ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-201808.00075

Adaptive Color Image Encryption Algorithm Based on Improved Cat Scrambling and Henon_Kent Chaotic System: Postprint

Authors: Xie Guobo, Zhiwei Chen

Date: 2018-08-13T00:00:00+00:00

Abstract

To address the security deficiencies arising from insufficient correlation between keys and plaintext images in color image encryption algorithms, as well as the validity conditions of Cat mapping, a color image adaptive encryption algorithm based on an improved Cat scrambling system and a Henon_Kent chaotic diffusion system is proposed. The algorithm first generates keys from the feature information of the plaintext image; then performs three-dimensional scrambling of pixel positions via the improved Cat scrambling system; subsequently employs three chaotic sequences produced by the Henon_Kent chaotic system to diffuse the pixel grayscale values of the three RGB channels, respectively; and repeats these two steps until the information entropy of the ciphertext image exceeds 7.99. Simulation results demonstrate that the algorithm can resist existing attack methods and exhibits strong encryption performance.

Full Text

Preamble

Color Image Adaptive Encryption Algorithm Based on Improved Cat Scrambling and Henon_Kent Chaotic System

Xie Guobo, Chen Zhiwei
(School of Computers, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: To address the security deficiencies arising from the lack of association between keys and plaintext images in color image encryption algorithms, as well as the conditional constraints of Cat maps, this paper proposes a color image adaptive encryption algorithm based on an improved Cat scrambling system and Henon_Kent chaotic diffusion system. The algorithm first generates

keys using feature information from the plaintext image. It then performs three-dimensional pixel position scrambling on the image through an improved Cat scrambling system, followed by diffusing the pixel gray values of the three RGB channels using three chaotic sequences generated by the Henon_Kent chaotic system. These two steps are repeated until the information entropy of the ciphertext image exceeds 7.99. Simulations demonstrate that the proposed algorithm can resist existing attack methods and exhibits strong encryption performance.

Keywords: image encryption; cat scrambling; Henon_Kent chaotic system; adaptive encryption

0 Introduction

In recent years, the Internet has been widely applied in people' s work and daily life, encompassing the transmission of digital audio, digital images, and other multimedia information. Consequently, the secure transmission of digital images has become increasingly important. Traditional encryption algorithms such as AES (Advanced Encryption Standard), DES (Data Encryption Standard), and RSA (public-key cryptography) require substantial computational time for image data and pose potential security risks. Chaotic systems, characterized by their pseudo-randomness and sensitivity to initial values, have inspired numerous image encryption algorithms proposed by scholars. However, algorithms using single low-dimensional chaos suffer from small key spaces and poor security, making them vulnerable to common attacks.

To enhance security, literature [5] proposed a color image encryption algorithm using two chaotic systems, which increases the key space. However, since color images only undergo one-dimensional and two-dimensional position scrambling, the security needs further improvement. Literature [6] presented an image encryption algorithm based on 3D Cat mapping, extending two-dimensional images to three dimensions for 3D Cat mapping. Yet, the encryption key was not associated with the plaintext image, making it ineffective against chosen ciphertext (plaintext) attacks. Literature [7] introduced a new block image encryption scheme based on hybrid chaotic mapping and dynamic random growth technology, which solved the periodicity problem of Cat mapping and effectively resisted chosen plaintext attacks. However, for equal-length images where the determinant of the scrambling transformation matrix is not coprime with n, or for non-equal-length images with non-integer m/n ratios, two-dimensional Cat mapping cannot establish a one-to-one correspondence, causing repeated mapping positions and pixel loss. Literature [8–10] addressed the conditional constraints of Cat mapping by adding rows and columns to form an $M \times M$ image, but this operation increases the storage size of the ciphertext image and proportionally increases the resources required for network communication.

To overcome these limitations—specifically the lack of association between keys and plaintext images and the conditional constraints of Cat scrambling—this

paper proposes a color image adaptive encryption algorithm based on an improved Cat scrambling system and Henon_Kent chaotic diffusion system. The improved Cat scrambling system modifies the one-to-one mapping rule of three-dimensional Cat mapping to grayscale value swapping, thereby resolving the periodicity and conditional constraints of Cat mapping. The proposed encryption algorithm first utilizes feature information from the color plaintext image to generate keys for the composite chaotic system. It then scrambles the color plaintext image pixels through the improved Cat scrambling system in three-dimensional space, distributing grayscale values uniformly across the R, G, and B components. Subsequently, the Henon_Kent chaotic system generates three chaotic encryption sequences to diffuse the pixel grayscale values of the three channels. These two steps are repeated until the security analysis of the ciphertext image meets specific standards. The algorithm adopts an adaptive cyclic structure of three-dimensional space scrambling followed by pixel diffusion. Experimental simulations demonstrate that the proposed algorithm exhibits robust resistance against statistical analysis attacks and differential attacks.

1 Principles of the Proposed Encryption Algorithm

This paper proposes a color image adaptive encryption algorithm based on an improved Cat scrambling system and Henon_Kent chaotic diffusion system, with the overall process illustrated in [Figure 1: see original paper]. The algorithm comprises four main components: (a) plaintext-image-related key generation; (b) improved Cat system scrambling; (c) Henon_Kent chaotic diffusion; and (d) adaptive loop judgment.

1.1 Plaintext-Image-Related Key Generation

Unlike conventional methods where encryption keys are directly generated, the keys in this algorithm are associated with plaintext features. From Equation (1), we obtain the sum of pixel grayscale values with position parameters for matrix A as *sum*. Equations (2)-(5) derive the initial values for the improved three-dimensional Cat scrambling system. The specific steps are as follows:

a) Select parameters for Equation (7) using Equations (2)-(4):
k , k , k , a , a , a

b) The key generation process utilizes the feature information of the plaintext image to produce composite chaotic system keys, ensuring a strong association between the encryption key and the plaintext characteristics.

1.2 Improved Cat System Scrambling

The two-dimensional generalized Cat map, also known as the Arnold map, is expressed by Equation (6), where (x, y) represents the original pixel position of the grayscale image, and N denotes the domain limitation. The condition for two-dimensional generalized Cat mapping requires that the determinant of the

scrambling transformation matrix and n be coprime for equal-length images, or that m/n be an integer ratio for non-equal-length images; otherwise, Cat transformation exhibits periodicity [11].

To address the conditional constraints of Cat mapping, this paper proposes an improved three-dimensional Cat scrambling system. This system employs three-dimensional Cat mapping [12] and modifies the one-to-one mapping rule to grayscale value swapping, thereby resolving the periodicity and conditional constraints of Cat mapping. The definition is given by Equation (7).

For a color image of size $m\times n\times 3$ with pixel position $(x,\ y,\ z)$, the three-dimensional matrix is transformed. For algorithmic convenience, let matrix A represent the $m\times n\times 3$ color plaintext image. The position $(x,\ y,\ z)$ calculated through Equation (7) yields $(x\ ,\ y\ ,\ z\ )$. The grayscale values of pixels at $(x,\ y,\ z)$ and $(x\ ,\ y\ ,\ z\ )$ are exchanged rather than performing matrix mapping. The improved three-dimensional Cat exchange is non-periodic; after multiple iterations, image pixels become uniformly distributed across the R, G, and B components with strong decorrelation, achieving superior encryption effects and attack resistance.

The specific steps are as follows:

a) Select parameters for Equation (7) using Equations (2)-(4): $a\ ,\ a\ ,\ a\ ,\ k\ ,\ k\ ,\ k\ .$

b) Starting from position (1,1,1) to $(m,\ n,\ 3)$ in matrix A, following the row-major, column-secondary, and RGB-last principle, the position $(u,\ v,\ w)$ in matrix A is calculated through Equation (7) to obtain $(u\ ,\ v\ ,\ w\ )$. The grayscale values $A(u,\ v,\ w)$ and $A(u\ ,\ v\ ,\ w\ )$ are then swapped.

c) The scrambled image A is converted into three two-dimensional grayscale matrices $A\ ,\ A\ ,\ A$ corresponding to the R, G, and B components, each of size $m\times n$.

1.3 Henon_Kent Chaotic Diffusion

The Henon map exhibits stronger sensitivity to initial conditions and better dynamical system characteristics compared to conventional maps, defined by Equation (8). The Kent map is a one-dimensional chaotic system defined by Equation (9), where d is the control parameter. When d (0,1], the Kent map possesses a positive Lyapunov exponent, indicating chaotic behavior.

The Henon_Kent chaotic system proposed in this paper combines two chaotic sequences generated by the Henon map and one chaotic sequence from the Kent map to produce three hybrid chaotic sequences, as defined by Equation (10). The generated chaotic sequences have a value range within [0,1]. The Henon_Kent map uses control parameters , , and ; the mod operation denotes the modulo operation; $k\ ,\ k\ ,$ and k are control parameters for the Henon map. A chaotic system must have at least one positive Lyapunov exponent. Sys-

tems in stable steady states or periodic motion cannot possess positive Lyapunov exponents. The Henon system has two positive Lyapunov exponents, and the Henon_Kent system can significantly enhance the sensitivity of the R, G, and B components to the key for color image encryption. The generated chaotic sequences are more sensitive to initial states than those from non-combined multi-chaotic systems, thereby improving the overall security of the encryption algorithm. Simulation of the Henon_Kent chaotic system for 1,000 iterations is shown in [Figure 2: see original paper].

The specific steps are as follows:

a) Select appropriate parameters and initial values for the Henon map in Equation (8) and Kent map in Equation (9). Using Equation (5) to calculate the Kent map initial value k , iterate s times to eliminate transient effects, then iterate $m \times n$ times to obtain three chaotic sequences of length $m \times n$. Apply Equation (10) with specific parameters , , to operate on the three sequences, forming three two-dimensional matrices of size $m \times n$. Perform XOR operations between these matrices and the pixel grayscale values of A , A , A to generate three intermediate ciphertext components M , M , M .

1.4 Adaptive Loop Judgment

To achieve adequate scrambling and diffusion of the plaintext color image while preventing excessive computational cycles, this algorithm employs the information entropy of the ciphertext image as the criterion for encryption effectiveness.

Information entropy measures the distribution of image grayscale values. Higher entropy indicates more uniform distribution. The formula is given by Equation (11), where $P(i)$ represents the probability of grayscale value i appearing. When the ciphertext image' s information entropy approaches 8, it demonstrates pseudo-randomness and high security, indicating the encryption algorithm can resist entropy attacks.

The specific steps are as follows:

a) Obtain intermediate ciphertext components M , M , M and calculate their information entropies $H(M$), $H(M$), $H(M$) using Equation (11). When all three values exceed 7.99, the cyclic algorithm terminates, with the number of cycles t serving as a key. Otherwise, repeat the improved Cat system scrambling and Henon_Kent chaotic diffusion while incrementing $t = t + 1$.

1.5 Ciphertext Decryption Process

The image decryption process is the inverse of the encryption steps described above.

2 Experimental Simulation and Security Analysis

The algorithm simulation employs a 256×256×3 color Lena image (Figure 3: see original paper) and a 500×400×3 color Lena image (Figure 3: see original paper) as plaintext images. For comparative analysis with other algorithms, the security analysis primarily uses Figure 3: see original paper with Figure 3: see original paper as supplementary. The algorithm keys are: Henon map initial values (x , y) = (0.501334562, 0.554157444) with control parameter a = 1.2, Kent map initial value k = 0.6006 with control parameter d = 0.3, and Henon_Kent diffusion control parameters = 10 , = 10 , = 10 . The improved three-dimensional Cat scrambling uses control parameters a = 10, a = 10, a = 10, k = 10, k = 10, k = 10, and other parameters x = 0, y = 0, z = 0, x = 0, y = 0, z = 0. The final cycle count is t = 2. The ciphertext image from plaintext Figure 3: see original paper is shown in Figure 3: see original paper, and the ciphertext from Figure 3: see original paper is shown in Figure 3: see original paper.

2.1 Image Statistical Histograms

The statistical histogram of plaintext image Figure 3: see original paper is shown in [Figure 4: see original paper], the histogram of ciphertext image Figure 3: see original paper in [Figure 5: see original paper], the histogram of plaintext Figure 3: see original paper in [Figure 6: see original paper], and the histogram of ciphertext Figure 3: see original paper in [Figure 7: see original paper]. The results demonstrate uniform distribution across R, G, and B component histograms with similar statistical totals for each grayscale value, thereby achieving the encryption objective.

2.2 Adjacent Pixel Correlation Analysis

Adjacent pixel correlation analysis calculates the correlation coefficients of neighboring pixels in horizontal, vertical, and diagonal directions. Lower correlation coefficients (approaching zero) in the encrypted ciphertext indicate effective encryption and strong resistance to statistical attacks based on adjacent pixel correlations. The correlation coefficient calculation formulas are given by Equations (12)-(15), where represents the adjacent pixel correlation coefficient.

The correlation coefficients for the ciphertext image using the proposed algorithm are compared with those from literature [13] and [14] in . The encrypted ciphertext image correlation coefficients are close to 0, with many values smaller than those in literature [13] and [14]. Therefore, the proposed encryption algorithm demonstrates stronger resistance to correlation analysis attacks.

2.3 Key Space Analysis

This encryption algorithm employs multiple rounds and multiple chaotic systems for color image encryption. The improved three-dimensional Cat scrambling

algorithm uses long integer-type keys, while the Henon_Kent chaotic system uses double-precision operations. The key space for control parameters a , a , a , k , k , k in the improved three-dimensional Cat scrambling algorithm is 10 . The pixel diffusion algorithm' s Henon map initial values x and y provide a key space of 10^2 , with control parameter a offering 10^1 possibilities. The Kent map initial value k contributes a key space of 10^1 . The control parameters , , and in Equation (10) provide a key space of 10 .

The algorithm' s keys are associated with plaintext pixel grayscale values. For a 256×256×3 color Lena image, randomly selecting one pixel and incrementing it by 1 creates a new image A . Calculating NPCR and UACI between A and A yields average values shown in , along with values from literature [15]. The proposed algorithm achieves NPCR > 99.6% and UACI > 33.3%, demonstrating high sensitivity to plaintext characteristics. The key space approaches 10^2 , effectively resisting brute-force attacks and enhancing algorithm security.

2.4 Plaintext Sensitivity Analysis

Plaintext sensitivity analysis measures the drastic changes in encrypted images when pixel grayscale values undergo 微小 modifications. The changes are typically evaluated using NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity), calculated by Equations (16) and (17). $D(i,j)$ indicates whether pixels at position (i,j) in images A and A have identical grayscale values.

The proposed algorithm demonstrates high plaintext sensitivity, with NPCR and UACI values significantly exceeding theoretical thresholds, indicating that minute changes in plaintext produce substantially different ciphertexts.

2.5 Key Sensitivity Analysis

Key sensitivity refers to the inability to recover plaintext feature information when keys are slightly modified. Rigorous simulations were conducted by independently and subtly altering all keys. The decryption results for Figure 3: see original paper with modified keys are shown in [Figure 8: see original paper]: (a) and (b) show results when Henon map initial values in Equation (8) are modified to $x = 0.501934561$ and $x = 0.501934562$, respectively, with control parameters $a = 1.25$ and $a = 1.26$; (c) and (d) show decryption results when diffusion control parameters $d = 0.4$ and $d = 0.5$ are modified; (e) shows the result when Cat scrambling control parameter = 10 + 1 is modified; (f) shows the correct decryption. These results demonstrate that any slight key modification prevents successful decryption, confirming the algorithm' s high key sensitivity.

2.6 Cropping Resistance Analysis

Cropping resistance analysis simulates local information loss during image transmission. The ciphertext image Figure 3: see original paper was subjected to 25%

and 50% cropping, as shown in Figure 9: see original paper and (c), with decrypted results in Figure 9: see original paper and (d). Additionally, Figure 9: see original paper shows the ciphertext with the R component set to 255, and Figure 9: see original paper its decrypted result. The simulations demonstrate that the encryption/decryption algorithm can recover images despite information loss during transmission, with decrypted results revealing partial plaintext information. This analysis also confirms the algorithm' s resistance to noise attacks.

3 Conclusion

This paper proposes a color image adaptive encryption algorithm based on an improved Cat scrambling system and Henon_Kent chaotic diffusion system. Compared with other encryption algorithms, the proposed method features: (a) An improved Cat scrambling algorithm for color images that resolves the conditional constraints and periodicity issues of traditional Cat mapping, enabling pixel scrambling without changing image dimensions, with pixels becoming more randomly distributed across R, G, and B components as iteration count increases; (b) A novel Henon_Kent chaotic system that generates chaotic sequences with stronger dynamical characteristics and pseudo-randomness, effectively diffusing plaintext image pixels to achieve uniform distribution across [0,255]. Simulations demonstrate that the algorithm exhibits strong robustness and resistance against various attack methods.

References

[1] El-Assad S, Farajallah M. A new chaos-based image encryption system [J]. Signal Processing Image Communication, 2016, 41: 144-157.
[2] Liu Hongjun, Wang Xingyuan. Color image encryption based on one-time keys and robust chaotic maps [J]. Computers & Mathematics with Applications, 2010, 59(10): 3320-3327.
[3] Wang Xingyuan, Yang Lei, Liu Rong, et al. A chaotic image encryption algorithm based on perceptron model [J]. Nonlinear Dynamics, 2010, 62(3): 615-621.
[4] Liu Hongjun, Wang Xingyuan, Kadir A. Image encryption using DNA complementary rule and chaotic maps [J]. Applied Soft Computing, 2012, 12(5): 1457–1466.
[5] Wang Leyuan, Song Hongjun, Liu Ping. A novel hybrid color image encryption algorithm using two complex chaotic systems [J]. Optics & Lasers in Engineering, 2016, 77: 118-125.
[6] Chen Guanrong, Mao Yaobin, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos Solitons & Fractals, 2004, 21(3): 749-761.
[7] Wang Xingyuan, Liu Lintao, Zhang Yingqian. A novel chaotic block image encryption algorithm based on dynamic random growth technique [J]. Optics & Lasers in Engineering, 2015, 66: 10-18.
[8] Ding Ma, Jing Fan. Digital image encryption algorithm based on improved

Arnold transform [C]//Proc of International Forum on Information Technology and Applications. Piscataway, NJ: IEEE Press, 2010: 174-176.
[9] Li Guohui, Zhang Songling, Wu Chengmao. An image encryption algorithm based on improving spatiotemporal chaos [J]. Journal of Xian University of Posts & Telecommunications, 2017, 22(3): 44-49.
[10] Tian Hanqing, Quan Jicheng, Cheng Hong, et al. An image encryption scheme combining cat map and henon map [J]. Computer Applications & Software, 2010, 27(9): 286-288.
[11] Zhao Liping, Tan Zheng, Gao Hongjiang, et al. 2-D Arnold transformation and non-equilateral image scrambling transformation [J]. Acta Electronica Sinica Computer, 2007, 35(7): 1290-1294.
[12] Mohamed N A, El-Azeim M A, Zaghloul A, et al. Image encryption scheme for secure digital images based on 3D cat map and Turing machine [C]//Proc of the 7th International Conference of Soft Computing and Pattern Recognition. Piscataway, NJ: IEEE Press, 2015: 230-234.
[13] Wu Xiangjun, Wang Dawei, Kurths J, et al. A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system [J]. Information Sciences, 2016, 349: 137-153.
[14] Tong Xiaojun, Zhang Miao, Wang Zhu, et al. A joint color image encryption and compression scheme based on hyper-chaotic system [J]. Nonlinear Dynamics, 2016, 84(4): 2333-2356.
[15] Niyat A Y, Moattar M H, Torshiz M N. Color image encryption based on hybrid hyper-chaotic system and cellular automata [J]. Optics & Lasers in Engineering, 2017, 90: 225-237.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv —Machine translation. Verify with original.