Advances in Artificial Intelligence and Machine Learning; Research 6 (1) 5049-5061 Received 12-11-2025; Accepted 14-02-2026; Published 21-02-2026

DeepCryptanalysis: Dense Attention U-Net to Break Chaos-Based Color Image Encryption

Sonia Amiri sonia.amiri@isimg.tn
Research Team in Intelligent Machines (RTIM), National Engineering School of Gabes (ENIG), University of Gabes, Tunisia.

Mourad Zaied mourad.zaied@univgb.tn
Research Team in Intelligent Machines (RTIM), National Engineering School of Gabes (ENIG), University of Gabes, Tunisia.

Corresponding Author: Sonia Amiri

Abstract

In this paper, we propose an innovative Convolutional Neural Network (CNN) for the cryptanalysis of color image encryption algorithms. Our model combines a dense U-net with attention mechanism to efficiently attack chaos based schemes, such as the Two-Dimensional Improved Logistic Coupling Map (2D-ILCM). For training process, we generated a large set of plaintext-ciphertext pairs using the CIFAR-10 dataset. Numerical results shows that reonstructed images are visually and statistically similar to their corresponding original plaintexts. The accuracy and flexibility of the proposed cryptanalysis model are validated by rigorous quantitative and qualitative evaluations based on multiple cryptographic and similarity metrics. Furthermore, our approach demonstrates its capacity to analyze security flaws in chaos-based image encryption schemes by showing strong resistance to partial occlusion and gaussian noise.

Keywords: Cryptanalysis, Deep learning, Color images, Encryption, Chaos, CNN, Known-plaintext.

1. INTRODUCTION

Recent years have seen an important use of digital colored images on the Internet, this imposes the need for data security and privacy protection. In this context, researchers have focused on exploring image encryption to protect against malicious access during transmission. Chaos is one of these encryption techniques, that uses initial parameters to auto-iterate and produce pseudo-random numbers [1–11]. These methods have been the subject of multiple security analysis studies since they have demonstrated their robustness for image encryption [12–16].

The chaotic techniques of encrypting colored images continue to evolve over time, they provide excellent security but also have flaws. Pak et al. (2017) [2] introduced an effective 1D chaotic map algorithm, which was later broken by Dou et al. (2020) [12] using a chosen plaintext attack. In

Citation: Sonia Amiri and Mourad Zaied. DeepCryptanalysis: Dense Attention U-Net to Break Chaos-Based Color Image Encryption. **Advances in Artificial Intelligence and Machine Learning.** 2026;6(1):280. https://dx.doi.org/10.54364/AAIML.2026.61280

2019, Pak et al. improved this method using a bit- level approach [3] broken by li et al. [13] and then improved using a 2D logistic coupling map [4]. Other studies have explored similar chaotic systems for color images encryption [1, 5, 6]. In most cases, researchers have designed specific cryptanalysis methods for each encryption technique, and reveal their vulnerabilities in specific attack scenarios.

Deep learning, a promising technique in cryptanalysis, was first introduced by Hai et al. [17] to analyze the optical encryption algorithm security. Then, in 2022 Wang et al. [18] used the U-net architecture to examine the security of an encryption method based on optical interference. In 2023, Liu et al. [19] applied Pix2Pix adversarial network to analyse the security of a computational-ghost-imaging cryptosystem. Based on the encoder-decoder framework, Fusen et al. [20] have created a neural network for image decryption (IDEDNet). Deep learning has proven its ability to retrieve encrypted images through a chaotic system without any knowledge of cryptosystems, thanks to its advanced feature extraction and pattern recognition capabilities.

In this research, we introduce a deep-learning-based cryptanalysis framework for chaos-based color image encryption, which is based on a novel Dense Attention U-Net architecture. By using paired encrypted–plaintext images for training, the proposed model successfully breaks the 2D-ILCM encryption scheme under a known-plaintext attack, without requiring access to encryption keys or system parameters. In addition, robustness analysis under Gaussian noise and partial occlusion exposes intrinsic weaknesses of deterministic chaos-based encryption. These findings demonstrate the effectiveness of deep learning as a practical and powerful tool for the security evaluation of chaos-based image encryption systems.

The structure of this document is as follows. We give a summary of Pak's encryption method in Section 2. Then, in section 3, we introduce our CNN autoencoder model and its implementation details. Section 4 is reserved for the results of numerical simulation to confirm the viability and efficacy of the suggested deep cryptanalysis method. Section 5 is devoted to conclusions and prospects.

2. AN OUTLINE OF PAK'S ENCRYPTION METHOD

Chanil Pak and colleagues proposed in 2021 [4] a two-dimensional Improved Logistic Coupling map (2D-ILCM) for color image encryption. FIGURE 1 demonstrates the encryption process, which boosts chaotic behavior by extending one-dimensional logistic maps to two dimensions. The 2D-ILCM is governed by the following equations:

$$x_{n+1} = \alpha x_n (1 - y_n) G(k) - \lfloor \alpha x_n (1 - y_n) G(k) \rfloor \quad (1)$$

$$y_{n+1} = mod((\beta y_n (1 - x_n) + (4 - \beta) y_n (1 - x_n)) G(k), 1) \quad (2)$$

- x_n, y_n : chaotic state variables.
- α, β : control parameters.
- $G(k) = 2^k$ is a scaling function, where k controls the complexity of the chaos.

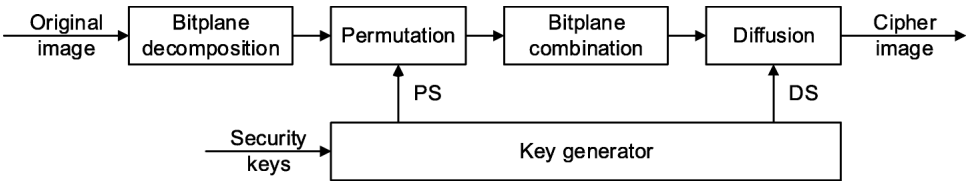

Figure 1: Pak's image encryption process [4].

The model integrates two improved 1D logistic maps, guaranteeing strong pseudo-randomness in the chaotic sequences by the following equations:

$$x_{n+1} = \alpha x_n (1 - x_n) 2^{12} - \left\lfloor \alpha x_n (1 - x_n) 2^{12} \right\rfloor \tag{3}$$

$$y_{n+1} = \mod (\beta y_n (1 - y_n) + (4 - \beta) y_n (1 - y_n)) 2^{12}, 1) \tag{4}$$

Six parameters $(x_0, y_0, \alpha, \beta, \sum, N_0)$ are used as security keys in the encryption algorithm. The following equations are used to determine the modified initial values:

$$x_0' = mod\left(\frac{sum}{255 \times H \times 3W} + x_0, 1\right) \tag{5}$$

$$\alpha' = mod\left(\frac{sum}{255 \times H \times 3W} + \alpha, 4\right) \tag{6}$$

$$y_0' = mod\left(\frac{sum}{255 \times H \times 3W} + y_0, 1\right) \tag{7}$$

$$\beta' = mod\left(\frac{sum}{255 \times H \times 3W} + \beta, 4\right) \tag{8}$$

Where H and W represent the dimensions of the image, and $\sum$ is the cumulative sum of pixel values.

Pak et al. have demonstrated that their proposed 2D-ILCM method represents an efficient and secure framework for encrypting colored images. In order to resist attacks, it takes advantage of chaos properties along with pixel-level diffusion and bit-level permutation. In the remainder of the paper, we test the security of this approach by applying our cryptanalysis model.

3. DEEP LEARNING CRYPTANALYSIS

3.1 Network Architecture

To break image encryption algorithms, we expand and adjust the improved U-Net model previously introduced in our earlier work [21]. This approach aims at deciphering complex structures found in chaos encrypted images. As in [21], it uses the classic U-Net encoder-decoder structure, as illustrated in FIGURE 2, and incorporates further changes to improve its color image cryptanalysis capacity.

A $32 \times 32 \times 24$ feature map is first created by applying a Conv2D layer characterized by 3×3 kernel and 24 filters. Then, it passes through an encoder-decoder network made up of transition layers and dense blocks. The last step creates a three-channel reconstructed image using a Conv2D layer with a 3×3 kernel, three filters, and sigmoid activation.

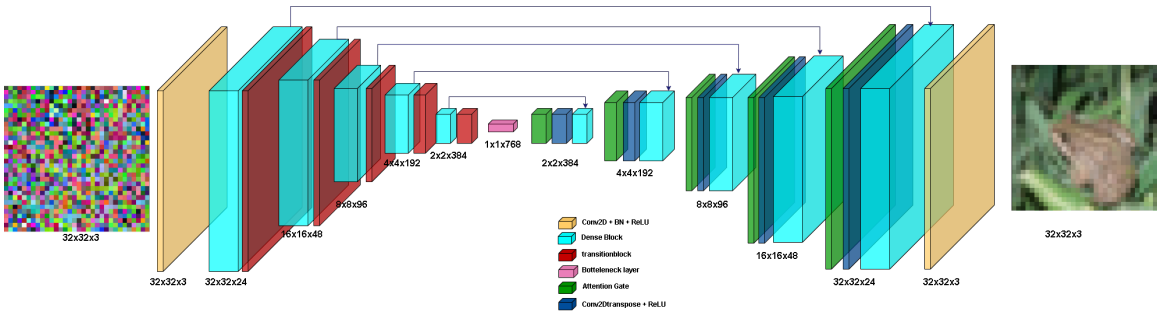

Figure 2: The proposed deep cryptanalysis overall architecture.

To permit hierarchical feature extraction and perform feature propagation, we replaced all encoder-decoder convolutional layers with dense blocks, which are composed by four layers: a 3×3 convolutional layer, rectified linear unit (ReLU), and batch normalization (BN) [22].

To prevent overfitting and enable effective subsampling, transition blocks come after each dense block. These blocks have BN, ReLu, a 3×3 convolutional layer, dropout with a ratio of 0.1, and averaging layers uses 2 x 2 kernel and 2 for stride. Furthermore, we integrated an attention mechanism that performs feature selection and modulates encoder-decoder skip connections to concentrate on the features of greatest importance when decrypting. The feature maps are gradually reconstructed by a number of upsampling blocks that make up the decoder path.. Each block is composed of attention-weighted skip connections, transposed convolutions, and dense blocks that guarantee accurate prediction of input images.

3.2 Implementation Settings

Datasets of encrypted images and implementation parameters are described in this section.

3.2.1 Dataset

The 2D-ILCM encryption algorithm proposed by Pak et al. [4] is well known for its effectiveness and security when encrypting color images. It makes the encryption process computationally efficient and resists to statistical and differential attacks by combining the benefits of pixel-level diffusion and bit-level permutation. Because of its strong cryptographic properties, we have chosen the 2D-ILCM encryption method as the center of our cryptanalysis model in order to analyze its performance and robustness against potential attacks.

The CIFAR-10 dataset, originally introduced by Krizhevsky et al. [23], is a widely used benchmark dataset consisting of 60,000 color images across 10 object categories. In this paper, we use 2D-ILCM encryption schemes on a CIFAR-10 dataset to generate 10000 ”plain-cipher” pairs of size 32×32. This dataset is used to improve training variety and facilitate multiple pooling for the network encoder. Training and testing sets are created by randomly dividing the ”plaintext-ciphertext”

pairs, with 8000 pairs used for training and 2000 pairs reserved for testing to evaluate our model's generalization.

3.2.2 Optimizer configuration

DL often uses the optimizer Adaptive Moment Estimation (Adam) to efficiently optimize network performance [24]. Similarly, we used Adam as an optimization strategy in our model, which updates the network weights during training at an adaptable learning rate, with a default value of 0.001. Additionally, all convolutional layers receive an L2 regularization with a weight decay of 0.001. Several datasets encrypted by 2D-ILCM scheme were used to test our model.

The model was implemented using the TensorFlow and Keras deep learning frameworks, and all experiments were conducted on a Windows-based workstation equipped with an NVIDIA RTX 3070 GPU with 8 GB RAM. The learning phase required around 27 minutes for 100 epochs. To prevent overfitting, we used early stopping with a patience of 20 epochs, and training was monitored using validation loss to ensure proper generalization.

3.2.3 Loss function

To assess the quality of the predicted image, we used the loss function mean squared error (MSE) [18], which computes the difference between the retrieved image and the plaintext (original image). It is described as:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(y_i - y_i'\right)^2 \tag{9}$$

Where n represents the plaintext pixels number, y_i is the original pixel value, and y_i' represents the output pixel value.

4. RESULTS AND DISCUSSION

4.1 Experimental Metrics

To evaluate the performance of our model, we used some metrics. The correlation coefficient (CC) [17] was used here to measure the similarity between original and retrieved images and it is calculated in the equation (10).

$$CC = \frac{\sum_m \sum_n \left(P - \overline{P}\right)(O - \overline{O})}{\sqrt{\sum_m \sum_n \left(P - \overline{P}\right)^2 \sum_m \sum_n \left(O - \overline{O}\right)^2}} \tag{10}$$

- n, m: the image dimensions.
- P, : the original and recovered images, respectively.

- $\overline{P}$, $\overline{O}$: their mean values.

For quantitative image quality evaluation, we used two known metrics; the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index (SSIM). SSIM concentrates on perceived visual quality by evaluating structural similarity across images, and it is computed as the equation (11):

$$SSIM\,(P,O) = \frac{\left(2\mu_p\mu_o + c_1\right)\left(2\sigma_{PO} + C_2\right)}{\left(\mu_P^2 + \mu_O^2 + C_1\right)\left(\sigma_P^2 + \sigma_O^2 + C_2\right)} \tag{11}$$

- μ_P, μ_O: the mean intensities of P and O,
- σ_P^2, σ_O^2: the variances,
- σ_{PO}: the covariance,
- C_1, C_2: constants used to stabilize the division.

While, PSNR compares the integrity of the reconstructed image to the original one, and it is calculated in equation (12):

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \tag{12}$$

MSE: the mean squared error between recovered and original images,

MAX_I : the image's maximum pixel value.

When combined, these three measures offer a thorough assessment of our cryptanalysis model's capacity to recreate plaintext images with both statistical and visual accuracy.

4.2 Experimental Results

4.2.1 The model visual evaluation

To illustrate the accuracy of the suggested deep learning-based attack technique, we analyzed the test set of CIFAR -10 images using our pre-trained CNN model. When analyzing the 2D-ILCM colored encryption algorithm, our model successfully reconstructs visually satisfactory images without requiring decryption keys, as shown in FIGURE 3, which illustrates six randomly selected images: row (I) shows the original clean images, (II) Encrypted images, and (III) the recovered images. The correlation coefficient (CC), which is shown under each image, is used to objectively determine the decryption quality. Our trained cryptanalysis model can reliably retrieve the unknown plaintext images with CC>=0.8.

4.2.2 Quantitative evaluation

As illustrated in FIGURE 4, the loss convergence curve demonstrates that MSE stabilizes at roughly 0.0095 after 300 epochs. This indicates that our model succeeds in breaking the 2D-ILCM en-

Figure 3: Ciphertexts and retrieved images using test data.

cryption algorithm. The MSE considerably decreases during the first 40 epochs that reflects quick learning during the initial training period. Then, the loss function slowly diminishes after 50 epochs with minor fluctuations, indicating that the network has found convergence with small MSE and it is now refining reconstruction details.

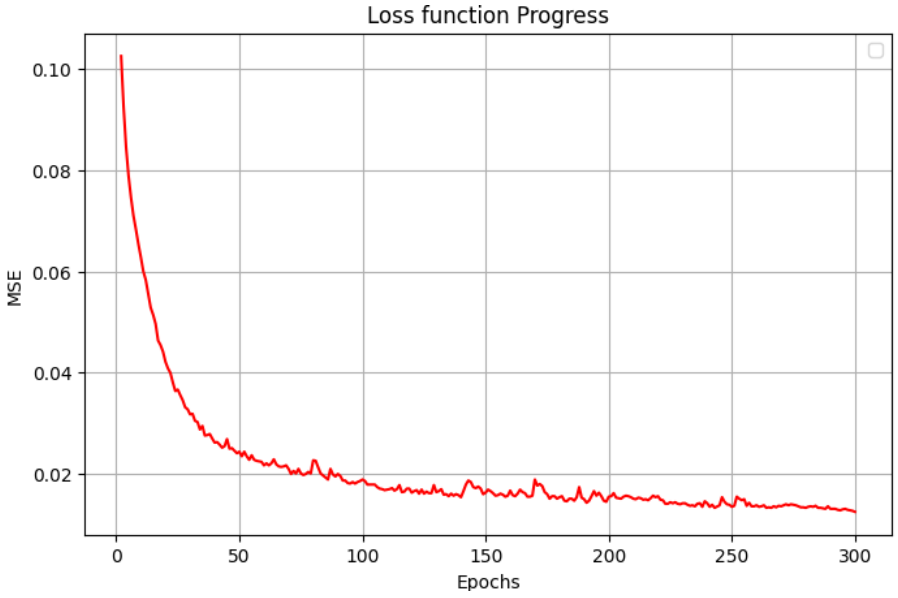

Figure 4: The MSE convergence curve during testing.

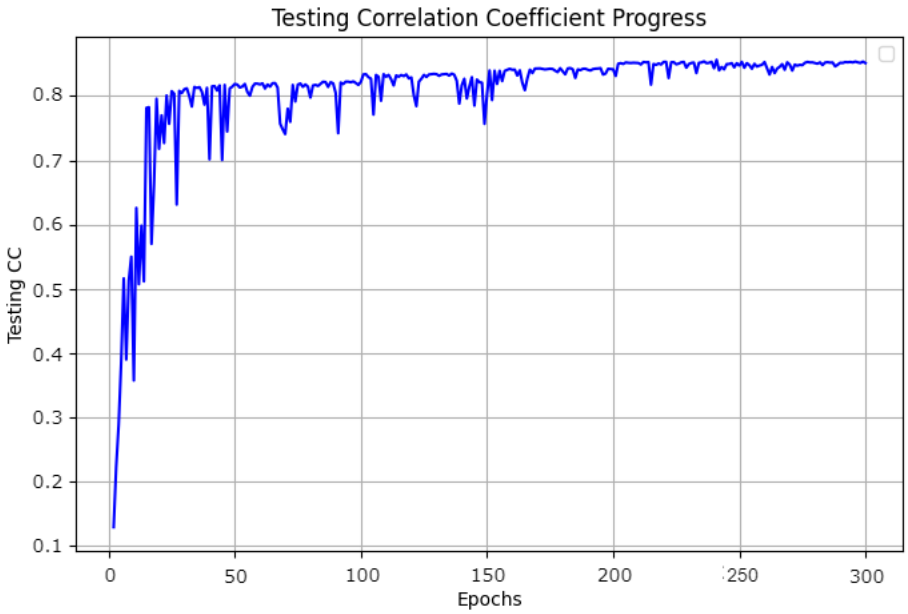

Figure 5: The CC evolution during testing phase.

FIGURE 5 shows the CC evolution during testing phase. We can see that the CC has increased and fluctuated over time, and the amplitude of the oscillations is gradually reducing. This shows that our model has successfully trained and stabilized its performance on the test dataset. The figure illustrates that CC increases considerably during the first 30 epochs, with a significant amplitude of fluctuation. After 40 epochs, it begins to stabilize and fluctuates between 0.7 and 0.8. Then, oscillations eventually fade until they are nearly nonexistent around 270 epoch. At the 300th epoch, CC has reached a value of 0.8514.

Three common image quality metrics were used to give a deeper understanding of our cryptanalysis method's efficacy; SSIM, PSNR, and CC. The performance of our cryptanalysis model when applied to the 2D-ILCM encryption method using CIFAR-10 dataset is summarized in TABLE 1. That provides the best and averaged values using 8,000 images for training process, and one thousand randomly selected test images for averaged results. Our model, as illustrated in TABLE 1, achieves PSNR = 19.23 dB, SSIM = 0.77, and CC = 0.848. These findings prove that our approach can successfully crack the 2D-ILCM scheme. The robustness and effectiveness of our deep cryptanalysis model is demonstrated by the consistently stable metric values. Also, our approach preserves both structural details and perceptual image quality while maintaining reliable decryption accuracy.

Table 1: Similarity metrics to evaluate the performance of the proposed cryptanalysis model.

	Dataset	Algorithm	PSNR	SSIM	CC
Averaged value	CIFAR-10	2D-ILCM [4]	19.23	0.77	0.848
Best value			23.12	0.89	0.934

Furthermore, two cryptographic metrics, unified average change intensity (UACI) and number of pixel change rate (NPCR), are used to evaluate the cryptographic sensitivity of the reconstructed images. These metrics determine the degree of difference between ecncrypted and recovered images in intensity and quantity at pixel level. They demonstrate the model's capacity to predict the original images without replicating the ciphertext by verifying that the retrieved images differ significantly from the input ciphertext.

The cryptographic performance of our proposed U-net model are illustrated in TABLE 2, that compares encrypted images to decrypted ones using basic 2D-ILCM against our cryptanalysis model. We achieve NPCR = 98.20% and UACI = 30.10%, which are slightly lower than the encryption system [4] but still within acceptable ranges. The reconstructed images match the original plaintext, but do not replicate the encrypted images' inherent unpredictability. These results show that the model remains cryptographically independent of the encrypted input and successfully learns to produce images whose structure and intensity distribution are consistent with the original plaintext. This demonstrates that U-Net is capable of approximating the underlying distribution of the plaintext while preserving the essential visual and statistical characteristics of the original images, instead of simply memorizing the patterns of the encrypted images.

Table 2: Evaluation of the proposed cryptanalysis model using cryptographic metrics compared with basic 2D-ILCM encryption values.

	NPCR (%)		**UACI (%)**	
Training Size	**2D-ILCM[4]**	**Cryptanalysis Model**	**2D-ILCM[4]**	**Cryptanalysis Model**
8,000	99.62	98.20	33.35	30.10

4.2.3 Robustness against noise and masking

We also examined our system robustness against noise attack. The encrypted images in FIGURE 6(I), 6(II) and 6(III) have been modified using gaussian noise with (0.1, 0.2, and 0.3) standard deviations. Their corresponding retrieved images are shown in FIGURE 6(IV), 6(V) and 6(VI). The CC values shown below each image are, on average, 0.815, 0.795, and 0.765, respectively. It is demonstrated that our suggested U-net deep learning network can extract enough information from ciphertext that has been affected by noise.

TABLE 3 uses the average PSNR over 1000 test images to quantify how robust the suggested U-Net cryptanalysis model is against Gaussian noise and partial occlusion. The model achieves 18.50 dB, 18.10 dB, and 17.60 dB for deviations of 0.1, 0.2, and 0.3, respectively. These results are lower than those of the original decryption system [4] but remain significant. The PSNR data reveal a slow but controlled deterioration, going from 18.08 dB to 17.03 dB for occlusion levels of 10%, 20%, and 30%. These findings verify that the suggested U-Net retains satisfactory reconstruction quality and shows robustness to both noise contamination and missing data, even with slight losses as compared to the reference scheme.

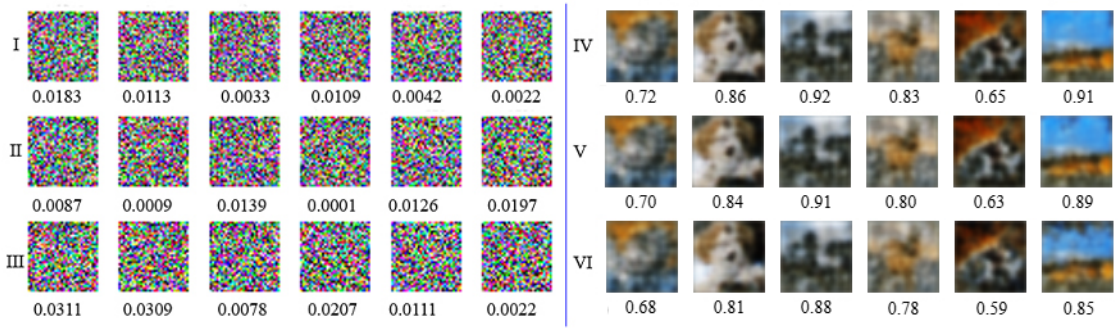

Figure 6: Robustness against noise attack. (I), (II) and (III) the affected ciphertexts. (IV), (V) and (VI) their corresponding retrieved images.

Table 3: Evaluation of the model's robustness face to noise and region masking in encrypted images: PSNR average over 1000 test images.

	Gaussian Noise (std)			**Occlusion (%)**		
Algorithm	**0.1**	**0.2**	**0.3**	**10**	**20**	**30**
Decryption Scheme [4]	26.41	25.33	24.58	25.07	24.19	23.22
Proposed Cryptanalysis Model	18.50	18.10	17.60	18.08	17.50	17.03

4.3 Security Implications

Our cryptanalysis model indicates a fundamental weakness in chaos-based image encryption. Despite the statistical unpredictability of encrypted images generated by the 2D-ILCM approach, our model successfully recovered a significant amount of visual information from encrypted images without prior knowledge of encryption keys or the system parameters. This indicates that statistical security cannot guarantee resistance to deep learning-based attacks. Furthermore, compared with existing approaches as illustrated in TABLE 4, the proposed method uniquely integrates dense connectivity and attention mechanisms for color image cryptanalysis, while providing a broader evaluation framework that includes both cryptographic and perceptual robustness metrics.

The results of the present research are a bit lower than those of our earlier work [21], which retrieved images with higher reconstruction fidelity. This disparity makes sense because 2D-ILCM strengthens the coupling between permutation and diffusion, making estimating the inverse mapping more challenging. Furthermore, using color image datasets increases structural complexity when compared to grayscale data. However, the recovery of structural content suggests that the underlying vulnerability is still present.

The deterministic character of chaotic maps is the source of the observed vulnerability; although producing intricate and seemingly random patterns, their transformations are nevertheless mathe-

Table 4: Comparison with Recent Deep Learning-Based Cryptanalysis Methods

Cryptanalysis approach	**Architecture**	**Encryption algorithm**	**Number of exemple**	**Dataset**	**Metrics Reported**	**Mean values**
Wang et al. [18]	U-Net	CIBOE	5	MNIST	CC	0.9205
				Fashion-MNIST	CC	0.9244
Liu et al. [19]	Pix2Pix GAN	CGI cryptosystem	100	FEI face	CC SSIM PSNR MSE	0.9934 0.9988 11.1788 0.0009
Fusen et al. [20]	IDEDNET	3 Chaotic Map	500	Mixed MNIST and Fashion-MNIST	CC	95.1% *
This work	**Dense Attention U-Net**	**2D-ILCM**	**1000**	**Cifar-10**	**CC** **SSIM** **PSNR** **NPCR** **UACI**	**0.848** **0.77** **19.23** **98.20** **30.10**

***** averaged value of 3 chaotic map

matically structured. A deep neural network can learn these hidden correlations and approximate the inverse mapping if it has access to a sizable enough collection of plaintext–ciphertext pairs.

As a result, in addition to conventional diffusion-confusion techniques, chaos-based encryption systems need to include other cryptographic protections. To withstand contemporary machine learning-driven cryptanalysis, it is especially important to improve key mixing, incorporate cryptographically robust substitution layers, or introduce controlled non-determinism.

5. CONCLUSION

This study analyzes the security of a chaos-based color image cryptosystem using a known-plaintext attack. To do this, we designed a CNN autoencoder model, which is trained on pairs of ciphertext-plaintext color images. Our approach combines an attention mechanism and denseblocks with a U-net architecture. We applied our model to the robust 2D-ILCM encryption algorithm. Experimental results on the Cifar-10 dataset demonstrated that 2D-ILCM may be broken, and high quality images can be retrieved using our DL cryptanalysis method. In general, this work presents a novel approach to evaluating the security of chaos-based encryption systems by utilizing deep learning techniques for cryptanalysis, which may also be applied to vulnerability analysis.

Overall, this work shows how deep learning methods might offer a fresh viewpoint on the security evaluation of encryption systems based on chaos. The proposed model's effectiveness as a useful

tool for identifying potential vulnerabilities is demonstrated by its capacity to reconstruct plaintext images with good precision even in the face of noise or partial missing data.

Future research should focus on improving current generalizations obtained with more complicated datasets, such as encrypted videos or high-resolution and real-world image datasets Such studies should strive to reduce the model's reliance on huge volumes of training data, enhance its resilience to adversarial perturbations, and use transformer-based designs to better capture global contextual information. Additionally, DL techniques create serious ethical concerns when applied to crypt-analysis because they can be used to both improve security and attack encryption systems. Then, it is crucial to develop stronger defense mechanisms to protect encryption systems from these assaults in order to guarantee data security.

References

[1] Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A. Color Image Encryption Through Chaos and KAA Map. IEEE Access. 2023;11:11541-11554.

[2] Pak C, Huang L. A New Color Image Encryption Using Combination of the 1D Chaotic Map. Signal Process. 2017;138:129-137.

[3] Pak C, An K, Jang P, Kim J, Kim S. A Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map. Multimed Tools Appl. 2019;78:12027-12042.

[4] Pak C, Kim J, Pang R, Song O, Kim H, et al. A New Color Image Encryption Using 2D Improved Logistic Coupling Map. Multimed Tools Appl. 2021;80:25367-25387.

[5] Demirtaş M. A New RGB Color Image Encryption Scheme Based on Cross-Channel Pixel and Bit Scrambling Using Chaos. Optik. 2022;265:169430.

[6] Huang Y, Zhang Q, Zhao Y. Color Image Encryption Algorithm Based on Hybrid Chaos and Layered Strategies. J Inf Secur Appl. 2025;89:103921.

[7] Salah RB, Zaied M. A Robust Medical Image Watermarking Approach Using Beta Chaotic Map DWT and SVD. In: 2023 international conference on cyberworlds (CW). IEEE. 2023:201-208.

[8] Fallah A, Zaied M. Image Encryption Based on Beta Discrete Wavelet Transform, New Beta Wavelet Chaotic Map, and Latin Square. In Fifteenth International Conference on Machine Vision. ICMV. SPIE. 2023;12701:480-487.

[9] Rim Z, Ridha E, Mourad Z. An Improved Partial Image Encryption Scheme Based on Lifting Wavelet Transform Wide Range Beta Chaotic Map and Latin Square. Multim Tools Appl. 2021;80:15173-15191.

[10] Benaissi S, Chikouche N, Hamza R. A Novel Image Encryption Algorithm Based on Hybrid Chaotic Maps Using a Key Image. Optik. 2023;272:170316.

[11] Fallah A, Hamdi M, Alturki N, Saidani O, Zaied M. Revolutionizing Image Encryption: Introducing the Beta Wavelet Map and DNA Coding Paradigm. IEEE Access. 2024;12:188349-188358.

[12] Dou Y, Li M. Cryptanalysis of a New Color Image Encryption Using Combination of the 1D Chaotic Map. Appl Sci. 2020;10:2187.

[13] Li M, Wang P, Liu Y, Fan H. Cryptanalysis of a Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map. IEEE Access. 2019;7:145798-145806.

[14] Wen H, Chen R, Yang J, Zheng T, Wu J, et al. Security Analysis of a Color Image Encryption Based on Bit-Level and Chaotic Map. Multimed Tools Appl. 2024;83:4133-4149.

[15] Zhou R, Yu S, Wang Q. Security Analysis of a Chaotic Encryption Algorithm Related to the Sum of Plaintext Pixel Value. Appl Phys B. 2023;129:92.

[16] Lin CY, Wu JL. Cryptanalysis and Improvement of a Chaotic Map-Based Image Encryption System Using Both Plaintext Related Permutation and Diffusion. Entropy. 2020;22:589.

[17] Hai H, Pan S, Liao M, Lu D, He W, et al. Cryptanalysis of Random-Phase-Encoding-Based Optical Cryptosystem via Deep Learning. Opt Express. 2019;27:21204-21213.

[18] Wang X, Wei H. Cryptanalysis of Compressive Interference Based Optical Encryption Using a U-Net Deep Learning Network. Opt Commun. 2022;507:127641.

[19] Liu X, Meng X, Wang Y, Yin Y, Yang X. Known-Plaintext Cryptanalysis for a Computational-Ghost-Imaging Cryptosystem via the Pix2Pix Generative Adversarial Network. Optics Express. 2021;29:43860-43874.

[20] Wang F, Sang J, Huang C, Cai B, Xiang H, et al. Applying Deep Learning to Known-Plaintext Attack on Chaotic Image Encryption Schemes. In ICASSP 2022-2022 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP). IEEE. 2022:3029-3033.

[21] Amiri S, Zaied M. Cryptanalysis of Chaos-Based Image Encryption Using DL Attack. Procedia Comput Sci. 2025;270:106-115.

[22] Huang G, Liu Z, Van Der Maaten L, Weinberger KQ. Densely Connected Convolutional Networks. In Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR).IEEE. 2017:4700-4708.

[23] https://www.cs.utoronto.ca/ kriz/learning-features-2009-TR.pdf

[24] D. P. Kingma and J. Ba, Adam: A Method for Stochastic Optimization. Proceedings of International Conference on Learning Representations. ICLR. 2015.