Improved Encryption Algorithm of Images Based on Three-Dimensional Chaos

Kefeng Wang, School of Computer Engineering, Jiangsu University of Technology, Changzhou, China
FeiYue Ye, School of Computer Engineering, Jiangsu University of Technology, Changzhou, China

ABSTRACT

It describes an improved encryption algorithm of a three-dimensional image based on multiple chaotic systems. The algorithm uses a variety of chaotic encryption system to cut the image into three-dimensional matrix systems, in three-dimensional space do the image scrambling transformation, three-dimensional chaotic sequence output by multiple chaotic systems achieved three color pixel substitution transformation of the spatial color image. Finally, according to the theoretical analysis and simulation results it shows that the encryption algorithm with large key space, good confidentiality, and the pixel values of the encryption image has a random uniform distribution features and zero correlation of the neighboring pixel values, verifies the proposed scheme has high security.

Keywords: Image Encryption Algorithm, Multi-Chaos, Multiple Chaotic Systems, Three-Dimension

1. INTRODUCTION

With the rapid development of network technology and wide use of multi-media, there is an increasing growth in the use and transmission of multi-media images through computer network. The security and privacy of the image information have become a major concern due to the openness and multi-access of the net. Since digital images have vast data of high correlation, it shows low efficiency to encrypt images in a traditional way. Recently, a variety of newly-developed chaos-based encryption approaches have been proposed as an effective way, which becomes a heated research issue.

In general, chaotic systems possess a number of important properties. For instance, it shows extreme sensitivity to any tiny difference of the initial circumstances and system parameters.

DOI: 10.4018/IJCINI.2015040105
Topological transitivity means that a chaotic state variable goes through all states in its phase space, and usually the system presents certainty and regularity, not a scene of chaos. Besides, chaotic systems generate random-like chaotic sequence in a deterministic way. These properties are consistent with diffusivity, miscibility and randomness required in cryptology. However, since there lacks studies on the color image encryption, the paper proposes a new color image encryption algorithm based on a kind of nonlinear chaotic system with higher dimension, combining with the generalized cat map and the unified chaotic models [Zhao, 2013].

It is a newly-developed image encryption technology to generate the key sequence with the randomness of the chaotic system. As chaotic signals are quite sensitive to the initial conditions, a tiny difference of initial conditions will separate exponentially with the increasing number of iterations and become irrelevant. Apart from that, chaotic signals possess other properties, like periodicity, aperiodicity, wide frequency spectrum and white noise, so as to suitable to implement the code system design. However, recently, one dimensional chaotic system is applied in many image encryption schemes, which lacks great security. One of the reasons is that it doesn’t have enough space of the key sequence and is vulnerable to attack, especially plaintext attack if intercepting plaintext / cipher text pairs long enough and decoding seed key by the means of phase space reconstruction. The first reference introduces parametric two-dimensional chaos mapping algorithm and the second one describes digital image encryption algorithm by means of Arnold and Fibonacci-Q tans transformation. Arnold transformation, however, is only two-dimensional. Although there exist some methods to extend the chaotic mapping to the three dimensional, it only limits to gray level scrambling. In the actual process of communication, we need to a large number of color image transmissions, which demands a technical encryption method for color images. Based on the theory of chaotic encryption, by means of multi-chaotic system, the paper tries to encrypt the three vectors x, y, z corresponding to R, G, B, these three primary color images. Moreover, in order to further increase the security strength, image coefficient are transformed at some ratio with the one-dimensional finite folding map so that it will resist the attack of plaintext and selective plaintext due to the enlarged key space and stronger anti-attack ability, greatly improving the encryption efficiency.

RGB color images will be split up into three primary color ones and each component image can be regarded as luminance one. In the scrambling algorithm of this paper, each primary color image will be scrambled by the generalized cat map, during which different key parameters (Ri,Gi,Bi), i=1, 2 or 3 are used to correspond to R, G, B, these three primary color images. Assume the original color image is stranded by matrix A, which is split up into three primary color images represented by the matrices RA, GA and BA. And these three matrices scrambled and transformed by cat maps with different parameters are synthesized into another color image matrix A1, which is the color image after scrambling [Huang, 2010].

This algorithm respectfully scrambling each primary color image brings great change to color components of the final synthetic color image, and confuses R, G, B, the three elements of each pixel, which makes color changes to the encrypted image visually. Therefore, it has higher security than scrambling three color values of the same point and unifying into the same new position.

2. THREE-DIMENSIONAL MULTI-CHAOTIC SYSTEM

First of all, the target JPEG color image is split into R, G, B, three primary color components and after scrambling the three components, XOR processing is implemented with multiple
Related Content

A Cognitive Framework for Core Language Understanding and its Computational Implementation
[www.igi-global.com/article/cognitive-framework-core-language-understanding/67792?camid=4v1a](www.igi-global.com/article/cognitive-framework-core-language-understanding/67792?camid=4v1a)

Constructivist Learning During Software Development
[www.igi-global.com/article/constructivist-learning-during-software-development/1542?camid=4v1a](www.igi-global.com/article/constructivist-learning-during-software-development/1542?camid=4v1a)

Affective Games: How iOpiates Elicit an Emotional Fix
[www.igi-global.com/chapter/affective-games-iopiates-elicit-emotional/49542?camid=4v1a](www.igi-global.com/chapter/affective-games-iopiates-elicit-emotional/49542?camid=4v1a)
Cognitive Informatics and Cognitive Computing in Year 10 and Beyond

www.igi-global.com/article/cognitive-informatics-cognitive-computing-year/63618?camid=4v1a