Optics and Lasers in Engineering 90 (2017) 238–246

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation

Yueping Li, Chunhua Wang, Hua Chen*

School of Information Science and Engineering, Hunan University, Changsha 410082, China

ARTICLE INFO

Keywords:
Image encryption
Multi-wing
Hyper-chaos
Bit-level permutation

ABSTRACT

Recently, a number of chaos-based image encryption algorithms that use low-dimensional chaotic map and permutation-diffusion architecture have been proposed. However, low-dimensional chaotic map is less safe than high-dimensional chaotic system. And permutation process is independent of plaintext and diffusion process. Therefore, they cannot resist efficiently the chosen-plaintext attack and chosen-ciphertext attack. In this paper, we propose a hyper-chaos-based image encryption algorithm. The algorithm adopts a 5-D multi-wing hyper-chaotic system, and the key stream generated by hyper-chaotic system is related to the original image. Then, pixel-level permutation and bit-level permutation are employed to strengthen security of the cryptosystem. Finally, a diffusion operation is employed to change pixels. Theoretical analysis and numerical simulations demonstrate that the proposed algorithm is secure and reliable for image encryption.

1. Introduction

Multimedia communication has become more and more important with the rapid development in internet technology and multimedia technology. Therefore, the security of image information has become an increasingly serious issue. However, due to bulky data capacity, high redundancy and strong correlations among adjacent pixels, traditional encryption algorithms, such as DES and AES, are poorly suited to image encryption [1].

Chaotic system has many excellent intrinsic properties, such as ergodicity, aperiodicity, high sensitivity to initial conditions and control parameters and random-like behaviors. Therefore, researchers have proposed many image encryption algorithms based on chaotic systems [2–21]. The typical ciphers based on chaotic map can be partitioned into two stages: permutation and diffusion. In [2–12], a number of image encryption algorithms using pixel-level permutation have been proposed. The permutation operation of these algorithms just changes the position of the pixel. And the chaotic sequence generated by chaotic system is independent of the plaintext and diffusion process. Therefore, the ciphertext can be easily deciphered by chosen-plaintext attack and chosen-ciphertext attack [13–15]. In [16], an image encryption based on one-time keys is proposed. In [17], a novel chaotic block image encryption algorithm based on dynamic random growth technique is proposed. Although the schemes adopt some measures in the encryption process to improve security, but they cannot resist chosen-plaintext attack and chosen-ciphertext attack totally. To avoid attackers crack cryptosystems by using the order from top to bottom and from left to right, Wang et al. proposed dynamical pixel order for diffusion and sub-images division method [18]. Belazi et al. [19] proposed a new chaos-based partial image encryption scheme which encrypts only the requisite parts of the sensitive information in frequency domain of Lifting-Wavelet Transform (LWT) based on hybrid of chaotic maps and a new S-box. Liu et al. [20] proposed a fast image encryption algorithm. In this algorithm, the confusion and diffusion processes are combined for one stage. Wang et al. [21] proposed a novel hybrid color image encryption algorithm using two complex chaotic systems to enhance the security and enlarge key space of color image encryption. In [22–27], a variety of image encryption algorithms using bit-level permutation have been proposed due to the advantages of bit-level permutations, which can change the position and value of a pixel simultaneously. In [29], Wang et al. introduced the perceptron conception of a neural network to a chaotic encryption system, and proposed a new bit-level encryption algorithm based on mathematical model to improve security. In [30], a new bit-level encryption algorithm based on the spatiotemporal non-adjacent coupled map lattices which makes it possible for any bit in pixels to break the limit of its bitplane without extra space in permutation process. In [31], a novel bit-level image encryption algorithm based on chaotic maps is proposed to modify the statistical information that is in each bitplane. Recently, the characteristics of DNA computing, massive parallelism, huge storage and ultra-low power consumption have been found. A number of image encryption algorithms use DNA rule are proposed [28,32,33,37]. However, they have the same weakness as pixel-level image encryption algorithms.

* Corresponding author.

http://dx.doi.org/10.1016/j.optlaseng.2016.10.020
Received 8 August 2016; Received in revised form 22 October 2016; Accepted 24 October 2016

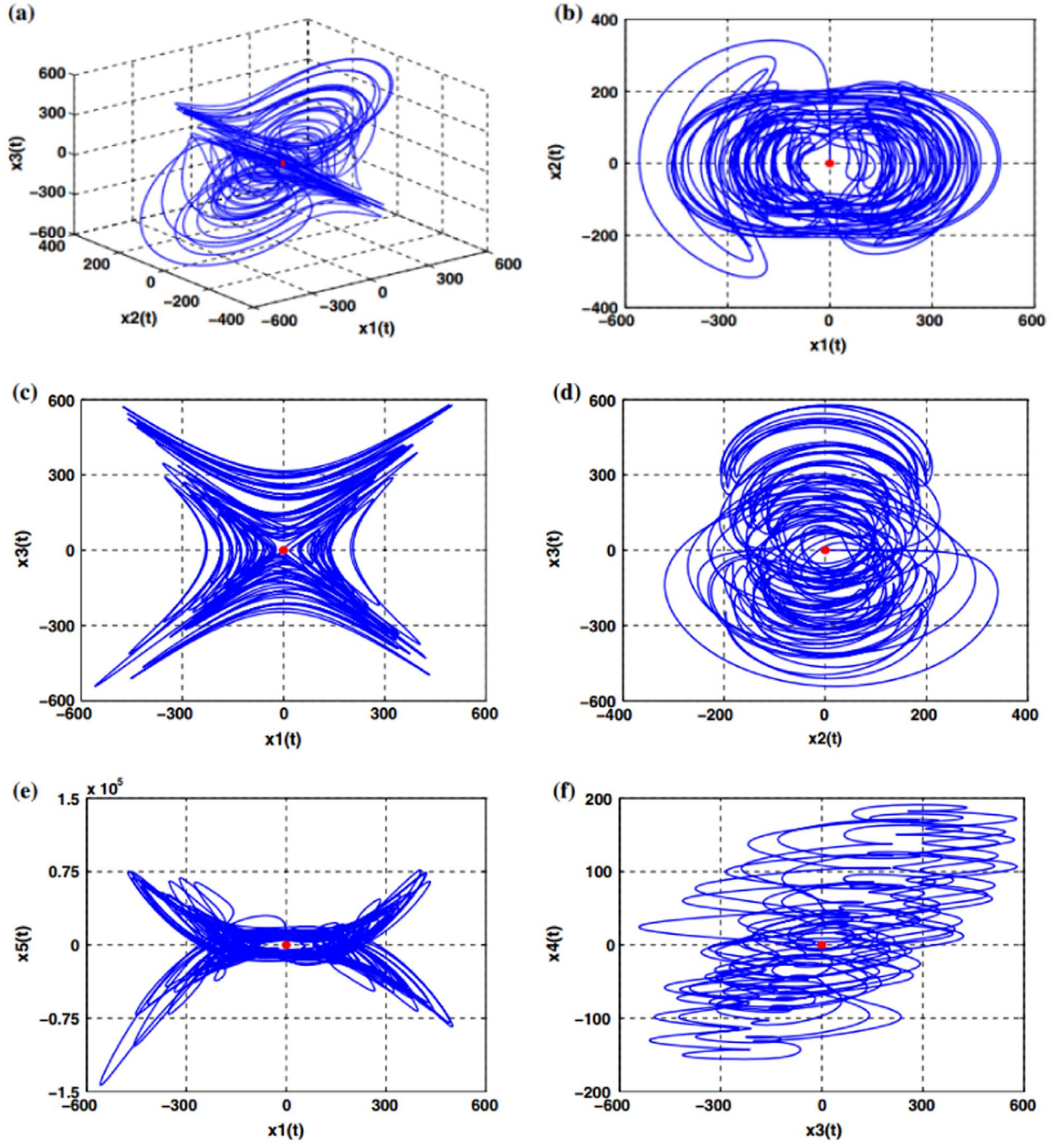

Fig. 1. Phase portraits of system (1) with parameters a=10, b=60, c=20, d=15, e=40, f=1, g =50, h =10, (a) 3D view in the x_1–x_2–x_3 space; (b) projection on x_1–x_2 plane; (c) projection on x_1–x_3 plane; (d) projection on x_2–x_3 plane; (e) projection on x_1–x_5 plane; (f) projection on x_3–x_4 plane.

In addition, compared with high-dimensional chaotic systems, image encryption algorithms employing the low-dimensional chaotic maps are not safe. Because high-dimensional chaotic systems, especially hyper-chaotic systems, have a larger key space, better sensitivity, more complex dynamic characteristics and randomness. The general methods that can decipher low-dimensional chaotic maps, such as phase space reconstruction and nonlinear prediction, are difficult to decipher high-dimensional chaotic systems. Therefore, a number of image encryption algorithms based on hyper-chaotic systems have been proposed [28,34–38]. In [34], Gao and Chen proposed a hyper-chaos-based image encryption algorithm using pixel-level permutation. Although this algorithm has the advantage of large key space, Ruouma and Belghith [35] proved that it could not resist the chosen-plaintext attack and the chosen-ciphertext attack; moreover, Jeng et al. [36] found that there is a weakness for Gao and Chen's algorithm and Ruouma and Belghith's improved algorithm, i.e., low sensitivity to change of plain-images. Meanwhile, hyper-chaos-based image encryption algorithms with DNA encoding were presented [28,37]. However, to date, there are not image encryption algorithms using pixel-level permutation and bit-level permutation.

To overcome the weaknesses above, this paper proposes a hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. First, the algorithm employs a hyper-chaotic system to resist the general methods which can decipher low-dimen-