ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-201810.00067

A Hyperchaos-Based Image Zero-Watermarking Algorithm Postprint

Authors: Zhang Haitao, Zhang Sibo

Date: 2018-10-11T00:00:00+00:00

Abstract

Hyperchaotic systems exhibit characteristics of large key space and high sensitivity to initial values, and with improvements made to their formulas, they possess certain advantages. To address the issues of poor robustness and low security in existing zero-watermarking algorithms, this paper proposes a hyperchaotic-based image zero-watermarking algorithm. First, the Chen three-dimensional hyperchaotic system is utilized to perform encryption preprocessing on the watermark information. By analyzing the impact of each bit plane on the image after decomposition, the least significant bit of the carrier image is initialized to zero. The block mean binary quantization method is employed for feature extraction. Finally, the zero watermark is obtained by performing XOR processing on the encrypted watermark and the feature matrix after Arnold scrambling. Simulation attack experiments and comparisons with previous zero-watermarking algorithms demonstrate that the algorithm maintains good robustness while being able to resist various attacks such as noise attacks, filtering attacks, compression attacks, and cropping attacks.

Full Text

A Hyper-Chaos-Based Zero-Watermarking Algorithm for Images

Zhang Haitao, Zhang Sibo
(College of Software, Liaoning Technical University, Huludao, Liaoning 125105, China)

Abstract: Hyperchaotic systems exhibit certain advantages due to their large key space and extreme sensitivity to initial values. This paper addresses the limitations of existing zero-watermarking algorithms, specifically their poor robustness and low security, by proposing a novel hyper-chaos-based image zero-watermarking algorithm. The approach employs the Chen three-dimensional

hyperchaotic system to encrypt watermark information as a preprocessing step. By analyzing the influence of each bit plane on the image after decomposition, the least significant bit (LSB) of the carrier image is initialized to zero. Feature extraction is performed using block mean binary quantization, and the final zero watermark is obtained through XOR operations between the encrypted watermark and the Arnold-scrambled feature matrix. Simulation experiments and comparative analysis with previous zero-watermarking algorithms demonstrate that the proposed algorithm maintains robust performance while effectively resisting various attacks, including noise, filtering, compression, and cropping attacks.

Keywords: hyper-chaos encryption; Chen chaotic system; robustness; zero watermarking

0 Introduction

With the rapid development of internet and multimedia technologies, digital content distribution has become increasingly convenient. However, this convenience also introduces significant security risks, as unauthorized individuals may steal, tamper with, or illegally distribute digital images and videos, causing substantial economic losses and social harm. Network transmission introduces additional uncertainties such as noise interference, image distortion, and packet loss, making it difficult for recipients to verify the authenticity and integrity of received data. Consequently, digital image copyright protection has emerged as a critical research priority.

Chaos-based cryptography was first proposed by Matthews in 1989, leveraging the extreme sensitivity of chaotic dynamical systems to initial conditions. Minute variations in initial values produce dramatically different chaotic sequences through complex dynamical behaviors. While chaotic systems follow deterministic equations, their unpredictable dynamics provide robust security guarantees. As system dimensionality increases, the dynamical behavior becomes more complex and harder to predict. The Chen chaotic system represents a classical three-dimensional chaotic system characterized by complex structure, abundant sequence generation, and enhanced randomness, making it particularly suitable for cryptographic applications. Its multi-parameter, multi-initial-value configuration significantly expands the key space, offering substantial advantages for encryption system design.

Numerous studies have investigated chaos-based watermarking algorithms. Wu Danhui and Zheng Enrang proposed an image watermarking algorithm based on logistic and Arnold dual chaotic encryption to address robustness issues. Ji Nuoran, Lyu Xiaoqi, and colleagues developed a Contourlet-domain color image watermarking scheme combining QR codes with chaotic encryption to improve resistance against geometric attacks and capacity limitations. Qu Changbo, Yu Zhilong, and Li Dongdong constructed a robust zero-watermarking algorithm using ridgelet transform, block-based FRIT-SVD, and bit-plane techniques. Qu

Changbo and Wu Deyang presented a strong robust zero-watermarking approach combining Curvelet-DSVD with visual cryptography and Arnold scrambling. While these methods utilize low-dimensional chaotic maps to enhance watermark robustness and security, this paper introduces a dimensionality reduction technique for the Chen three-dimensional chaotic system, transforming it into a one-dimensional system to generate encryption sequences. By analyzing the impact of bit-plane decomposition on image quality and initializing the LSB to zero, the algorithm employs block mean quantization for feature extraction. The feature matrix undergoes Arnold transformation before XOR operation with the encrypted watermark to construct the zero watermark. Experimental results demonstrate that this approach achieves excellent robustness against multiple attack types.

1.1 Watermark Preprocessing

The Chen chaotic system is described by the following dynamical equations:

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = (c - a)x - xz + cy \\ \frac{dz}{dt} = xy - bz \end{cases}$$

To enhance sensitivity to initial values, the system is reduced to a one-dimensional chaotic map using the following dimensionality reduction model:

$$L(k) = H \cdot \text{floor}(C \cdot k \cdot z(k)) + x(k) + y(k) + z(k), \quad k = 0, 1, 2, \ldots, N \times N$$

where $x(k)$, $y(k)$, and $z(k)$ represent the three state variables at iteration k, and H, C are control parameters. The factor H dramatically amplifies initial value sensitivity, while C provides moderate amplification, making the resulting one-dimensional map more sensitive than the original Chen system.

The algorithm selects a binary watermark image of size $N \times N$ with initial values x_0, y_0, and z_0 stored as key K_1. Starting from these initial values, the Chen system generates three chaotic sequences $x(k)$, $y(k)$, and $z(k)$. To ensure the reduced-dimensional sequence maintains superior hyperchaotic properties and good diffusion uniformity, the parameter $C = 1.27$ is selected. The resulting hyperchaotic sequence is illustrated in [Figure 1: see original paper].

Since one-dimensional chaotic maps exhibit simpler dynamical behavior compared to high-dimensional systems, the algorithm employs the Chen three-dimensional system for two-dimensional image encryption. The sequence $L(k)$ is first reshaped into a two-dimensional matrix $LL(k)$ of size $N \times N$:

$$LL = \text{reshape}(L, N, N)$$

Binary quantization is then performed using:

$$ml = \text{mean}(LL)$$

$$J(i,j) = \begin{cases} 1, & \text{if } LL(i,j) > ml \\ 0, & \text{otherwise} \end{cases}$$

The final encrypted watermark $C(i,j)$ is obtained through XOR operation with the original binary watermark $W(i,j)$:

$$C(i,j) = J(i,j) \oplus W(i,j)$$

The complete watermark encryption preprocessing flowchart is shown in [Figure 2: see original paper].

1.2 Feature Matrix Extraction and Zero-Watermark Construction

Feature extraction is crucial for zero-watermark construction and determines algorithm robustness. The proposed algorithm processes a 256×256 Lena grayscale image through bit-plane decomposition as shown in Figure 3: see original paper-(i). The most significant bit (MSB) plane exhibits the clearest contour, followed by the sixth and seventh planes. As plane significance decreases, pixel distribution becomes increasingly irregular and random. This occurs because visual significance and information content increase with bit-plane significance.

Analysis reveals that the least significant bit (LSB) plane contains minimal information, resembling random noise. To preserve texture information, the algorithm initializes the LSB plane to zero. The processed image achieves a PSNR of 51.12 dB, significantly exceeding the 35 dB threshold, indicating minimal perceptual difference from the original image.

The zero-watermark construction process, illustrated in [Figure 4: see original paper], proceeds as follows:

a) Initialize the LSB of original carrier image I to zero, obtaining I_{LS0}.

b) Partition I_{LS0} into non-overlapping blocks of size $m \times m$, labeling each block as P_k.

c) Calculate the mean value T_k for each block:

$$T_k = \frac{1}{m^2} \sum_{i=1}^{m} \sum_{j=1}^{m} P_k(i,j)$$

d) Construct binary matrix B by comparing each pixel with its block mean:

$$b_k(i,j) = \begin{cases} 1, & \text{if } P_k(i,j) \geq T_k \\ 0, & \text{otherwise} \end{cases}$$

e) Apply Arnold transformation K times to matrix B, obtaining scrambled matrix B_S.

f) Perform XOR operation between B_S and encrypted watermark sequence C to generate the final zero-watermark sequence LSI of length $N \times N$.

2 Simulation Experiments and Security Analysis

All experiments were conducted in Matlab R2010b using a 256×256 standard Lena image as the carrier and a binary watermark containing Chinese characters for copyright protection. The chaotic system parameters were set as $x_0 = 0.123$, $y_0 = 0.321$, $z_0 = 0.231$, $H = 30$, $C = 1.27$, stored as key K_1. The Arnold transformation iteration count was set to 75, stored as key K_2. The original carrier and watermark images are shown in [Figure 5: see original paper].

2.1 Performance Against Various Attacks

2.1.1 Compression and Filtering Attacks Compression and filtering represent the most common attack types. JPEG compression reduces data volume to alleviate transmission channel pressure, while median filtering removes high-frequency noise components. Both processes inevitably cause pixel loss. The experiments tested JPEG compression with quality factors of 60, 70, and 80, and median filtering with 3×3 and 5×5 templates.

Visual results in [Figure 6: see original paper] and [Figure 7: see original paper] demonstrate that while filtering degrades carrier image quality, the extracted watermark remains clearly legible. Similarly, JPEG compression introduces minor artifacts, but watermark readability persists. Quantitative evaluation using Normalized Correlation (NC) values, presented in , shows NC values exceeding 0.85 for all filtering tests and above 0.87 for compression tests, confirming the algorithm' s robustness against these attacks.

2.1.2 Noise Attacks Noise interference frequently occurs during image transmission. Gaussian and salt-and-pepper noise represent two predominant attack types. Experiments evaluated various noise intensities, with results shown in [Figure 8: see original paper] and [Figure 9: see original paper]. While increasing noise levels degrade image quality, the extracted watermark maintains recognizable contours. presents NC values that remain above 0.73 even under severe Gaussian noise (intensity 0.003) and exceed 0.89 under salt-and-pepper noise (intensity 0.03), validating the algorithm' s noise resistance capabilities.

2.1.3 Cropping Attacks Cropping attacks directly remove image regions, causing irreversible information loss. Experiments evaluated three cropping positions (top-left, center, bottom-right) with four area ratios (1/16, 1/8, 1/4, 1/2). Visual results in [Figure 10: see original paper] and [Figure 11: see original paper] show that while larger cropping areas reduce watermark clarity, the text remains distinguishable even when half the image is removed. NC values in consistently exceed 0.86 across all cropping scenarios, demonstrating strong resistance to cropping attacks.

2.1.4 Image Tampering Attacks Tampering attacks including content deletion, text addition, and copy-paste operations were evaluated. [Figure 12: see original paper] through [Figure 14: see original paper] illustrate that extracted watermarks remain clearly visible after such manipulations. reports NC values above 0.98 for all tampering types, indicating exceptional robustness. The algorithm effectively detects unauthorized modifications while preserving watermark integrity.

2.2 Watermark Encryption Security Analysis

The encryption scheme employs both Chen hyperchaotic system and Arnold transformation, generating two independent keys (K_1, K_2). Successful watermark extraction requires both keys. [Figure 15: see original paper] demonstrates that errors in either key produce random noise-like outputs, preventing unauthorized extraction. This dual-key mechanism ensures high security, as compromise of a single key cannot reveal the watermark.

2.3 Algorithm Performance Comparison

Comparative analysis with literature methods [13, 14] across noise, cropping, and filtering attacks is summarized in . The proposed algorithm outperforms existing methods in resisting Gaussian noise and median filtering while maintaining competitive performance against cropping attacks. Unlike methods that modify the LSB plane directly, our zero-watermarking approach preserves the original carrier image completely. The block-mean-based feature extraction ensures stability under attacks, as block averages remain relatively invariant, yielding superior robustness compared to LSB-substitution techniques.

3 Conclusion

This paper presents a hyper-chaos-based image zero-watermarking algorithm that achieves robust copyright protection without modifying the original carrier image. By leveraging the Chen hyperchaotic system and Arnold transformation for encryption, the algorithm provides enhanced security and large key space. Comprehensive experimental validation demonstrates effective resistance against compression, filtering, noise, cropping, and tampering attacks. Comparative analysis confirms superior performance over existing methods, particu-

larly in maintaining watermark integrity under severe attacks. The proposed approach offers a practical solution for robust and secure digital image watermarking applications.

References

[1] Seitz J. Digital watermarking for digital media [M]. London: Information Science Publishing, 2005: 1-30.
[2] Cox I, Miller M, Bloom J, et al. Digital Watermarking and Steganography [M]. San Francisco, California: Morgan Kaufmann Publishers, 2007.
[3] Matthews R A J. On the derivation of a chaotic encryption algorithm [J]. Cryptologia, 1989, 13(1): 29-42.
[4] Chen Guanrong, Dong Xiaoning. From Chaos to order methodologies, perspectives and applications [J]. World Scientific, 1998, 24(16): 760.
[5] Ueta T, Chen Guanrong. Bifurcation analysis of Chen' s equation [J]. International Journal of Bifurcation and Chaos, 2000, 10(8): 1917-1931.
[6] Yassen M T. Chaos control of Chen chaotic dynamical system [J]. Chaos, Solitons & Fractals, 2003, 15(2): 271-283.
[7] Wu Danhui, Zheng Enrang. Research of encryption algorithm of image watermarking based on logistic and Arnold of chaos [J]. Computer Measurement & Control, 2017, 25(04): 193-196.
[8] Ji Nuoran, Lyu Xiaoqi, Gu Yu, et al. Blind watermarking algorithm for color image in contourlet domain based on QR code and chaotic encryption [J]. Packaging Engineering, 2017, 38(15): 173-178.
[9] Qu Changbo, Yu Zhilong, Li Dongdong. A robust zero-watermarking algorithm based on the block FRIT-SVD [J]. Computer Engineering and Science, 2018, 40(06): 1005-1016.
[10] Qu Changbo, Wu Deyang. Strong robust zero-watermarking algorithm based on Curvelet-DSVD and visual cryptography [J/OL]. Application Research of Computers, 2019, 36(3). [2018-09-13]. http://kns.cnki.net/kcms/detail/51.1196.TP.20180209.1115.064.html.
[11] Yang Jinxia, Ju Jie, Shao Feng. Semi-fragile audio watermarking algorithm based on hyper-chaos encryption [J]. Computer Applications and Software, 2014, 31(11): 295-298.
[12] Yao Xue. Research on information hiding algorithm based on bit-plane and HVS [D]. Huludao: Liaoning Technical University, 2014.
[13] Wu Weimin, Ding Ran, Lin Zhiyi, et al. Chaos-based zero-bit watermarking scheme for medical image tamper location [J]. Application Research of Computers, 2014, 31(12): 3685-3688.
[14] Sanjay R, Raman B. A chaotic system based fragile watermarking scheme for image tamper detection [J]. International Journal of Electronics and Communications, 2011, 65(10): 840-847.

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

Source: ChinaXiv —Machine translation. Verify with original.