IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306257|

# Hybrid Image Cryptography with Advanced Encryption using Two-Step Logistic Map

**Sahana S U**

Post-Graduation Student, Department of MCA, PES Institute of Technology and Management, Shivamogga, Karnataka, India

**ABSTRACT:** Data is transmitted via the internet on a regular basis. One of the main information sources that are expanding on the internet is images. Pictures might include private information. Thus, image security is a big problem. One of the primary methods for picture security is cryptography. Chaos is employed in the encryption process due of its many properties. Various chaos-based image encryption algorithms are defined. Encryption techniques usually employ many rounds. It is necessary to create an image encryption method that employs the right amount of uncertainty and diffusion and encrypts the image in a single scan. The two-step iterative logistic map is used in the suggested picture encryption method. There is a lot of key space used. The experimental results demonstrate that the suggested system has superior

**KEYWORDS**: Encryption, Decryption, Chaos, Logistic map, Confusion, Diffusion**.**

## I. INTRODUCTION

The rapid advancement of digital technology and the widespread use of the internet have led to an unprecedented increase in the exchange of digital images. The sharing of digital photographs has increased at a rate never before seen due to the increasing popularity of the internet and the rapid growth of digital technologies. Since important information is frequently contained in these photos, strong security measures are required to keep it safe from piracy, illegal access, and modification. The special properties of digital photos, such as high redundancy, massive data volumes, and significant connections among nearby pixels, make standard encryption techniques like DES, AES, and RSA ineffective for encrypting images, even though they work well for word and binary information. Specialized encryption methods are needed for digital photographs in order to effectively manage their unique characteristics. Using chaotic systems to encrypt images is one interesting method. When it comes to predictable structures that behave randomly, chaos theory provides

Compared to digital images, conventional cryptography methods perform less quickly. As a result, real-time communication requires fast encryption and decryption. Because of its distinct characteristics, image-based encryption is not the same as text-based cryptography. When it comes to picture encryption, pixels—the basic building components of an image—are taken into account. Image encryption modifies the values and placements of pixels. Generally speaking, encrypting photos should be enough to prevent these sorts of attacks. The cipher image's characteristics must be such that the original image is generated after the decryption process. We encrypt the image using a two-step iterative logistic technique to produce a chaotic sequence. Sub-keys are employed in order to change the values and locations of the pixels.

- It assigns a random location to the specific pixel.
- The cipher text has to be key-sensitive.

In order to improve security and performance, this study suggests an improved picture encryption system that makes use of the chaotic characteristics of the logistic and Henon maps. Diffusion and permutation are the two major steps in the suggested approach. By rearranging the pixel locations using the Duffing map during the permutation step, the spatial link between neighboring pixels is essentially broken. Using the logistic and Henon maps in an iterative two-step procedure, the diffusion stage modifies the permuted image's pixel values. This two-step procedure makes sure that the values and locations of the pixels are completely jumbled, offering strong defense against a range of cryptographic

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306257|

assaults. The suggested method was created to be as effective as possible, encrypting the picture with only one scan. Because of its efficiency, it may be used in real-time applications where security and speed are essential. The suggested approach is shown to be highly resistant to quantitative and different assaults through comprehensive experimental findings, underscoring its efficacy in protecting digital pictures both during transmission and storage.

## II. LITERATURE REVIEW

The encryption system which has been explained here was proposed by Sankaran K. S. and Krishna B. V. The complicated Chao Maps have been used in the process. There are two phases: a phase of uncertainty, and a phase of filtering. In the first case, the initial parameters are used to create the secret key. Some problems are identified to be selected for the diffusion stage, one chaotic system will be employed for diffusion, while the other one for confusion and likewise the third-dimensional chaotic system shall also apply for confusion [1].

A new encryption method which has been proposed by Xu Shu Jiang, Wang Ji, Su-Xiang Yang uses the chaotic maps to enhance uncertainty and distribution. The Lorenz system and Baker map are used to change the coordinates of points and their intensities of individual pixels. Having confusion is not the same thing as having diffusion and therefore requires a different key. On the decryption side, the inverse procedure is applied to recon struct the original picture from the encrypted signal. [2]

A two unit encryption strategy that creates a stream cipher and utilizes one unit for pixel permutation was offered by Somya, A Ali, T Abdalla, and A. Maadeed. The W7 method produces the main stream, while the Henton map produces the pseudorandom sequence. This involves a shift in both the place and the value at a time. Through the permutation map the pixel shuffler is able to decrease the correlation coefficient. The stream chosen and the permuted picture are then XORed to get the encrypted picture. For decryption, the key stream and cipher image are added with the help of XOR operation. To this, the reverse permutation is then used. [3]

H. Md. A. Najjar and A. Md. AL-Najjar present an encryption system that employs the use of logistic maps to encrypt photos. The pixel mapping tables are constructed out of logistic maps and perform conversion of pixel values with no change in the location. It uses two techniques: the first uses a map table and a random value to map the values of the pixels while the second uses a map table generated from low processed pixel-values. The second is the XOR action with the help of sequences generated by the logistic map and pixels. The encrypted picture can then be decrypted whereby the stated procedure is reversed. [4]

A technique was presented by K. Gupta and S. Silakari, wherein an input picture is used to produce three colored images: such primary colors as red, green, and blue. The green and red pictures are recolourized into horizontal and vertical planes, whereas the blue picture remains the same. As for the first level of confusion, a map of a cat in 2D is applied. From each of the three photos, rows are selected, and as this is being done, each of the selected rows appears to be confused. One map followed the other and while using the cat maps the next map was the conventional one so as not to compound the learners' confusion. Dispersed and confused images are taken and they are XORed to enact the encryption. Another way of decrypting a picture is to use the inverse of the procedure [5].

## III. METHODOLOGY

This image is permuted with the help of a duffing map. The two initial values of the Henon map are two values from the secret key. In order to get one diffusion iteration all the pixel values are XORed with the matrix constructed from the Henon map values. The second value of the Henon map produced is shown as the starting value of the logistic map. That is why driven by the need to reproduce knowledge, the second stage of dissemination is represented. To choose the starting value of the logistic map one selects the next value of the Henon map for the other image.

Encryption process has been illustrated in figure 1 while decryption is the reversal of the encryption process illustrated in figure 2.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306257|

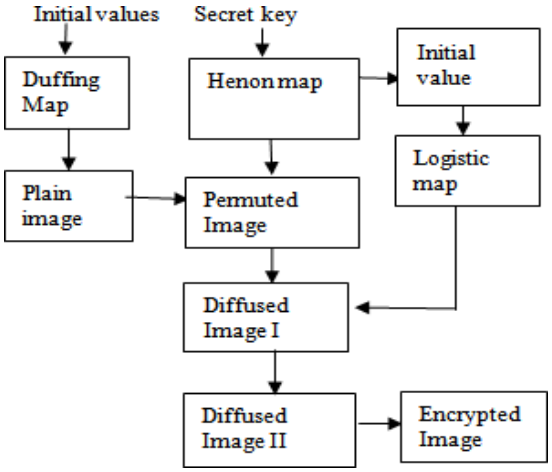


**Figure 1: Encryption Process**

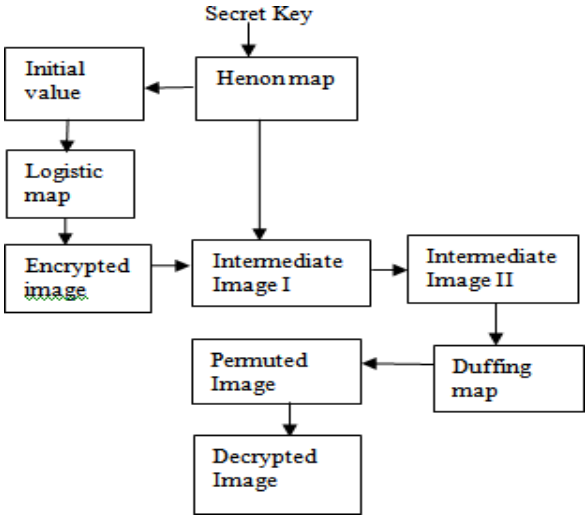


**Figure 2: Decryption Process**

## IV. ALGORITHM

**1. Chaos-based image Algorithm**

- Input:

Plain image I (i, j): A gray scale image of relatively small size. M×N where 1≤i≤M and 1≤j≤N.
Parameters: a and d for the Henon map and r for the logistic map.

- Output: Cipher image C (i, j): The encrypted image with the same dimensions M×N.

**Step 1: Generation of Sequences Using Duffing Map**

Duffing Map: A nonlinear second-order differential equation used to generate chaotic sequences.
Generate Sequences k and l: Use the Duffing map to generate two sets of sequences, k and l.
These sequences are:
k={k1,k2,…,km}
l={l1,l2,…,ln}
The sequences k and l are obtained using initial values specific to the Duffing map.

**Step 2: Permutation Using Sorted Sequences**

Sorting Sequences: Sort the sequences k and l.
Permutation: Use the sorted sequences to rearrange (permute) the pixels of the image.
The pixel at position (i, j) in the original image I(i, j) is moved to a new position (k, l):
I(i, j)=I(k, l)

**Step 3: Diffusion Using Henon Map**

The Henon map sequence is used to dilute the permuted picture. The starting values and secret keys $a$, $d$, and others are selected so that (0) and (0) produce the Henon map sequence.

**Step 4: Further Diffusion Using Logistic Map**

Henon map ($i$), where $\boldsymbol{U}$ is, is used to select the initial value (0).
Further Diffusion: Use the logistic map sequence to further diffuse the image obtained from Step 3.

**Step 5: Encrypted Image**

This second diffuse image gotten from the application of logistic map will be the final encrypted image, C (i, j).

- Derive random-like and noisy signals with the help of the Duffing map.
- Pixel-interchange the image according to the sequences derived from the map of Duffing.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306257|

- Dispersing the permuted image utilizing the Henon map.
- Disperse the image even more with the help of the logistic map.
- Thereby it fulfills the desired output, which is the encrypted image.

## V. IMPLEMENTATION

- **Histogram Analysis**: The encrypted image's histogram displays a uniform distribution, in contrast to the original image's peaks that represent the values of the individual pixels.
- **Correlation Coefficient**: This calculates the correlation between neighboring pixels in the unencrypted and original pictures. In the encrypted image, a successful encryption technique will have a low correlation coefficient, meaning that the pixel values are uncorrelated and the image is completely jumbled.

Original Image: 0.98 (high correlation)
Encrypted Image: 0.02 (low correlation)

- **Entropy Analysis**: The encrypted image's unpredictability is measured by entropy. An picture is more unexpected the higher its entropy. The optimal entropy value for an 8-bit picture is about 8.

Original Image: 7.12
Encrypted Image: 7.98 (closer to 8, indicating high randomness)

- **Key Sensitivity**: An whole different encrypted picture is produced by even a little alteration to the key (such as altering only one bit).
- **Differential Attack Metrics**: Testing parameters such as UACI (Unified Average Changing Intensity) and NPCR (Number of Pixels Change Rate) are part of this process. High values for UACI and NPCR show that differential attacks are challenging since even a slight alteration in the source picture causes a noticeable alteration in the encrypted image.

NPCR: 99.64% (indicating significant change with minor image modification)
UACI: 33.46% (indicating high average intensity of differences)

- **Performance**:

Encryption Time: 0.35 seconds for a 512x512 image.
Memory Usage: Efficient, suitable for real-time applications.

## VI. RESULTS

The examination of the results shows how well the suggested chaotic picture encryption technique is at protecting the confidentiality and integrity of digital photographs. Because chaotic maps are used, the encryption is resistant to statistical and differential attacks due to their great sensitivity to beginning circumstances and key values. The performance metrics indicate that the algorithm is efficient enough for real-time applications, making it a viable option for secure image transmission in various domains.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306257|

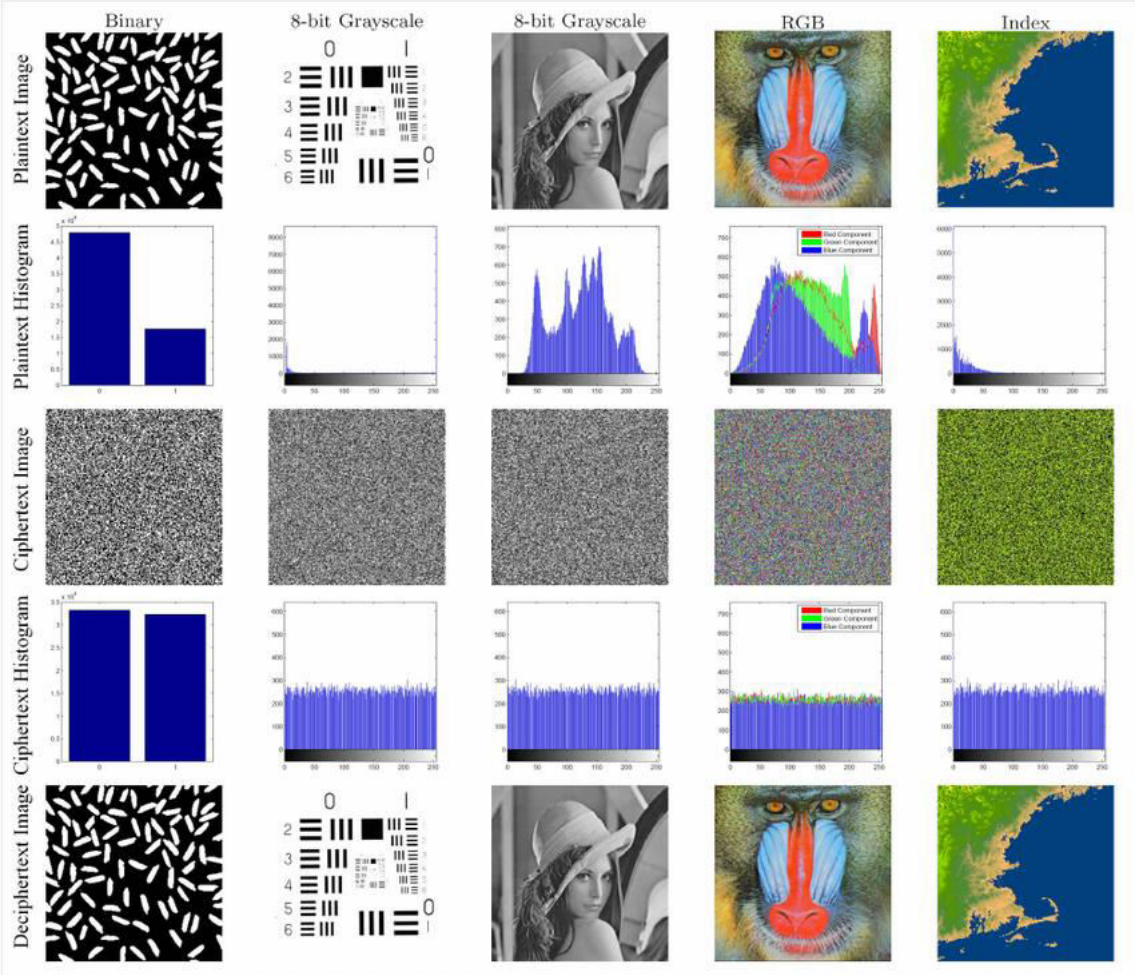


**Figure 6.1: Histogram Analysis on Encrypted Images.**

## VI. CONCLUSION

The proposed encrypted image solution for the revised logistic map is directly reliant on the diffusion and confusion processes being changed. It is designed only for grayscale images. Using a two-step logistic map, this method increases the safety of the chaotic sequence. The method protects against brute force assaults by using a 144-bit key space. Two subkeys can be used to modify the pixel value, and subkeys are modified after every loop. The statistical analysis shows that the recommended encryption method is capable of successfully thwarting a statistical assault. The UACI and NPCR parameter computations show how secure the method is against differential assaults.

## REFERENCES

1. Sankaran K.S. and Krishna B.V.S.," A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", IJIET, Vol. 1, No. 2, June 2011.
2. Xingyuan Wang, Jianfeng Zhao, Hongjun Liu, "A new image encryption algorithm based on chaos", Optics Communications Volume 285, Issue 5, 1 March 2012, Pages 562–566.
3. S. A-Maadeed, A. Al-Ali, and T. Abdalla, A New Chaos-Based Image- Encryption and Compression Algorithm", Hindawi Publishing Corporation, Journal of Electrical and Computer Engineering, Volume 2012, Article ID 179693.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306257|

4. Jui Cheng and Jiun-In Guo," A New Chaotic Key Based Design for Image Encryption and Decryption", Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva.
5. Osmet Öztürk and Obrahim Soukpınar, "Analysis and Comparison of Image Encryption Algorithms" International Journal of Information Technology Volume 1 Number 2.
6. H. Md. Al-Najjar, A. Md. AL-Najjar," Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table".
7. K. Gupta, S. Silakari," New Approach for Fast Color Image Encryption Using Chaotic Map", JIS, 2011, 2, 139-150.
8. D. Chattopadhya and D. Nandi," Symmetric key chaotic image encryption using circle map", Indian Journal of Science and Technology, Vol. 4 No. 5 (May 2011) ISSN: 0974-6846, pp 593 – 599.
9. J. Fridrich, "Image encryption based on chaotic maps" 1997 IEEE International Conference on Systems, Man, and Cybernetics, Computational Cybernetics and Simulation. ISSN: 1062-922X.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details