Secure Image Encryption via Image-Dependent Key Generation and High-Dimensional Chaos

Sharad Salunke[1], Arvind Kumar Tiwari [2]

[1,2]Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia, [2]Kamla Nehru Institute of Technology, Sultanpur, 228118, Uttar Pradesh, India;

Email ID [1] pdf.sharad@lincoln.edu.my, [2] arvind@knit.ac.in

---

Abstract: Images sent through systems of healthcare, surveillance, and defence and smart infrastructure must be encrypted with strength. Conventional cryptography algorithms are computationally complex and do not match the image properties. Most of the chaos-based encryption systems use fixed keys and this makes them less adaptive and prone to attacks. In this paper, a secure image encryption scheme that combines image-dependent key generation and high dimensional chaotic dynamics is proposed. The technique attaches image content to encryption keys based on the extraction of features, whereby each input should have a unique key. Chaotic generators of high dimension generate high-entropy keystreams, which are more difficult to confuse and mix. Experimental results indicate almost perfect entropy rate, great NPCR/UACI rates and the ability to resist noise and cropping attacks but still be computationally efficient to apply in real-time.

Keywords: Image Encryption; Image-Dependent Key Generation; High-Dimensional Chaos; Hyperchaotic Systems; Confusion and Diffusion; Differential Attack Resistance; Information Entropy; NPCR; UACI; Robust Image Security.

Introduction

Digital communication technologies allow exchanging visual data in a network, on cloud platforms, and edge devices in ways never seen before. Applications of images are very wide in telemedicine, biometric authentication, defense surveillance, and monitoring of smart infrastructure. But traditional crypto tools like AES and DES are computationally expensive and structurally inefficient with image properties like high pixel affinity, high degree of redundancy and massive data volumes [1]. Chaos-based image encryption methods have recently been of interest because of the nonlinearity, ergodicity and sensitivity to initial conditions [2]. Chaotic systems offer pseudo-random sequences which adds confusion and diffusion aspects. In addition to enhancing key space and dynamical complexity, hyperchaotic and multi-dimensional systems enhance the dynamical complexity [3]. The majority of the currently available schemes are however vulnerable to known-plaintext and chosen-plaintext attacks because they depend on fixed or image independent keys [4]. Recent studies put the focus on image-dependent and adaptive key generation schemes. The key dynamic strategies based on image content make images secure because each image generates a unique encryption key [5][6]. The proposed work is a secure image

encryption framework, which is an image-dependent key generation, which is combined with high-dimensional chaotic dynamics, which increases entropy, diffusion strength, and resistance to attacks with a significantly low computational complexity.

Related Work and Research Gap

Image encryption using chaos has become a force of study. High-dimensional and hyper chaotic systems overcome low-dimensional map key space limitations. Recent publications combine DNA-based encoding with chaos theory[7], but cryptanalysis shows that it might not be secure when key generation has not been done well[8]. Deep learning has been analyzed in the field of secure key generation and cryptographic enhancement with the help of biometrics [9][10]. In spite of such developments, there are critical limitations: Numerous plans are based on fixed or image independent keys minimizing uncertainty. Mechanisms that use static keys make it more vulnerable to known-plaintext attacks. Inappropriate choice of parameters can decrease productive key space. A lot of schemes show good results in ideal situations but fail in noisy situations and attacks by cropping. Pattern inference is more dangerous when encryption is performed in a static manner. This paper fills these gaps by coming up with a framework that ensures high plaintext-key coupling, high-dimensional chaotic dynamics to achieve a high key space, global diffusion, resistance to attacks, and computational efficiency.

Proposed Method

The framework combines image-dependent key generation with high-dimensional chaotic dynamics using five components, namely image feature extraction, image-dependent key generation, high-dimensional chaotic sequence generation, confusion stage and diffusion stage.

Brief steps are as follows;

- Image dependent key seed to high dimensional chaotic system parameters - extract features (mean, variance, pixel sum) to image - hash - 256 bit image dependent key seed.
- Generate chaotic sequence → derive permutation indices and keystream $\{\{K_i\} \rightarrow$ permute pixels (confusion) → get P_i.
- Diffuse intensities using

$$C_i = (P_i \oplus K_i \oplus C_{i-1}) mod 256 \quad (1)$$

To get encrypted image; decryption uses inverse diffusion and inverse permutation where the same image dependent parameters are used

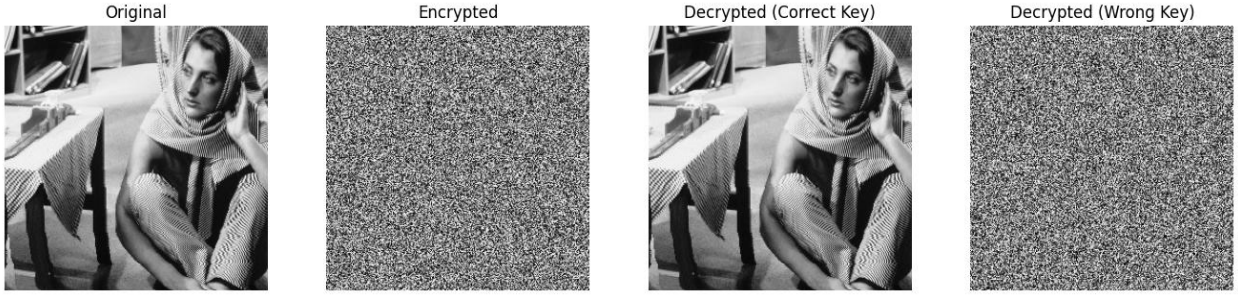

Fig:2 Encryption and decryption results on test images.

Experimental Results

The standard grayscale benchmark images of 512 x 512 which were used to implement the framework are Barbara, Penguin and Airplane as demonstrated in figure 1. The metrics of evaluation are histogram analysis, correlation coefficient, information entropy, metric of differential attack (NPCR/UACI) and robustness tests.

I. Statistical Security Analysis

Encrypted images are totally distorted in their visuals and do not have any structural similarity with original ones. Histogram distributions depict that there is close uniformity in all the levels of intensities, indicating high levels of randomness. Table 1 summarizes the values of entropy of test images.

Table 1: Information entropy comparison

Image	Entropy (Original)	Entropy (Encrypted)
Barbara	7.42	7.997
Penguin	7.18	7.996
Airplane	7.36	7.998

Encrypted entropy values are as close to theoretical maximum of 8 bits that reflects great randomness. Correlation coefficients of the adjacent pixels were calculated with original and encrypted images. In the case of Barbara image, the horizontal correlation was reduced to 0.003 as compared to its initial 0.945, the vertical correlation was reduced to -0.002 as compared to its initial 0.932, and the diagonal correlation was reduced to 0.001 as compared to its initial value of 0.910. Other test images had similar trends ensuring successful disruption of spatial dependency.

II. Differential Attack Analysis

Differential analysis was tested by altering one pixel in the original picture and testing the effect on the ciphertext. Results are shown in Table 2.

Table 2: NPCR and UACI results

Image	NPCR (%)	UACI (%)
Barbara	99.5819	33.5352
Penguin	99.6246	33.4517
Airplane	99.5880	33.4675
Baboon	99.6475	33.5846

The values of NPCR are over 99, whereas the values of UACI are around 33, which indicates high sensitivity and diffusion.

III. Robustness Analysis

Salt and Pepper noise (2 percent density) and 25 percent cropping attacks tests were robustness tests. In noise attacks, values of PSNR of 21-22 dB with SSIM values of 0.71-0.79 denotes a moderate distortion

with an ability to capture structure. In the case of cropping attacks, SSIM values of over 0.93 assure the structural integrity is not compromised with the loss of information. It is characterized by a controlled global degradation as a result of feedback-based diffusion mechanism and therefore it is appropriate to transmit in real time over noisy channels.

Discussion

As shown by the experimental outcomes, the combination of the process of the image-dependent key generation with the high-dimensional chaotic dynamics is quite helpful in improving security performance. Close interaction between plaintext and key-ceasing resists minor changes on the plaintext cause a whole orbit of chaotic trajectories, making it impossible to reuse keys and to mount an adaptive modeling attack. Strong diffusion property and good statistical security are verified by achieved entropy values that are above 7.99 bits, correlation coefficients that are close to zero, NPCR values that are above 99.6, and UACI values that are close to 33%.

The framework also has a controlled degradation to noise and cropping attacks, which has been useful in wireless transmission setting as well as real-time multimedia. In contrast to structurally delicate schemes, which aggravate the overhead of the algorithm, the suggested model is computationally efficient with image-dependent key seeding with lightweight chaotic iteration.

Conclusion

The paper introduces a safe image encryption system that offers customary key creation to each input image, giant key area, using high-dimensional chaos, close to ideal entropy values, high decorrelation, and structural resistance to assaults. The hybrid scheme attains a moderate trade-off between the security strength and the computation efficiency and offers a scalable solution to support secure real-time transmission of images in the new digital systems.

References

[1] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, no. 4, pp. 917-935, 2022.

[2] A. Dinu and M. Frunzete, "Image encryption using chaotic maps: Development, application, and analysis," *Mathematics*, vol. 13, no. 16, 2588, 2025.

[3] M. Huo, Y. Zheng, and J. Huang, "Enhancing AES image encryption with a three-dimensional hyperchaotic system for increased security and efficiency," *PLOS ONE*, vol. 20, no. 7, e0328297, 2025.

[4] W. Feng et al., "A novel multi-channel image encryption algorithm leveraging pixel reorganization and hyperchaotic maps," *Mathematics*, vol. 12, no. 24, 3917, 2024.

[5] C. Lin, G. Hu, C. Chan, and J. Yan, "Chaos-based synchronized dynamic keys and their application to image encryption with an improved AES algorithm," *Applied Sciences*, vol. 11, no. 3, 1329, 2021.

[6] S. W. Jirjees, F. F. Alkalid, and W. F. Shareef, "Image encryption using dynamic image as a key based on multilayers of chaotic permutation," *Symmetry*, vol. 15, no. 2, 409, 2023.

[7] L. Huang, C. Ding, Z. Bao, H. Chen, and C. Wan, "A DNA encoding image encryption algorithm based on chaos," *Mathematics*, vol. 13, no. 8, 1330, 2025.

[8] Y. Zhao, Q. Shi, and Q. Ding, "Cryptanalysis of an image encryption algorithm using DNA coding and chaos," *Entropy*, vol. 27, no. 1, 40, 2025.

[9] Y. Wang, B. Li, Y. Zhang, J. Wu, and Q. Ma, "A secure biometric key generation mechanism via deep learning and its application," *Applied Sciences*, vol. 11, no. 18, 8497, 2021.

[10] H. B. Hwang et al., "Preliminary study of novel bio-crypto key generation using clustering-based binarization of ECG features," *Sensors*, vol. 24, no. 5, 1556, 2024.