



RESEARCH ARTICLE - COMPUTER SCIENCE

Chaotic Image encryption using Arnold's cat map and mod function with an auxiliary image key

Hind Jumaa Serteep^{1*}

¹ Department of computer science, Education College, Mustansiriyah University, Baghdad, Iraq

* author E-mail: hind_2018@uomustansiriyah.edu.iq

Article Info.	Abstract
<i>Article history:</i> Received 8 may 2025 Accepted 18 August 2025 Publishing 30 September 2026	This paper introduces a novel image encryption and decryption approaches depending on a hybrid chaotic system that merge Arnold's cat map (ACM) with additional security layers. The proposed solution merge modulo operation and XOR functions applied to and auxiliary pictures to improve overall security level. The performance indicators are used to assess the algorithm's effectiveness such as Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and entropy. Experimental indicating high randomness and security robustness where the results show that the proposed algorithm achieves an average values of MSR about 17706 and the PSNR is about 35 db while the entropy exceed 7.3 bits per pixel Showing her ability to resilience to brute-force and statistical attacks. The security has been enhancing by the method's wide key space and high sensitivity to minor changes to the keys, making it a strong choice for secure image communication.
This is an open-access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/) <i>The official journal published by the College of Education at Mustansiriyah University</i>	
Keywords: Image encryption, Image decryption, Arnold cat map (ACM), Chaotic map, entropy, XOR function	

1. Introduction

In our current era, are stand on a huge requisition for instant content and real-time secure image and video transfer as a result of fascinating evolution in multimedia processing and network communication via internet and any wireless means [1]. For maintain the frequent flow of digital Multimedia and to overcome the challenges associated with it, various encryption algorithms were proposed and developed by computer and software specialists, these algorithms were find to secure Multimedia that depicting sensitive information like medical records, fingerprints and satellite Images [2]. In such an open environment, many security concerns. Related to the process and transmission of digital images are raised, Therefore the confidentiality and integrity of the image should be confirmed, there are several approaches to encryption algorithms. The one that uses a single key for both encryption and decryption while ensuring secure key distribution between the sender and receiver is known as symmetric key algorithms [3]. Another approach where two secret keys used, the first key is for encryption which is called the public key and the other one for decryption which is called the private key, this approach is good to be used in safe data transfer over unsecure channels and no required to share a secret key this approach is called asymmetric encryption [4]. The third approach, which is to use both symmetric and asymmetric encryption, is known as hybrid encryption, where the actual data is encrypted by a symmetric algorithm; however, the asymmetric algorithm encrypts the secret key of the symmetric algorithm [5].

The process of protecting information from uncontrolled access is called encryption, which is the transformation of plain data into cipher data, and that is for ensuring the data's confidentiality and not revealing it to unwanted parties. An encryption phasing delay when processing large data such as digital images or videos in real-time applications in such scenarios, a computationally intensive approach is necessary [6]. Chaos-based algorithms have had particular study of their exposure to stunning properties, which are a combination of high security, complexity, speed, reasonable computational overhead, and power [7]. Chaotic systems possess another excellent feature for data encryption, such as good pseudo-random performance and sensitivity to initial conditions [8]. Chaos-based data encryption was first initially suggested by Robert Matthews in 1989. Since then, scientists have investigated the characteristics of chaotic systems and how they transition from orderly to chaotic states [9].

Images share many innate characteristics, including high correlation among pixels and bulk data capacity [10], and during the pressure of online communication, some conventional encryption algorithms such as RSA, DES, and IDEA, which are proper for encrypting text data, face difficulty to encrypting images while chaos-based algorithms can handle such tasks efficacy showing fast and highly secure Image encryption [11]. If any dynamic system has the following features, it can be classified as chaos.

- (i) sensitive to initial condition.
- (ii) topological in mixing state.
- (iii) dense for periodic orbits.

Image encryption depending on chaos has attracted more attention since the pioneer work adding to those desired results of broadband, noise-like and difficult to predict nominating the most complex dynamic nonlinear system is chaotic behavior [12].

2. Overview of the Arnold's Cap Map Chaotic System

There are two main phases for construction of a chaos-based picture cryptosystem, the confusion phase and the diffusion phase [13]. The scientific facts show that the might of the chaos-based cryptosystem based on these two phases, where pixels locations and values are alternated by those two phases, the diffusion phase is responsible for altering the values of the pixels, while the confusion phase deals with the positions of the pixels throughout the image [14], each phase has its own algorithm where the diffusion phase use various algorithm that transmit of a secret image such as chaotic XOR operation or modular arithmetic, while the confusion phase uses a different algorithm like (ACM) and 2D- Henon map and another chaotic map approach's [15].

Researchers in encryptions algorithms get simplicity and speed when the image is encrypted using only one chaotic algorithm but they face a number of drawbacks such as limited key space which makes brute force attacks more feasible [16], and the encryption algorithm is more vulnerable when attackers gain access to both the plaintext and cipher text using the known plaintext attacks, this scenario usually limits its application to a specific use and when high security is not the main need.

3. Overview of the used methods.

Regarding respect for chaos-based image encryption algorithm, there are two stages confusion and diffusion. On which such encryption methods depend. A confusion phase utilizes a chaotic maps behavior which it has disorderly and random results but in facts it follows a specific pattern that manage by mathematical equations that are sensitive to any changes in initial conditions [17]. (ACM) will be used as confusion phase which it proposed by a Russian Mathematics Specialist Vladimir Arnold [18]. Where it is suitable for scrambling by changing the position of the image pixels, which it done by multiply each pixel coordinate (x, y) by a matrix to obtain the new pixel coordinate. (ACM) required image size to be of (N x N). See equation (1) below.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \bmod N \quad \dots\dots\dots(1)$$

Where

$x, y, x', y \in \{1.2.3.\dots\dots\dots N\}$

a, b: positive integer

where the image dimensions contribute to finding the new pixel's locations by modular arithmetic modulo N, the pixels changing Location process is periodic and after repeating this process certain time number the original image can be restore so this process should be stoped after the new pixel's location is far enough from the original Location achieving the lowest correlation between pixels [19] [20].

Early in the 19th century the mathematical specialist Carl Fridric Gauss presented the idea of the modulo operation in his book *Disquisitiones Arithmeticae*, the modulo value can be determined when a number is divider by another, the remainder from this operation is known as modulus, beside these benefits it's help in another different fields, such as Hashing and hashing table, Error detection and Cryptography.

3.1. The Features of Arnold Cap Map

- 1- Unpredictability: (ACM) has chaotic behavior where it produces a significantly different outcome due to small changes in initial conditions and this is very desirable in encryption and scrambling application.
- 2-The (ACM) has good performance in image scrambling in image processing field, because it alters an image to make it seem random, it may be used for encryption and safe visual data transfer.
- 3-Data recovery applications: The reversible transformation of (ACM) is one of its main benefits, it is possible to return the scrambling image to its original state after specific number of iteration. Application involving data recovery and cryptography benefit greatly from this feature in the controlled environments or educational demonstrations.
- 4- Arnold's Cat Map is mathematically easy to create using simple matrix operations.
- 5- The Arnold's Cat Map (ACM) provides effective diffusion in cryptographic application, ensuring that the scrambling process influences every pixel across the entire image. This enhances security by thoroughly concealing the original structure of the image.

Despite its strengths in unpredictability, ACM has several limitations in cryptographic and image-processing applications:

Periodicity, Restriction to Square Images, Limited to 2D Systems, Computational Overhead for Large Data.

4. The proposed Method

For resolving some of the problems mentioned in the third part above and enhancing the (ACM), the following method has been proposed which it consists of two main stages, First stage represents the confusion where it done by applying (ACM) to the original image and stop at certain iteration number (this iteration number consider as secret key K5), secondly, is the diffusion stage which it done by selection of an auxiliary image as an encryption key and the encryption process is done by applying (ACM) and stopped at certain iteration (this iteration number consider as secret key K6) than apply modulo function between pixels values of image resulted from first stage (as the dividend) and the pixels values of the auxiliary image (as the divisor)

4.1. Encryption Algorithm

Inputs: - Original Image O1, Auxiliary Image A1, (ACM)Keys (K1, K2) for original, image Arnold Map Keys (k3, k4) for Auxiliary Image.

Output: - Encryption image size (n x 2n)

Step1: - Apply (ACM)for both Original Image (O1) and auxiliary image A1, and for original image will stop at iteration (K5) and for auxiliary image stop at iteration (K6), both (K5, K6) are positive integer considered as keys for iterations.

Step 2: - Spread the three color channel (Red, green, blue) for the Images (O1, A1) that result from step 1

Step 3: - Apply the Modulo function between each pixel in the individual color channel of the Image (O1) and the pixels of (A1) Image until last pixel of the (O1) to create image (O2)

Step 4: - Apply (XOR) function between the individual pixel value result from step 3 (image O2) and the pixel for auxiliary image (A2) , then combine the (RGB) channel to create (R image)

step 5: - Calculate the round times value for each pixel of the original Image (O1) by the following equation (2) and create Image (T1) that its pixel's value equal to Round time value(T1).

$$T1 = (O1 - M)/A2 \dots\dots\dots (2)$$

Where

O1: Pixel value of the original image.

M: Modulo value result from step 3.

A2: Auxiliary image (A2) pixels value.

step 6: Merge the two images (R image from step 4) and (image T1 from step 5) (one beside one) to create the final result image (R1) with size (n x 2n).

Step 7: Send the result image to the receiver.

Regarding the encryption algorithm, see Fig. 1, where the flowchart is demonstrating the keys used in the encryption process, and they are listed as follows.

I: K1, K2: (ACM)Keys for Original Image which are the positive integer a, b equation 1

II: K3, k4: (ACM)Keys for Auxiliary Image which are the positive integer a, b equation 1

III: K5: Iteration No. for original Image

IV: K6: Iteration No. for Auxiliary Image

V: A1 Auxiliary image.

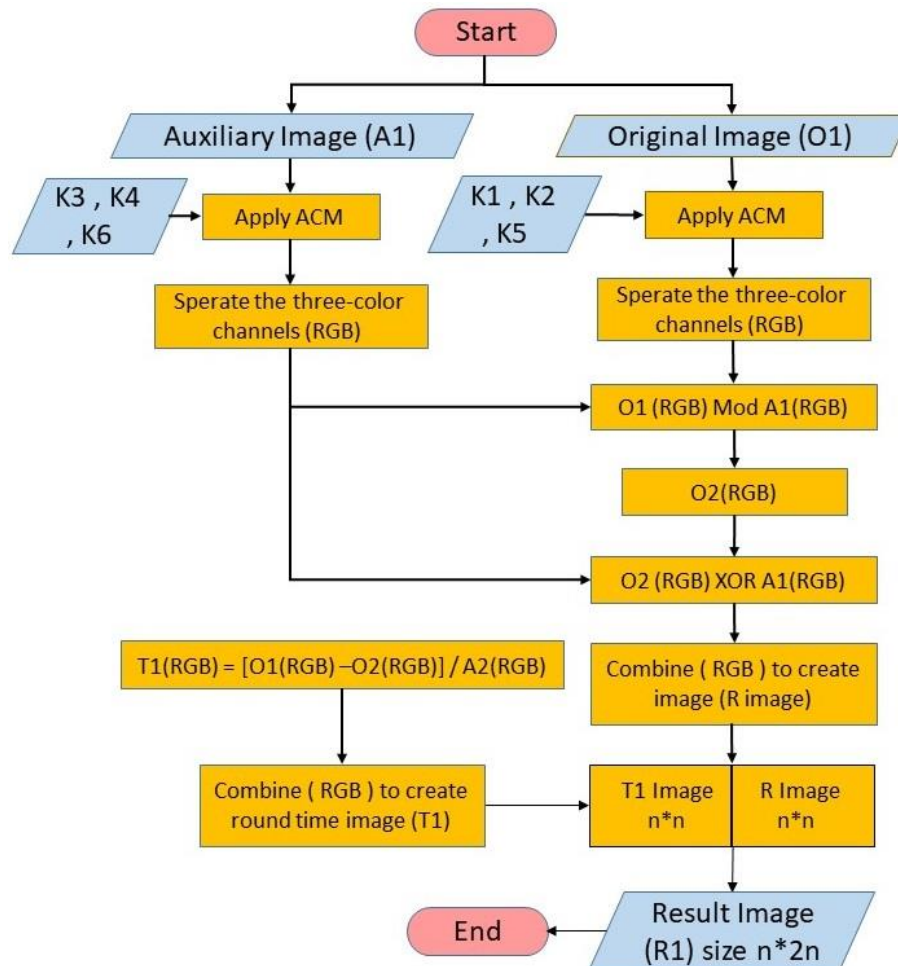


Figure. 1: Flow chart of the encryption algorithm

4.2. Decryption Algorithm

In order to obtain the original image (O1) at the receiver end, the following decryption algorithm must be applied, assuming the encryption keys described above have been send security from the sender to receiver.

Input: result image (R1) with size (n x 2n)

Output: Original Image O1

Step1: Separate the result Image (R1) with size (n x 2n) in to two halves, the first half represent the (R image) and the second half represent Round Time Image (T1)

Step2: Apply (ACM)for the Auxiliary (A1) Image using (K3, K4) as keys and K6 as Iteration key

Step3: Apply (XOR) function between the Image (R image) pixel values and the pixel's values of the auxiliary image A1 that result from step 2

Step4: - Apply the following equation (3) for obtain the original image

$$O1 = (A1 * T1) + O2 \dots\dots\dots (3)$$

Where:

O1: Original image pixels' value before (ACM)

A1: Auxiliary image pixels' value

T1: Round time image pixels' value

R: Pixels value of (R image)

Step 5: Apply (ACM) for the Original Image (O1) using K1, K2 as (ACM) key and K5 as an iteration to obtain the original image.

In order to successful image recovery at the recipient end, the flowchart illustrates in Fig. 2 provides a clear visualization of the decryption steps.

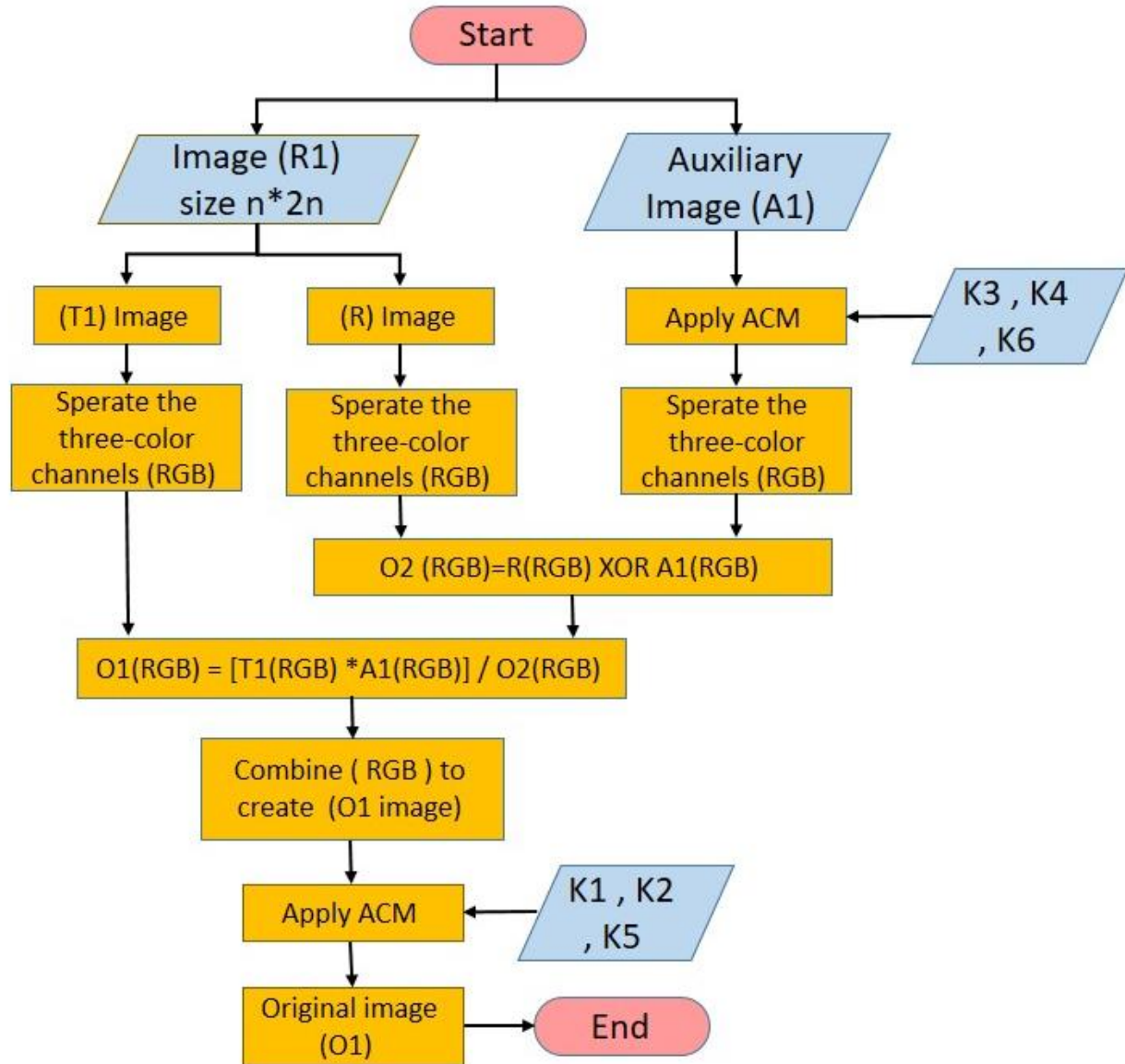


Figure 2: Flow chart of the decryption algorithm

5. Result and Discussion

The confusion-diffusion architecture is used as key base for many image encryption procedures, the outcomes of the undertaken proposed algorithm are presents in this section where the algorithm effectiveness are evaluated, for that four digital images with size of (512 x 512) are candidate as plain images (original images) and another four digital images with size of (512 X 512) as auxiliary Images as shown in Fig.3 below.

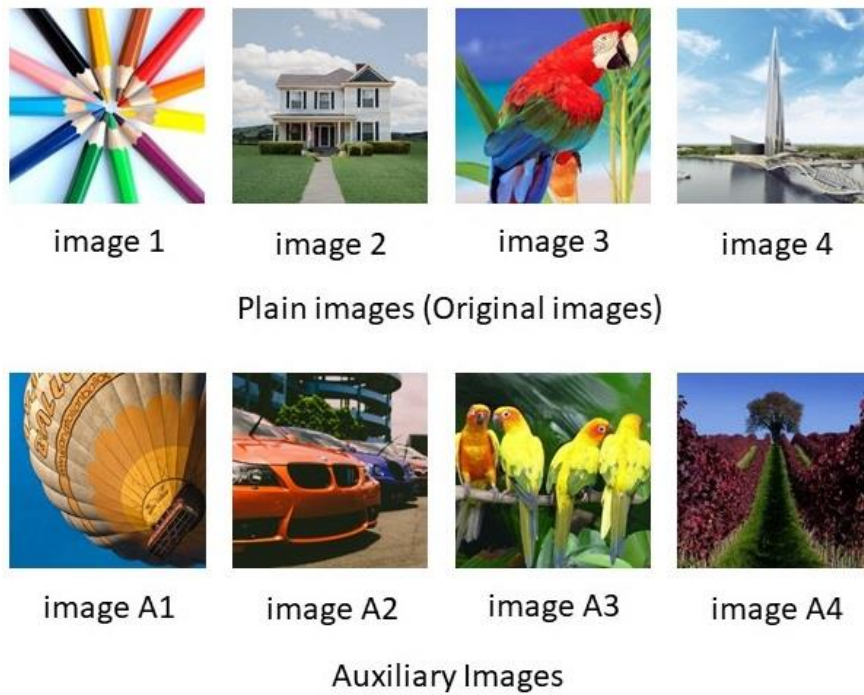


Figure 3: Set of plain and auxiliary images

In Fig. 4 below, it shows a set of encrypted images result from using the encryption algorithm where applying different iteration at plain image (image1) by (ACM) while the Auxiliary Image (A2) iteration Stay fixed at 50.

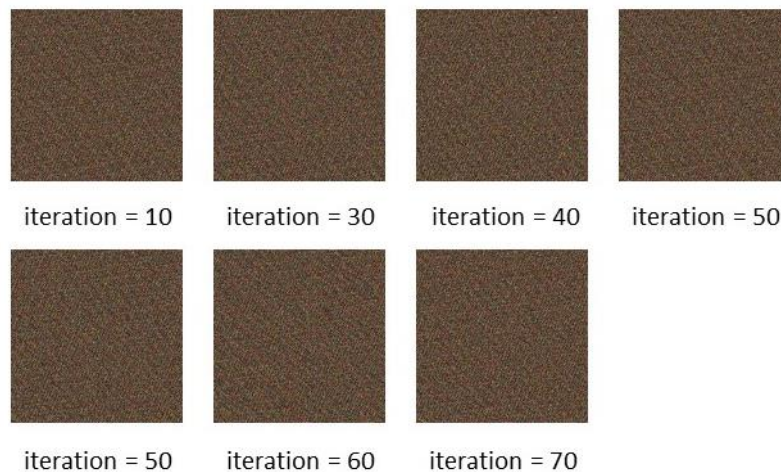


Figure 4: Set of result image

Visually, there is no indication of the original image's content or any significant information in the encrypted image at first glance, and there are no discernible patterns.

For evaluate the performance of the encryption algorithm there are several metric achieving this propose such as Mean square error (MSE), Peak signal to Noise ratio (PSNP) and Entropy (H).

Randomness and unpredictability are feature of encryption algorithms which the entropy give the uncertainty amount in the data, a maximum value obtained or close to maximum occur when the intensities of pixels are uniformly distributed and completely random. Making the decrypt the cipher image very difficult without using the correct encryption Keys.

Another metric is used in the evaluation process which it the mean square error (MSE) where it indicates the amount of different between the original Image and the encrypted Image, this different result from the quantity of distortion inserted in the original image. A strong encryption produces high MSE value and vice versa low MSE value indicate poor encryption.

With the above Metric used, The Peak Signal to noise Ratio (PSNR) also help in evaluation of the encryption algorithm, a strong encryption algorithm is considered when the value of PSNR is low result from large difference between original and encrypted Image. (Usually good performance

when $PSNR < 10$ db.) and vice versa when the value of PSNR exceed 30 db comes from low distortion in the encrypted image that indicate bad performance of encryption algorithm.

Table (1) below show the three metric mentioned above where the original Image 1 encrypted at different iteration and auxiliary image (A2) used in with fixed iteration at (50).

Table1: The MSE, PSNR and Entropy of encrypted image 1

Iteration of image 1	MSE	PSNR	Entropy
10	22117.683	4.683	7.4472
30	22116.733	4.683	7.4476
40	22104.004	4.686	7.4517
50	22114.881	4.683	7.4473
60	22086.647	4.689	7.4458
70	22116.647	4.683	7.4431
80	22109.492	4.685	7.4447

as seen in the above table when get high value (More than 5000) of MSE and low PSNR (less them 10) beside. the entropy value near maximum value, all that indicate good performance of encryption algorithm

table (2&3) below show the result of the MSE, PSNR and the Entropy for all original image encrypted by the proposed algorithm with using of all auxiliary images where the iteration is stopped at (10) for both original and auxiliary images.

Table2 : the MSR, PSNR and Entropy of encrypted image 1 &2

	original Image 1			original Image 2		
	MSE	PSNR	Entropy	MSE	PSNR	Entropy
auxiliary Image A1	17706.387	5.649	7.7918	11278.48	7.608	7.7933
auxiliary Image A2	22133.35	4.68	7.4217	14486.933	6.521	7.4522
auxiliary Image A3	20484.666	5.016	7.461	13559.728	6.808	7.4412
auxiliary Image A4	23337.987	4.45	7.2919	15256.388	6.296	7.2956

Table3: the MSE, PSNR and Entropy of encrypted image 3 & 4

	original Image 3			original Image 4		
	MSE	PSNR	Entropy	MSE	PSNR	Entropy
auxiliary Image A1	11038.61	7.701	7.8409	15726.217	6.164	7.778
auxiliary Image A2	12390.347	7.199	7.4737	20567.637	4.9989	7.4251
auxiliary Image A3	11659.112	7.464	7.5245	18860.962	5.375	7.4534
auxiliary Image A4	12927.817	7.015	7.2585	20964.736	4.915	7.2785

5.1 Comparison with previous works

In the field of chaotic image encryption this is a comparison presentation of the propose method with other related works, beginning with Subashini (2018) work , which proposed a new version of Arnold's cap map by combining interweaving and shearing to increase complexity [18],

The second article used in comparison done by K. K. Sud (2020) where the authors produce a novel technique to encrypt image using chaotic map to achieve security , their technique scramble image pixels effectively by unpredictably nature of chaos theory [21].

Our proposed algorithm also compared with the method created by N. K. Pareek et al (2006), their method utilized a combination of two logistic map with an 80 –bit external secret key , the pixels of the image are encrypted by pseudo-random sequences that are created by the chaotic maps[7].

Below tables show the comparison between the proposed algorithm and the previous work [18.21.7], the comparison is made based on the aspects of Encryption technique , Use of Auxiliary Data , Key Space and sensitivity , Resistance to Attacks and Performance Indicator.

Table 4: Comparison based on Encryption Technique

Proposed algorithm	Hybrid chaotic system consists of Arnold's cat map (ACM) , modulo, XOR , and auxiliary image key
Reference # 21	Using high-dimensional chaotic system s for chaotic map-based permutation and diffusion
Reference # 7	Directly uses chaotic map (Like the logistics map) for pixel shifting and value changes
Reference # 18	Present as an updated version of the Arnold's cat map (ACM) this improve security and pixel shuffling

Table 5: comparison based on Use of Auxiliary Data

Proposed algorithm	Yes, increase security and key sensitivity by using an auxiliary image key for dissemination.
Reference # 21	No, it mostly uses parameters and chaotic maps
Reference # 7	No, primarily depend on chaotic maps avoiding auxiliary image
Reference # 18	primarily suggests a transformation of ACM; auxiliary images not emphasized

Table 6: comparison based on Key Space and sensitivity

Proposed algorithm	A large key space results from many factors and significant sensitivity caused by small key changes
Reference # 21	Large key space, highly sensitive to parameter changes
Reference # 7	Depends on initial chaotic map parameter; limited key sensitivity because of fewer parameters
Reference # 18	Aims to improve security by increasing key sensitivity

Table 7: Comparison based on Resistance to Attacks

Proposed algorithm	high entropy and key sensitivity caused resistance brute-force , statistical and differential attacks
Reference # 21	Made to withstand statistical and differential attacks
Reference # 7	susceptible to statistical and known-plaintext attacks, bounded security features
Reference # 18	increases unpredictability of the chaotic map , making cryptanalysis more challenging

Table 8: compassion based on Performance Indicator

Proposed algorithm	High entropy (more than 7.3 bits/pixel) , MSR , PSNR , secure diffusion
Reference # 21	NIST randomness tests, PSNR , and entropy (values vary)
Reference # 7	Standard measures demonstrate effective scrambling but less focus on information entropy or robustness
Reference # 18	Emphasizes transformation properties to improve pixel randomness and reduce correlation, indirectly impact metrics

6. Conclusion

In order to ensure the security and confidentiality of images during their massive use in communications, which is a critical issue, an improvement to the (ACM) has been proposed to achieve this goal, to evaluate the algorithm, MSE, PSNR and Entropy are calculated of the result images, the numbers shown in tables (1,2,3) above show that the algorithm has good performance where the entropy is more than 7.2 and MSE is more than 5000 and the PSNR is less than 10. A large key space also contributes in the strength of the algorithm which it a combination of integer number and an image.

References

- [1] Sahar MazaLoom, Amir Masud Eftekhari, Moghadam, "color image encryption based on Coupled Nonlinear chaotic Map," *Chaos, Solitons & Fractals* , Vol. 42, Issue 3, pp. 1745-1754 , 15 Nov. 2009,
- [2] Marwa Tarek ELkandoz, Wassim Alexam, “ Image encryption based on a combination of multiple chaotic map, “ *Multimedia Tools and Application, Springer Link*, Vol. 81, pp. 25497-25518, 23 Mar 2022.
- [3] 3-Suha Husam Jasim , Haider Kadhim Homood , Khalid Ali Hussein , “Hybrid Algorithm (DES- Present) for encryption color image using 2D-Chaotic System,” *Mustamsiryah Journal of pure and applied sciences* , Vol.3 , No.1 , pp 49 -63. 2025
- [4] M. E. Hellman, “An overview of public key cryptography,” *IEEE Communications Magazine*, Vol. 40 , Issue 5 , pp 42-49 , 01 May 2002.
- [5] Qixin Zhang, “An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption ,” *Conference: 2021 2nd International Conference on Computing and Data Science (CDS)* , 28-29 January 2021.
- [6] Mohammed Dhiaa Elden Taha, Khalid Ali Hussein, “An Image Encryption Method Using Six-Dimensional Hyper Chaotic System and RC6,” *Mustamsiryah Journal of pure and applied sciences*, Vol 3 , No.1 pp. 1-11, 2025 ,
- [7] N.K. Pareek, Vinod Patidar, K.K. Sud, " Image encryption using chaotic Map,” *Image and Vision Computing*, Science Direct, Vol. 24, Issue 24, pp. 926-934, 1 Sep 2006.
- [8] Sadiq A. Mebli, Abid Ali H. Alta'ai, Salim Ali Abass, "A novel chaotic System for color Image Encryption, “*Mustansiriyah Journal for Sciences and Education*", Vol. 2, pp. 1-11, 2022.
- [9] Bowen Zhang, ling feng Liu, " Chaos-Based Image Encryption: Review, Applica, and Challenges,” *Chaos-Based Secure communication and Cryptography*, Vol. 11, Issue 11, pp. 1-39, 5 June 2023
- [10] A. Jolfaei and X. Wu, "Security analysis of image encryption using chaotic logistic map," *2013 International Conference on Signal Processing and Multimedia Applications (SIGMAP)*, Reykjavik, Iceland, pp. 1–7 , 2013,

- [11] Wang Xing-yuan, Yu Qing. "A block encryption algorithm based on dynamic Sequence of Multiple chaotic system, " *Communication in Nonlinear Science and Numerical Simulation*, Vol. 14. Issue-2, pp. 547- 581, Feb 2009.
- [12] F. Anstett; G. Millerioux; G. Bloch, " Chaotic Cryptosystem ; cryptanalysis and identifiability," *IEEE Transactions on circuits and system*, Vol. 53 , Issue 12 , pp. 2673-2680 , 11 Dec 2006.
- [13] U. Zia, M. McCartney, B. Scotney, J. Martinez A. Tair, J. Maman, A. Sajjad," Survey on Image encryption techniques using chaotic maps in spatial. Transform and spatiotemporal domains " , *International Journal of information Security, SPRINGER Link*, Vol. 21, pp. 917-935, 7 April 2022.
- [14] A. Hilmi, S. Me 2 rour, A. EL Oyalkadi, "An Image Encryption Based on confusion- diffusion using Two chaotic Maps and Frobenius Endomorphism," *SALEE Africa Research Journal, SAIIEE South Africa Institute of Electrical Engineers* , Vol. 114 .4, pp. 98-105, Dec. 2023
- [15] Mohammed Mazyad Hazzazi, Mujeeb ur Rehman, Arslan shafique, Amer Aljaedi, Zaid Bassfar and Aminu Bello Usman," Enhancing Image security via chaotic maps, Fibonacci, Tribon acci. transformations, and DWT diffusion, a robust data encryption approach," *Scientific Reports*, Article number 12277 (2-24) , pp. 1-23
- [16] M. Khan and T. Shah, "A literature review on image encryption techniques based on chaotic maps," *International Journal of Computer Applications*, vol. 975, no. 8887, pp. 1–7, 2014.
- [17] M. Riyadh, S.A. Alrubaie, D. Riadh Alshibani, "Text Encryption Based on Biological Operation in chaotic Image Hiding," *Mustansiriyah Journal for Sciences and Education* " , Vol. 23, Issue 2, pp. 1 - 11 , 4/30/2022.
- [18] V.d. Subashini, S. Poornachandra, "A New Transformation for chaotic Image Encryption based on the Arnold Cap Map, " *Applied Mathematics & Information Sciences*, Vol. 12, Issue 4, pp. 797- 805, Jul 2018.
- [19] M. Turan, E Gokcay, H. Tora, " An unrestricted Arnold's cat map transformation", *Multimedia Tools and Applications*, Vol. 83, pp. 70921-70935, 06-Feb-2024.
- [20] Atheer J. Mansoor, Hikmat N. Abdullah, Hadi T. Zeboom, "Image Encryption Method Based on Image Dimension Transformation Using Chaotic Flow Systems," *Opcion Ano 35 ,Especial N° 20*, Vol. 35, Special Edition No.20 , pp. 2899-2921 , 2019.
- [21] K. K. Sud , Vinod Patidar , "Chaotic Map-Based Image Encryption with High Security " , *IEEE Access* , Vol. 8 , pp. 179136 – 179148 , November 2020