The initial parameters of the Hénon map,  $a$  and  $b$ , are kept secret, which adds another layer of protection. This makes the proposed algorithm highly secure for encrypting private data, particularly in cloud environments. The proposed system comprises three phases,

- i) Sender phase
  - Generate the AES key using a 2D Hénon map: choose the initial values for the Hénon map parameters:  $a$  and  $b$ ; choose the randomly initialized values for the  $X_0$  and  $Y_0$  (the range between -1 to 1); apply the Hénon map (3) and (4) to compute the chaotic series; iterate the equations for 50 times; concatenate the values of  $x$  and  $y$  into a string; and apply a hash function like SHA-256 to generate the AES key.
  - Creating a searchable index that includes the keywords in a way that such keywords can be queried later.
  - The sender encrypts the searchable index using the proposed algorithm CHO-AES, shown in Figure 3, and a cryptographic hash function.
  - The sender encrypts the files using the same algorithm.
  - Uploads the encrypted searchable index and files to the cloud server.
- ii) Receiver phase
  - The receiver encrypts the trapdoor-based search using the proposed algorithm CHO-AES.
  - Send the generated trapdoor to the cloud server.
- iii) Cloud phase
  - The server searches on uploaded encrypted searchable index to compare the keyword and trapdoor.
  - If there is a match between the keyword and trapdoor, the server returns the relevant encrypted file to the receiver.
  - The receiver decrypts the relevant files using the inverse steps of the encryption algorithm.

The proposed data encryption algorithm CHO-AES is shown in Figure 3; this algorithm includes: i) generating the AES key using a 2D Hénon chaotic equation, ii) encrypting the files using modified AES, iii) creating a searchable index, and iv) encrypting and hashing the searchable index.

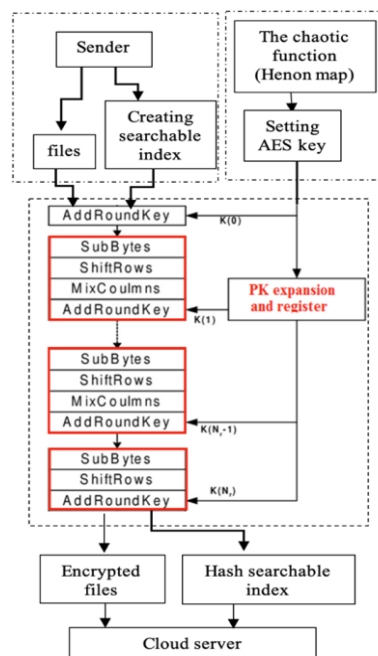


Figure 3. Proposed data encryption algorithm CHO-AES

### 4. RESULTS AND DISCUSSION

This section performs an evaluation study to analyze the performance of the proposed approach. Text and image files of different types and sizes are used for the test. We use the standard Mona Liza, Baboon, and Barbara images for color images. The suggested encryption algorithm's strength is evaluated by

conducting performance tests on multiple parameters. Visibility test, information entropy analysis, PSNR, NPCR, UACI, and correlation coefficient.

#### 4.1. Information visibility test

Figure 4 shows the visibility test using CHO-AES. The proposed encryption technique is applied in the standard Mona Liza image, Baboon image, and Barbara image, as illustrated in Figure 4(a), respectively. The results of the encrypted images, Figure 4(b), display the complete concealment of information.



Figure 4. Visibility test using CHO-AES of (a) plain images and (b) encrypted images of the plain images

#### 4.2. Information entropy analysis

Entropy analysis is a crucial parameter in image encryption that establishes the information's unpredictability. Excellent statistical randomness and information entropy characterize a secure encrypted image. It is observed that eight bits per pixel is the maximum entropy value for a grayscale image. For many previous studies, the entropy average value has ranged from 7.90 to 7.99. Table 1 illustrates that the information entropy of the encryption algorithms is close to 8.

Table 1. Entropy values for AES and proposed AES-CHO for different images

Image	Entropy	
	AES encryption	AES-CHO
Mona Liza	7.5635	7.5423
Baboon	7.4883	7.4851
Barbara	7.6373	7.6369

#### 4.3. Peak signal-to-noise ratio analysis

The encryption techniques can be assessed using the PSNR. The encrypted image is treated as noise, whereas the original plain image is treated as a signal in the computation of the PSNR. Lower PSNR values are anticipated for encrypted images. Let  $P(i, j)$  be the pixel value of the plain image and  $E(i, j)$  be the pixel value of the encrypted image at the location  $(i, j)$ . The MSE and PSNR between these two images are computed by (5).

$$PSNR = 20 * \log_{10} \left( \frac{255}{\sqrt{MSE}} \right) dB \quad (5)$$

Where MSE is the mean square error and is defined as (6).

$$MSE = \frac{1}{HW} \sum_{i=1}^H \sum_{j=1}^W (|E(i, j) - P(i, j)|)^2 \quad (6)$$

Table 2 shows low PSNR values, indicating that attackers will have difficulties extracting the plain image from the cipher image.

Table 2. Peak signal-to-noise ratio values for AES-CHO for different images

Image	PSNR for AES	PSNR for AES-CHO
Mona Liza	9.976301	9.302878
Baboon	8.764933	8.452932
Barbara	9.964285	9.853762

#### 4.4. Differential analysis

System sensitivity is a crucial security assessment aspect for image encryption algorithms against differential attacks. NPCR, which stands for the number of changing pixel rate, and UACI, for unified averaged changed intensity, are the most often used metrics for the above purpose. A high NPCR value means that the positions of pixels have been altered arbitrarily, and UACI values indicate that almost all pixel intensity values of the encrypted image have differed from their value in the plain image. Their definitions are as (7) and (8).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (7)$$

$$UACI = \frac{1}{W \times H} \left[ \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \quad (8)$$

Where  $W$  and  $H$  represent the image's width and height, respectively.  $C_1(i,j)$  and  $C_2(i,j)$  are the corresponding pixels of two images. If  $C_1(i,j) = C_2(i,j)$ , then  $D(i,j) = 0$ , otherwise  $D(i,j) = 1$ . The optimal values of UACI and NPCR are 33% and 99% respectively.

Table 3 illustrates the test percentage of NPCR and UACI for AES and the proposed algorithm, AES-CHO. The calculated NPCR and UACI values for AES-CHO are greater than 97% and 18%, respectively. As a result, the computed values for AES-CHO exhibit higher measurements than the AES. This indicates a clear distinction between the two algorithms, suggesting the effectiveness of the proposed encryption algorithm against differential attacks.

Table 3. NPCR and UACI values for AES and AES-CHO for different images

Image	NPCR for AES (%)	NPCR for AES-CHO (%)	UACI for AES	UACI for AES-CHO
Mona Liza	96.40	98.65	21.6599	23.4626
Baboon	96.63	97.45	17.3196	18.7651
Barbara	97.35	98.50	20.6834	22.8492

#### 4.5. Correlation analysis

Each pixel in a plain image containing visual content is typically highly associated with its neighboring pixels in the horizontal, vertical, and diagonal dimensions. Such correlations in neighboring pixels should not occur in encrypted images generated by a competent encryption technique. The correlation coefficient between neighboring pixels is computed using (9)-(12). The correlation coefficient  $r_{xy}$  between neighboring pixels  $x$  and  $y$  can be defined using the (9)-(12).

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (9)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (10)$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (11)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (12)$$

Where  $x$  and  $y$  are neighboring pixels,  $E(x)$  and  $E(y)$  are the mean values of  $x$  and  $y$ ,  $D(x)$  is the standard deviation for the mean,  $cov(x,y)$  is the covariance between neighboring pixels and  $r_{xy}$  is the correlation coefficient. Tables 4-6 present the calculated correlation coefficients between the original and encrypted

images for different images. As observed, there is a strong correlation between every two neighboring pixels in the original image. In contrast, the correlation coefficients for encrypted images are extremely near to zero. Therefore, the suggested method is resistant to statistical attacks.

Table 4. Correlation coefficients of neighboring pixels: Mona Liza

Direction of adjacent pixels	Plain image	Encrypted image
Vertical	0.937127	0.003745
Horizontal	0.964832	0.053981
Diagonal	0.918751	0.006301

Table 5. Correlation coefficients of neighboring pixels: Baboon

Direction of adjacent pixels	Plain image	Encrypted image
Vertical	0.953201	0.000742
Horizontal	0.963013	0.004329
Diagonal	0.944320	0.007273

Table 6. Correlation coefficients of neighboring pixels: Barbara

Direction of adjacent pixels	Plain image	Encrypted image
Vertical	0.874609	-0.001451
Horizontal	0.736188	-0.0016502
Diagonal	0.853092	-0.001284

#### 4.6. Comparison with some existing encryption algorithms

In terms of encryption execution time, the simple comparative analysis, using the Baboon image as a benchmark, reveals that the proposed AES-CHO outperforms existing techniques, as demonstrated in Table 7. The results show that while some researches offer robust security, it often comes at the cost of higher computational complexity. In contrast, the proposed AES-CHO maintains a balance between security and efficiency, making it more appropriate for real-time applications.

Table 7. Encryption time (in seconds) of the Baboon image for the proposed AES-CHO compared to different related works

	Proposed	[22]	[24]	[21]
Time(s)	0.1708	0.2338	0.3033	1.28

## 5. CONCLUSION

In this paper, to enhance the efficiency and suitability of AES for cloud computing, we propose a modified AES encryption utilizing a chaos system. The proposed scheme, AES-CHO, improves security by integrating the Hénon map's chaotic characteristics with the AES algorithm's robustness. The Hénon map generates unpredictable, pseudo-random keys, making it difficult for attackers to predict the key. Furthermore, using a cryptographic hash function ensures that the created keys are uniformly distributed and appropriate for the AES algorithm. The computed results shown in the previous section showed that security coefficients are already high, so the proposed approach can be adopted as SE to upload different images to the cloud server. According to statistical assessments, this method can protect the image against various attacks. The average entropy attained is 7.55477, not far from the optimal value, 8. The low PSNR values of all encrypted images show that it is difficult to distinguish encrypted from plain images. The NPCR and UACI values are close to their optimal values. Therefore, the present method was robust against differential attacks. Furthermore, the analysis results also showed the efficiency of the proposed method in significantly reducing the pixel correlation. Finally, the proposed AES-CHO achieves a lower execution time compared to existing approaches, making it more efficient and suitable for real-time and cloud computing applications. For future work, we can use other chaotic maps like the Lorenz system because of its higher level of security and nonlinear complexity compared to the Hénon map. Its strong sensitivity to initial conditions and chaotic dynamics makes it a promising technique for enhancing the security of encryption and secure communication systems.

## FUNDING INFORMATION

Authors state no funding involved.

## AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.



Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Fairouz Sherali	✓	✓		✓	✓			✓	✓	✓		✓		
Falah Sarhan			✓			✓	✓		✓	✓	✓		✓	✓

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review &amp; Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

## CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

## DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [FS], upon reasonable request.




## REFERENCES

- [1] P. Prajapati and P. Shah, "A review on secure data deduplication: cloud storage security issue," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 3996–4007, 2022, doi: 10.1016/j.jksuci.2020.10.021.
- [2] K. Sasikumar and S. Nagarajan, "Comprehensive review and analysis of cryptography techniques in cloud computing," *IEEE Access*, vol. 12, pp. 52325–52351, 2024, doi: 10.1109/ACCESS.2024.3385449.
- [3] Q. Zhang, M. Fu, Z. Zhao, and Y. Huang, "Searchable encryption over encrypted speech retrieval scheme in cloud storage," *Journal of Information Security and Applications*, vol. 76, 2023, doi: 10.1016/j.jisa.2023.103542.
- [4] A. Rajagopalan *et al.*, "Empowering power distribution: unleashing the synergy of IoT and cloud computing for sustainable and efficient energy systems," *Results in Engineering*, vol. 21, 2024, doi: 10.1016/j.rineng.2024.101949.
- [5] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 44–55, 2000, doi: 10.1109/secpri.2000.848445.
- [6] E. Roback and M. Dworkin, "First advanced encryption standard (AES) candidate conference-ventura, CA, August 20-22, 1998," *Journal of Research of the National Institute of Standards and Technology*, vol. 104, no. 1, 1999. [Online] Available: <https://www.proquest.com/openview/32c12ed15ad907640f7e0612a4beae20/1?cbl=48071&pq-origsite=gscholar>
- [7] F. Sherali, "A new approach for enhancing AES-based data encryption using ECC," *International Journal of Mathematics and Computer Science*, vol. 19, no. 1, pp. 229–235, 2024. [Online] Available: <https://future-in-tech.net/19.1/R-FairouzSherali.pdf>
- [8] R. M. Davis, "The data encryption standard in perspective," *IEEE Communications Society Magazine*, vol. 16, no. 6, pp. 5–9, 1978, doi: 10.1109/MCOM.1978.1089771.
- [9] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Computer Science*, vol. 78, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.
- [10] F. Sherali and S. Falah, "An efficient two factor user authentication and key exchange protocol for telecare medical information system," *International Journal of Mathematics and Computer Science*, vol. 15, no. 4, pp. 1015–1027, 2020. [Online] Available: <https://future-in-tech.net/15.4/R-Fairooz.pdf>
- [11] F. Mallouli, A. Hellal, N. S. Saeed, and F. A. Alzahrani, "A survey on cryptography: comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms," in *Proceedings - 6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 and 5th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2019*, 2019, pp. 173–176, doi: 10.1109/CSCloud/EdgeCom.2019.00022.
- [12] L. Li, "A novel chaotic map application in image encryption algorithm," *Expert Systems with Applications*, vol. 252, 2024, doi: 10.1016/j.eswa.2024.124316.
- [13] T. Umar, M. Nadeem, and F. Anwer, "Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage," *Expert Systems with Applications*, vol. 257, 2024, doi: 10.1016/j.eswa.2024.125050.
- [14] M. Alawida, "A novel image encryption algorithm based on cyclic chaotic map in industrial IoT environments," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 8, pp. 10530–10541, 2024, doi: 10.1109/TII.2024.3395631.
- [15] R. Li, T. Liu, and J. Yin, "An encryption algorithm for color images based on an improved dual-chaotic system combined with DNA encoding," *Scientific Reports*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-71267-9.
- [16] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, "Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home," *Electronics*, vol. 11, no. 7, 2022, doi: 10.3390/electronics11071083.
- [17] Z. Qiao, S. E. Assad, and I. Taralova, "Design of secure cryptosystem based on chaotic components and AES S-Box," *AEU - International Journal of Electronics and Communications*, vol. 121, 2020, doi: 10.1016/j.aeu.2020.153205.
- [18] E. Gokcay and H. Tora, "A novel data encryption method using an interlaced chaotic transform," *Expert Systems with Applications*, vol. 237, 2024, doi: 10.1016/j.eswa.2023.121494.
- [19] Ü. Çavuşoğlu, S. Kaçar, A. Zengin, and I. Pehlivan, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," *Nonlinear Dynamics*, vol. 92, no. 4, pp. 1745–1759, Jun. 2018, doi: 10.1007/s11071-018-4159-4.
- [20] F. Artuğer and F. Özkaynak, "A new post-processing approach for improvement of nonlinearity property in substitution boxes," *Integration*, vol. 94, 2024, doi: 10.1016/j.vlsi.2023.102105.
- [21] J. Arif *et al.*, "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, pp. 12966–12982, 2022, doi: 10.1109/ACCESS.2022.3146792.
- [22] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Chen, "2D Sine logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015, doi: 10.1016/j.ins.2014.11.018.




- [23] M. Shariatzadeh, M. J. Rostami, and M. Eftekhari, "Proposing a novel dynamic AES for image encryption using a chaotic map key management approach," *Optik*, vol. 246, 2021, doi: 10.1016/j.ijleo.2021.167779.
- [24] A. Alanezi *et al.*, "Securing digital images through simple permutation-substitution mechanism in cloud-based smart city environment," *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/6615512.
- [25] F. S. Ali and S. Lu, "Searchable encryption with conjunctive field free keyword search scheme," *2016 International Conference on Network and Information Systems for Computers (ICNISC)*, pp. 260–264, 2016, doi: 10.1109/icnisc.2016.064.
- [26] H. B. How and S. H. Heng, "Blockchain-enabled searchable encryption in clouds: a review," *Journal of Information Security and Applications*, vol. 67, 2022, doi: 10.1016/j.jisa.2022.103183.
- [27] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A survey of provably secure searchable encryption," *ACM Computing Surveys*, vol. 47, no. 2, 2014, doi: 10.1145/2636328.
- [28] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3027, pp. 506–522, 2004, doi: 10.1007/978-3-540-24676-3\_30.
- [29] F. S. Ali, H. N. Saad, F. H. Sarhan, and B. Naaem, "Enhance manet usability for encrypted data retrieval from cloud computing," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 1, pp. 64–74, 2019, doi: 10.11591/ijeecs.v18.i1.pp64-74.
- [30] M. S. Ummah, "Advanced encryption standard (AES)," *Sustainability*, vol. 11, no. 1, pp. 1–14, 2019, doi: 10.6028/NIST.FIPS.197.
- [31] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, vol. 16, no. 1, 2017.
- [32] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric encryption algorithms: review and evaluation study," *International Journal of Communication Networks and Information Security*, vol. 12, no. 2, pp. 256–272, 2020.
- [33] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017, doi: 10.1016/j.sigpro.2017.03.011.
- [34] R. L. Devaney, *An introduction to chaotic dynamical systems*. New York, USA: Chapman and Hall/CRC, 2021.
- [35] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019, doi: 10.1109/ACCESS.2019.2893538.
- [36] M. Hénon, "A two-dimensional mapping with a strange attractor," *Communications in Mathematical Physics*, vol. 50, no. 1, pp. 69–77, Feb. 1976, doi: 10.1007/BF01608556.
- [37] M. A. Lone and S. Qureshi, "A security algorithm for images based on 2D logistic map using bit-level and pixel-level image encryption approaches," *International Journal of Computing and Digital Systems*, vol. 14, no. 1, pp. 633–641, 2023, doi: 10.12785/ijcds/140148.
- [38] A. Salim, K. A. Mohammed, F. M. Jasem, and A. M. Sagheer, "Image steganography technique based on Lorenz Chaotic system and bloom filter," *International Journal of Computing and Digital Systems*, vol. 16, no. 1, pp. 851–859, 2024, doi: 10.12785/ijcds/160161.
- [39] S. Niu, R. Xue, and C. Ding, "A dual image encryption method based on improved Hénon mapping and improved logistic mapping," *Multimedia Tools and Applications*, vol. 11, no. 1, pp. 1–14, 2024, doi: 10.1007/s11042-024-19157-0.
- [40] D. Singh, S. Kaur, M. Kaur, S. Singh, M. Kaur, and H. N. Lee, "A systematic literature review on chaotic maps-based image security techniques," *Computer Science Review*, vol. 54, 2024, doi: 10.1016/j.cosrev.2024.100659.

## BIOGRAPHIES OF AUTHORS



**Fairouz Sherali**    is an Associate Professor at the Department of Computer Science, Kufa University, Iraq. She received her Ph.D. in information security from Huazhong University (HUST) in 2017. Her main teaching and research interests include developing Searchable encryption algorithms in cloud computing. She has published several research articles in International Journals of Mathematics and Computer Science. She can be contacted at email: fairouz.m.jaafar@uokufa.edu.iq.



**Falah Sarhan**    is an Associate Professor at the Department of Mathematics, Kufa University, Iraq. He received his Ph.D. in numerical analysis from Huazhong University (HUST) in 2017. His main teaching and research interests include numerical analysis, functional analysis, and applied mathematics. He has published several research articles in International Journals of Mathematics and Computer Science. He can be contacted at email: falahh.sarhan@uokufa.edu.iq.