Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

Chaotic-Maps Based Low Complex Image Encryption for Secured Drone Deliveries

Siva Ganesh Golla[1], Hari Krishna Kanneboina[2], Krishna Veni Challa[2]

[1]- Assistant Professor, School of Avionics, Institute of Science and Technology, JNTUK, Kakinada

[2]- Assistant Professor, Department of Electronics and Communication Engineering, University College of Engineering, JNTUK, Kakinada

E-mail – sivaganeshgolla@gmail.com, hari412.k@gmail.com, krishnaveni.challa.486@gmail.com

Article History:

Received: 12-01-2025

Revised: 15-02-2025

Accepted: 01-03-2025

Abstract:
Earlier, the military used drones for various defence purposes only. But now their usage has been dramatically extended for packages deliveries to civilians by e-commerce companies. Companies must ensure proper deliveries to save their resources and ensure customer retention. This tendency prompts the drone system to capture the customer's image and transmit the same to the database for authentication and proper delivery. It resulted in the emergence of cryptosystems that ensure the secured transmission of the captured data during delivery by employing the technique of encryption. Previous researchers identified several crypto techniques, of these AES, DES, Triple DES, and RSA are reliable for textual data but not for multimedia data. Against this backdrop, there is a need for the development of a computationally low complex, easy to implement, less energy-consuming, and attack-resistant crypto technique that even works on a limited processing capacity platform and ensures secured transmission of sensitive information through drones.

Aimed to develop a novel technique that addresses the problems of complexity and computational cost, this study designed a chaotic-maps based cryptosystem where the confusion process employs a Tent map and the diffusion process a Henon shuffling. The study conducts image encryption on different input images and verifies the robustness of the designed technique using standard approaches like statistical analysis, differential attack analysis, information entropy, time analysis, and the key-analysis.

Keywords: Drone, Cryptosystem, Chaotic-maps, Tent map, Henon shuffling, Image Encryption.

1. Introduction

A drone is an unmanned aerial vehicle (UAV) navigated by the Ground Control Station (GCS) or an on-board system. Unlike a conventional airplane, the drone is composed of sensors, is small and lightweight, plays a vital role in missions like reconnaissance, surveillance, target acquisition, etc. The drone performs dull, dirty, and dangerous operations that human beings cannot do. Nowadays, drones are not limited to military operations. They have various applications like package deliveries, construction, monitoring, and search/rescue operations. Package delivery is one such application that has grabbed the attention of the businessmen where they depend on drones to deliver goods to the intended person against the conventional way of in-person delivery. Towards ensuring correct delivery of the goods, the drone has to capture the image of the person to whom it has to deliver the product

with the help of an onboard image acquisition system and transmit the same to the base station to check whether the person collecting the product is the intended person or not. This process of image encryption, transmission, and subsequent authentication may be tampered with by malicious people (attackers), resulting in an un-accomplishment of the mission. Thus, this is a difficult task as it must ensure the security of the data transmitted. This situation demands the introduction of a cryptosystem for secure goods delivery using drones. The discussion regarding drone dynamics and how the base station authenticates the image are beyond the scope of this work.

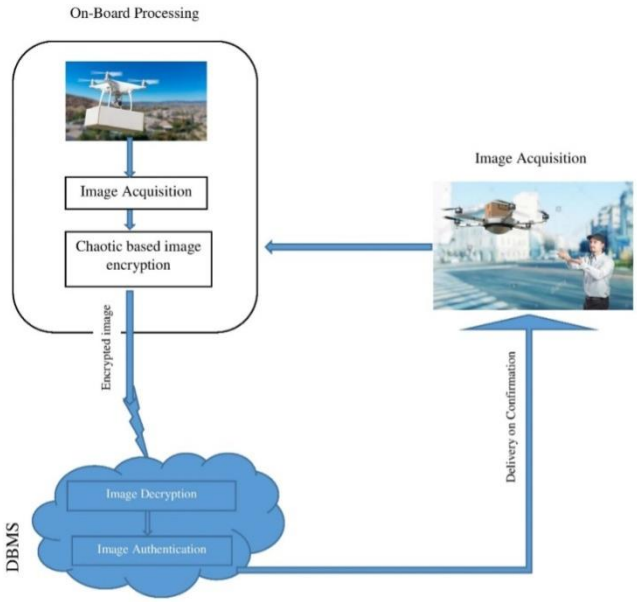

Fig.1: Overall Scenario of the work

Cryptography is concealing messages to ensure secrecy in information security. In Greek, ‘Krypto’ means hidden, and ‘graphene’ means writing [1]. Egyptians also rehearsed cryptography by communicating with the help of hieroglyphs. Modern research on cryptography has inclined more towards mathematical computations. Based on the nature of the key used for encryption and decryption, there are two types of cryptographic techniques. While 'symmetric key cryptography uses the same key for both, asymmetric key cryptography uses two distinct Keys.

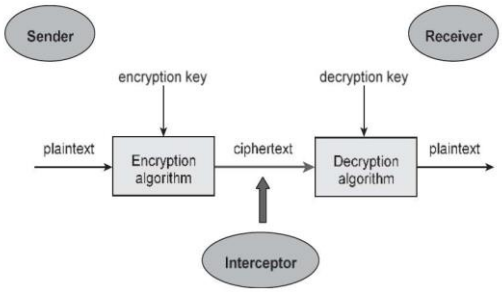

Fig 2: General representation of a cryptosystem

Classical cryptographic techniques like AES, DES, RSA, and BLOWFISH are well suitable for textual data, but they require more computation to transfer multimedia information like voice, image, and video as these have more information contained in them. For example, an RGB image of size 256*256 contains 1,96,608 pixels where the intensity of every pixel represents a number between 0 to 255,

making it feasible to fit within 8 bits. Towards encrypting such an image, 1,96,608 numbers have to be encrypted, which involves much computational power and time, making it unsuitable for a less computational capability platform drone to utilize these techniques.

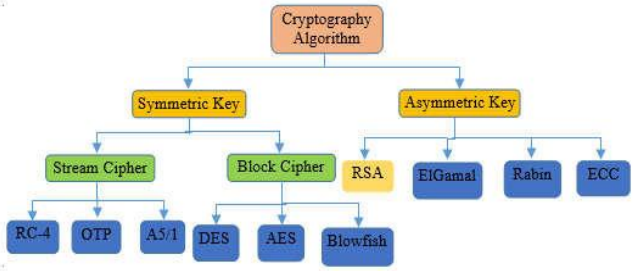

Fig 3: Classification of crypto techniques

2. Chaotic Based Cryptography

Chaos is an approach that utilizes a framework of nonlinear dynamical strategies that depends on starting conditions yielding in arbitrary-like practices. The basic ways of applying chaos theory/map to a cryptosystem are i) to generate pseudo-random key stream, which corresponds to stream ciphers, and ii) iterating chaotic system designed based on preliminary conditions (using plain text or secret keys) and control parameters to generate cipher text corresponding to block of data.

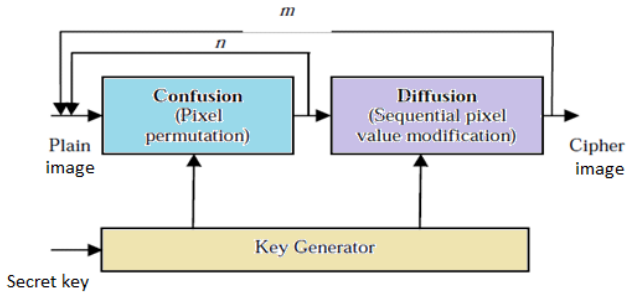

Fig 4: Typical Architecture of Chaos Based Image Cryptosystem

The general architecture of chaos-based cryptosystem shown in Fig. 4 contains three subsections viz. Key generation: based on which the entire strength of cryptosystem depends; Confusion: rearrangement of the pixels to alter the information distribution than that of the original image; and Diffusion: embedding new values to the pixels to modify the image. Both confusion and diffusion are performed based on the key generated by the generator.

There is a wide range of chaotic maps for generating random vectors to compute keys. This work used the Tent and Henon maps for the key generation and confusion, respectively.

a. TENT MAP:

The tent map is described by the following expression:

$$X_{k+1} = X_k/P \text{for } 0 < X_k \leq P, \quad (1)$$

$$= 1- X_k/1-P \text{for } P < X_k < 1, \quad (2)$$

The tent map is topologically conjugate, and thus the behaviors of the map are in this sense identical under iteration [8].

***b. HENON MAP*:**

The Henon map is probably the most popular example of an invertible two-dimensional map. Sometimes called Hénon-Pomeau attractor/map, is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behaviour. General expression for Henon map is provided below:

$$X_{n+1} = 1 - aX_n^2 + Y_n \quad (3)$$

$$Y_{n+1} = bX_n \quad (4)$$

where a and b are dimensionless parameters.

The mathematical equation is iterated no. of times based on the size of the image.

3. Proposed Methodology

The flow chart shown below (Fig. 5) provides the detailed approach employed towards realizing the objective of this study. Following various phases in the flow chart, code was developed in MATLAB environment to test the effectiveness of the proposed methodology. The description of each step in the flow chart is provided below:

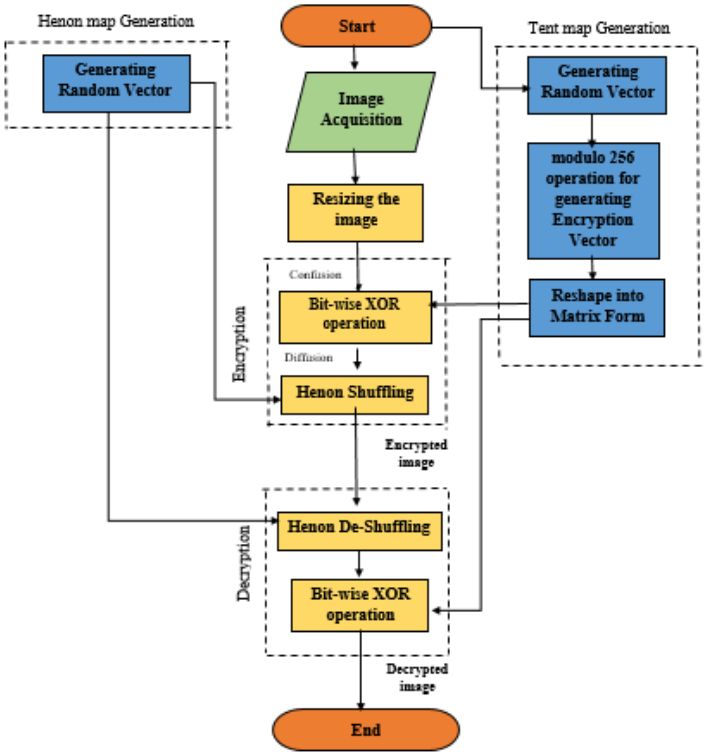

Fig 5: Flow Chart of the proposed methodology

Step 1: We have acquired the image by accessing the webcam using the inbuilt functionality available in the MATLAB environment and then converted the image into greyscale. Later, we have resized this greyscale image to a matrix of size 256*256.

Step 2: We have generated a random variable of size 65,536 (see Fig. 6) using the Tent map with the abovementioned general equations. Each individual element in the random variable is multiplied by 10^14 and made to undergo modulo 256 operations to obtain the remainder.

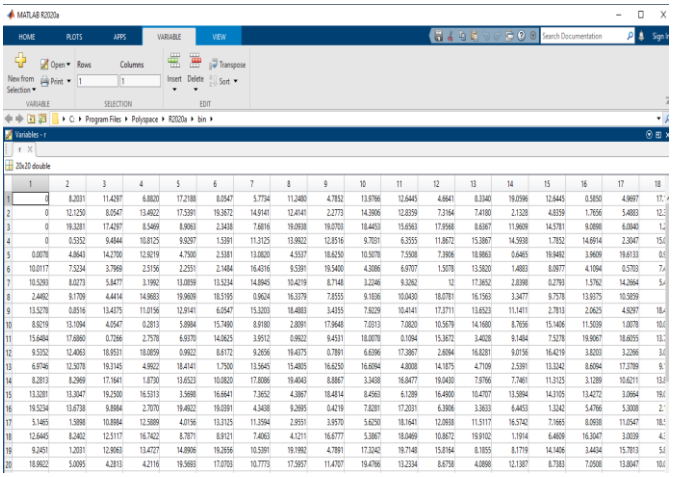

Fig 6: Example of random vector obtained from chaotic map after reshaping

Here, Fig. 7 provides the elements of a sample random vector generated using a Tent map. We have then reshaped the random vector elements into a matrix form for effective visualization.

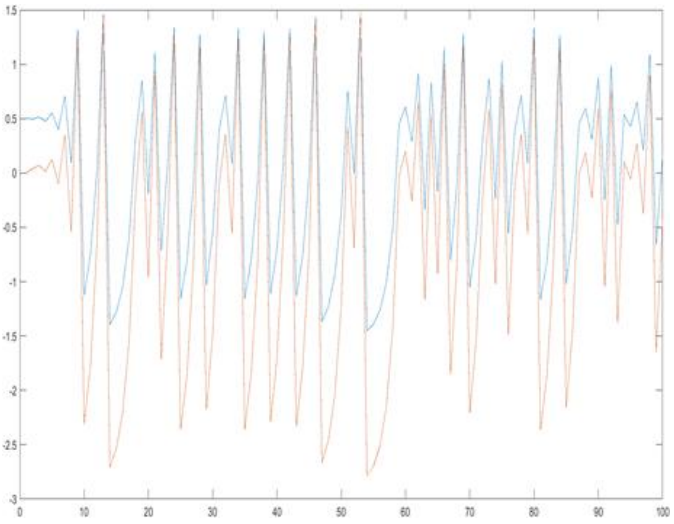

Fig 7: Comparative plot of generated random vector corresponding to variations in initial conditions

Step 3: The obtained remainders are then reshaped to obtain a 256*256 matrix and are bitwise XORed with the resized image. It resulted in achieving the Diffusion process in the chaotic cryptosystem.

Step 4: Using the Henon map, we have generated another random variable of 65,536 elements whose values range from 1 to 256 and have arranged them in the form of 256 rows where each row has 256 distinct values.

Step 5: We have utilized this random vector to permute the pixels obtained after diffusion and served as a Confusion process which resulted in an encrypted image. Thus, the image encryption corresponds to steps 3, 4, and 5, respectively.

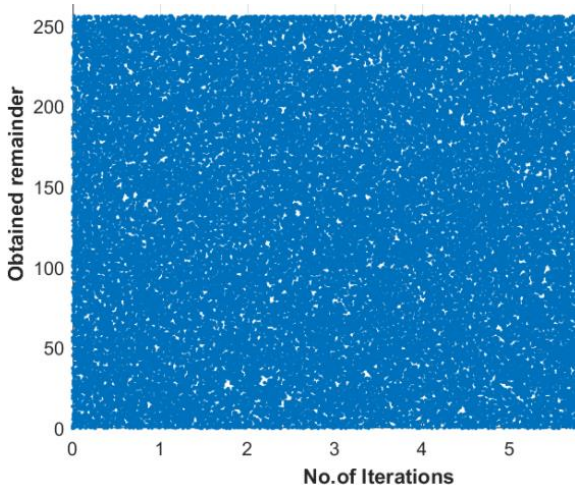

Fig 8: Remainder corresponding to random vector

Step 6: We have then fed this encrypted information to the decryption process. At this stage, we have performed a reshuffling process based on the Henon map and EXORed the obtained data with the reshaped random variable generated from the Tent map. After this, we have got the original image without any loss or disturbance in the data. This process is considered decryption.

4. Simulation Results

We have tested the MATLAB code developed by us, running it on a workstation with MATLAB 2019 version having 4GB RAM and a 2.20 GHz processor. Taking A=0.5, B=1.99, Φn=0.5 as initial conditions for Tent map and a=1.4, b=0.3 for Henon map. This section will discuss the results obtained at different stages of the proposed methodology.

Fig 9: Input to be encrypted or plain text image

The image shown in Fig. 9 is obtained by resizing the original image to 256*256, captured by the camera system, and then converting it into greyscale. Fig. 10 is the diffused image obtained after performing the EX-OR operation between remainders of the random vector generated by the Tent map and original image.

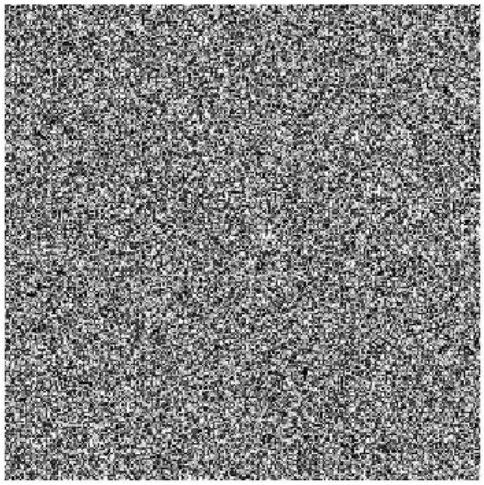

Fig 10: Diffused Image

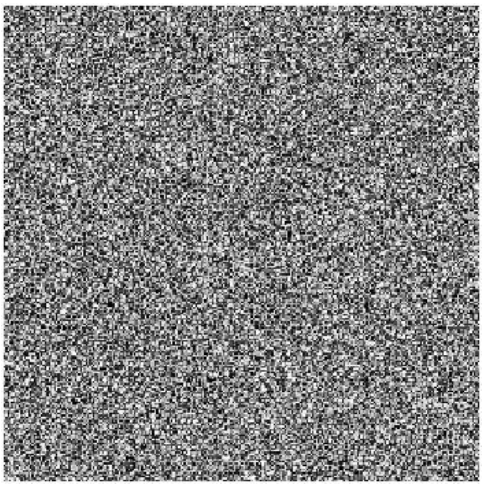

Fig 11: Confused image

Fig. 11 is the confused/encrypted image obtained by applying the generated Henon map to shuffle the rows and columns of the diffused image.

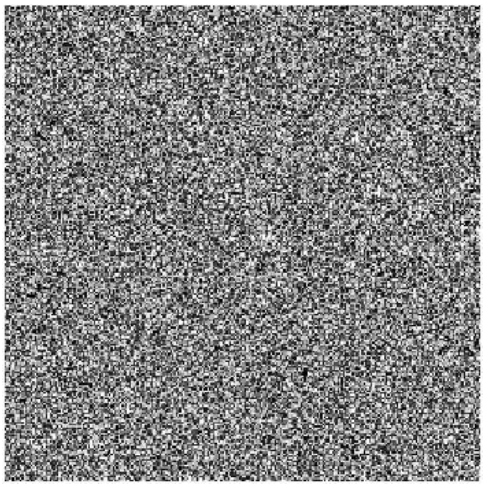

Fig 12: Reshuffled image

Fig 13: Decrypted Image

Fig. 12 is the reshuffled image generated by applying the reverse approach followed in obtaining the confused image. It is to be noted that the reshuffled image should be exactly the same as the diffused image. Fig. 13 provides the decrypted image obtained by performing bitwise EX-OR operation using the same remainder vector generated with random vector using Tent map.

5. Security Investigation

Security analysis of the image demonstrates the relationship between the original and ciphered image. The cipher image must be completely different from the original [14]. One can perform security analysis through several approaches and parameters available in the current literature.

(1) Statistical Analysis: It is vital for a cryptosystem to resist any statistical attack. There are two important parameters that highlight the statistical strength of an image encryption scheme: (a) Histogram analysis and (b) Correlation coefficient analysis [10].

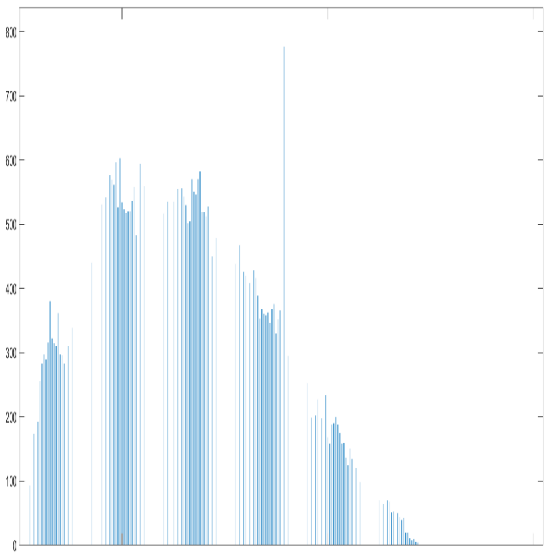

Fig 14: Histogram Corresponding to Input/Original Image

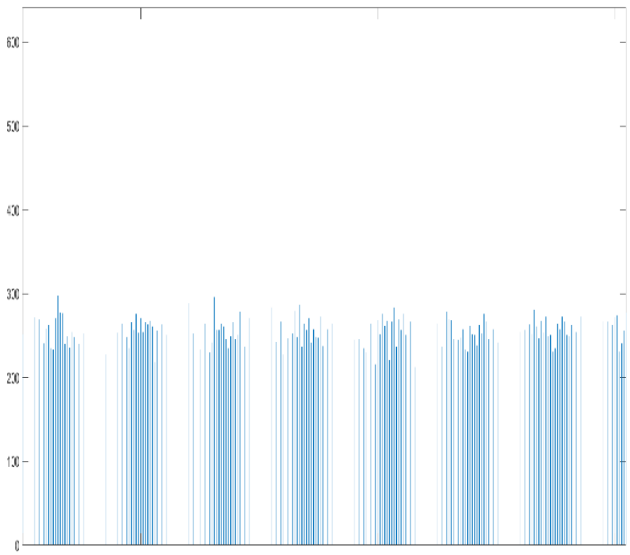

Fig 15: Histogram Corresponding to Encrypted Image

The observed variations in the histogram (see Fig. 14) indicate the information distribution of a given image. The flat histogram (see Fig. 15) signifies uniform distribution of information in the encrypted image. Therefore, it does not provide any clue about the original image.

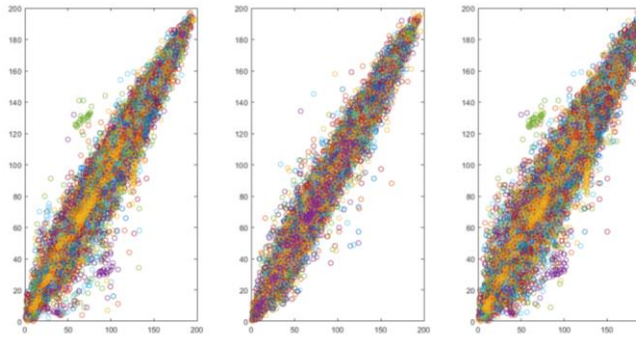

Fig 16: Correlation coefficient analysis of original image

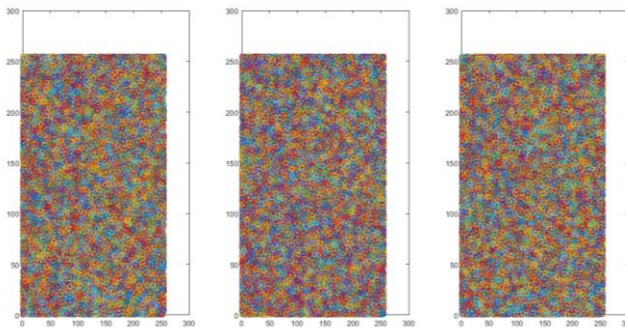

Fig 17: Correlation coefficient analysis of encrypted image

Fig. 17 provides the pictorial representation of correlation coefficient analysis showing the broad distribution of the encrypted image in contrast to the narrow distribution of the original image (see Fig. 16), justifying the efficiency of the employed encryption technique.

Table 1: Correlation coefficient values of two adjacent pixels in original and encrypted image

Type of Image	Directions	
	Vertical	**Diagonal**
Original Image	0.9899	0.9769
Encrypted Image	0.0002	0.0030

Table 1 shows the computed values of the correlation coefficients for adjacent pixels of the encrypted image in vertical and diagonal directions. A value close to 1 reflects a high correlation, and 0 equals no correlation. The calculated values indicate low correlations among the adjacent pixels making it difficult for the intruder to understand what is being transmitted.

***(2) Differential attack Analysis*:** The purpose of this analysis is to examine the effectiveness of the crypto technique towards small variations in the plain text.

(a)Number of Pixel Change Rate (NPCR) – This measure evaluates the percentage change in the number of pixels present in the two encrypted images obtained using the same crypto technique with one-bit variation in the pixels corresponding to one of the input images when compared to the other. Let I_{E1} (i, j) and I_{E2} (i, j) be the pixels values of the encrypted images corresponding to both the input images at the i^{th} row and j^{th} column, respectively. Thus, it provides the following mathematical expression:

NPCR=$\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) * (100 /M * N)$

Where, D(i,j)=0 if I_{E1}(i,j)= I_{E2}(i,j) if not then D(i,j)=1

(b) Unified Average Changing Intensity (UACI) - A small change in plaintext image would cause some significant change in cipher-text image. It is helpful to identify the average intensity of difference in pixels between the two images.

$UACI=\sum_{i=1}^{M}\sum_{j=1}^{N}[|Io(i,j) - Ienc(i,j)|/255] * (100 /M * N)$

Table 2: NPCR and UACI Analysis of Chaotic Map

Test type	Grey image
NPCR	99.8
UACI	21.037

The NPCR value 99.8 specifies that the employed encryption technique generates an entirely different encrypted image even for the one-bit change in the input image. It provides concrete evidence that the encryption technique is resilient to differential attacks.

(3) Information entropy - The entropy of the ciphered image is the measure of randomness in the generated image, and a value of 8 represents the best entropy. The technique we have employed in this study resulted in an entropy value of 7.9970, justifying the strength of the encryption technique.

(4) Key Space and Keys Sensitivity Analysis - Key space is the number of attempts necessary to guess a correct decryption key. Strong encryption should have an encryption key no lesser than 2^100. Key sensitivity reflects the susceptibility of the encryption technique to produce a new image for a minute change in the parameters contributing to the key generation.

Table 3: Key Space and Keys Sensitivity Analysis of Chaotic Map

Test type	Grey image
Key space	2^{250}
Keys sensitivity	99.4904

(5) Time analysis – This tool analyses the time taken by the developed technique to encrypt and decrypt the input fed to the system. As already stated, the simulations were carried out on the workstation, which has 4.00GB RAM and a clock frequency of 2.20 GHz. The time elapsed for the whole process is 3 seconds, which tells us that the technique is well suited even for a low-capacity platform like a drone.

6. Conclusion

We have encrypted the acquired image with the proposed chaotic-map-based technique developed in MATLAB wherein the Confusion process is achieved based on 'Tent Map' and the Diffusion process based on 'Henon Shuffling' We have performed encryption and decryption on different images to observe the robustness of the proposed technique and found the soundness of the same. Further, to analyze the much-needed quality of any cryptosystem which is resilient to attacks, the obtained encrypted image is subjected to Statistical analysis, Differential attack analysis, Information entropy, Time analysis, and Key analysis. Results showed concrete evidence about the strength of the proposed technique. Also, they supported the main objective of developing a low complex chaotic-map-based cryptosystem to deliver the products securely using drones.

REFERENCES

[1] Ahmad, Seong Oun Hwang, Arshad, “An Experimental Comparison of Chaotic and Non-Chaotic Image Encryption Schemes”, Jawad Ali Wireless Pers Commun © Springer Science+Business Media New York 2015

[2] Attila A. Yavuz Dronecrypt – “An Efficient Cryptographic Framework for Small Aerial Drones” Conference: MILCOM IEEE Military Communications Conference (MILCOM) 2018

[3] Constantin Balan, “Aspects of airborne continuous surveillance systems: practical image encryption module”, 10th WSEAS International Conference on Mathematical Methods and Computational Techniques in Electrical Engineering, May 2008.

[4] Chengqing Li1, Dongdong Lin1, Bingbing Feng2, Jinhu Lü3, And Feng Hao4 “Cryptanalysis of A Chaotic Image Encryption Algorithm Based On Information Entropy” Vol. X 4, 26 Nov 2018

[5] Chunhu Li · Guangchun Luo · Ke Qin “An image encryption scheme based on chaotic tent map” © Springer Science+Business Media Dordrecht 2016.

[6] Guodong Ye∗ Chen Pan, Xiaoling Huang, Zhenyu Zhao and Jianqing “Chaotic Image Encryption Algorithm Based on Information Entropy He International Journal of Bifurcation and Chaos”, Vol. 28, No. 1 (2018) 1850010 (11 pages) ©World Scientific Publishing Company

[7] Jan Sher Khan1 · Jawad Ahmad2 “Chaos based efficient selective image encryption” © Springer Science Business Media, LLC, part of Springer Nature 2018

[8] Jeena Pappachan1, Jinu Baby2 “Tinkerbell Maps based Image Encryption using Magic Square” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Vol. 4, Issue 7, July 2015

[9] Komal D Patel1, Sonal Belani2 “Image Encryption Using Different Techniques: A Review International Journal of Emerging Technology and Advanced Engineering” Website: www.ijetae.com ,56

[10] Ljpuco Kocarev and Shiguo Lian (Eds.), Chaos-Based Cryptography Theory, Algorithms and Applications ©2011 Springer

[11] Manjunath Prasad et al./ Elixir Elec. Engg. 38 (2011) 4492-4495 “Chaos image encryption using pixel shuffling with henon map “

[12] Priya R Sankpal, P A Vijaya. "Image Encryption UsingChaotic Maps: A Survey", 2014 Fifth International Conference on Signal and Image Processing, 2014

[13] Ravi Shanker Yadav1, Mhd. Rizwan Beg2 & Manish Madhava Tripathi3 “Image Encryption Techniques: A Critical Comparison” International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 1, Mar 2013, 67-74 © TJPRC Pvt. Ltd.

[14] Riham AlTawy and Amr M. Youssef, 2016. “Security, Privacy, and Safety Aspects of Civilian Drones: A Survey.” *ACM Trans. Cyber-Phys. Syst.* 1, 2, Article 7 (December 2016), 25 pages.

[15] R. Clarke, “Understanding the drone epidemic,” Computer Law & Security Review, vol. 30, no. 3, pp. 230 – 246, 2014.

[16] Rushi Lan, Jinwen He, Shouhua Wang, Tianlong Gu, Xiaonan Luo, “Integrated Chaotic Systems for Image Encryption”, *Signal Processing* (2018),

[17] Samson Chepuri, “An RGB Image Encryption using RSA Algorithm” International Journal of Current Trends in Engineering & Research (IJCTER) e-ISSN 2455–1392 Volume 3 Issue 3, March 2017 pp. 1 – 7

[18] Sabah Fadhel1*, Mohd Shafry2, Omar Farook3, “Chaos Image Encryption Methods: A Survey Study” Bulletin of Electrical Engineering and Informatics ISSN: 2302-9285 Vol. 6, No.1, March 2017, pp. 99-104,

[19] “Secure Communications in Unmanned Aerial Vehicle” Network December 2017 Lecture Notes in Computer Science In book: Information Security Practice and Experience (pp.601 -620)

[20] Shahab saquib sohail and Musheer Ahmad, “Chaos Based Encryption” ©2012 LAMBERT Academic Publishing