Chapter 22
A Novel Algorithm for Block Encryption of Digital Image Based on Chaos

Jun Peng
Chongqing University of Science and Technology, China

Du Zhang
California State University, USA

Xiaofeng Liao
Chongqing University, China

ABSTRACT

This paper proposes a novel image block encryption algorithm based on three-dimensional Chen chaotic dynamical system. The algorithm works on 32-bit image blocks with a 192-bit secret key. The idea is that the key is employed to drive the Chen's system to generate a chaotic sequence that is inputted to a specially designed function G, in which we use new 8x8 S-boxes generated by chaotic maps (Tang, 2005). In order to improve the robustness against differental cryptanalysis and produce desirable avalanche effect, the function G is iteratively performed several times and its last outputs serve as the keystreams to encrypt the original image block. The design of the encryption algorithm is described along with security analyses. The results from key space analysis, differential attack analysis, and information entropy analysis, correlation analysis of two adjacent pixels prove that the proposed algorithm can resist cryptanalytic, statistical and brute force attacks, and achieve a higher level of security. The algorithm can be employed to realize the security cryptosystems over the Internet.

DOI: 10.4018/978-1-4666-2476-4.ch022

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

In the last decades, extensive studies have been done in the theory of chaos in different fields such as physics, engineering, biology, and economics (Hao, 1993). Chaos theory consistently plays an active role in modern cryptography. As the basis for developing cryptosystems, the main advantage of the chaos-based approaches lies in the random behavior and sensitivity to the initial conditions and control parameters, hence the study on using chaos theory in information security has attracted great attentions (Chen, 2004; Li, 2005; Peng, 2008; Yang, 2004). The close relationship has been observed in (Álvarez, 2006; Fridrich, 1998; Kocarev, 2001) between chaotic maps and cryptosystems. In particular, the following connections between them can be established: (1) Ergodicity in chaos vs. confusion in cryptography; (2) Sensitive dependence on initial conditions and control parameters of chaotic maps vs. diffusion property of a good cryptosystem for a slight change in the plaintext and in the secret key; (3) Random-like behavior of deterministic chaotic-dynamics which can be used for generating pseudorandom sequences as key sequences in cryptography.

In recent years, the transmission of digital images over the Internet or personal digital mobile phones has been highly developed. Secure storage and transmission of digital images are becoming critically important. Most traditional ciphers, such as DES, IDEA, and AES are not suitable to conduct the digital image encryption in real time due to large data volume involved. Hence, the main purpose of this paper is to design a new image block encryption algorithm by using non-traditional methods such as chaos theory.

A brief review is in order on existing results of chaos-based encryption scheme. Yen et al. (2000) proposed a chaotic key-based algorithm (CKBA) in which a binary sequence as a key is generated based on a chaotic map. According to the binary sequence, image pixels are rearranged and then XORed with the key. However, as pointed out later in (Li, 2002), this algorithm has some drawbacks: it is vulnerable to the chosen or known-plain-text attack using only one plain image, and its security to brute-force attack is also questionable. Chen et al. (2004) used a 3D Arnolad's cat map for the purpose of substitution and employed Chen's chaotic system for generating key streaming and diffusion. A more complex system which combines discrete- and continuous-time chaotic systems has been proposed by Guan et al. (2005). Recently, Tong et al. (2009) presented a new compound two-dimensional chaotic functions design which acted as a chaotic sequence generator, and suggested a feedback image encryption scheme by using the new compound chaos and perturbation technology based on 3D Baker map. At the same time, in (Lian, 2009) the author employed a chaotic neural network (CNN) composed of a chaotic neuron layer and a linear neuron layer to construct a block cipher, in which the chaotic neuron layer realizes data diffusion and the linear neuron layer realizes data confusion, and the two layers are repeated for several times to strengthen the cipher. Obviously, these research results laid a good foundation to the subsequent studies on the chaos-based image encryption algorithm.

Motivated by the aforementioned results, a new image block encryption algorithm based on three-dimensional Chen dynamical system is proposed in this paper. Since cryptosystems play a pivotal role in a very important engineering application of cognitive informatics, i.e., information assurance and security, the subject topic of this paper is within the broad scope of cognitive informatics. The main novelty of the algorithm can be summarized as follows: (1) the 3D Chen system with complex dynamical behaviors is adapted; (2) within the algorithm, a 192-bit secret key is used to drive the Chen system and the keystreams are generated through iteratively performing a specially designed function G; (3) when designing the function G, we use new 8×8 S-boxes produced by chaotic maps in (Tang, 2005) in order to obtain desirable confusion and diffu-

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/novel-algorithm-block-encryption-digital/72300

Related Content

Efficacy of Deep Neural Embeddings-Based Semantic Similarity in Automatic Essay Evaluation
Manik Hendre, Prasenjit Mukherjee, Raman Preetand Manish Godse (2023). *International Journal of Cognitive Informatics and Natural Intelligence (pp. 1-14).*
www.irma-international.org/article/efficacy-of-deep-neural-embeddings-based-semantic-similarity-in-automatic-essay-evaluation/323190

Towards Psychologically based Personalised Modelling of Emotions Using Associative Classifiers
Aladdin Ayesh, Miguel Arevalillo-Herráezand Francesc J. Ferri (2016). *International Journal of Cognitive Informatics and Natural Intelligence (pp. 52-64).*
www.irma-international.org/article/towards-psychologically-based-personalised-modelling-of-emotions-using-associative-classifiers/160830

Listening, Corporeality, Place and Presence
Susan Turner (2009). *Exploration of Space, Technology, and Spatiality: Interdisciplinary Perspectives (pp. 113-127).*
www.irma-international.org/chapter/listening-corporeality-place-presence/18680

MobiGaze: Gaze Interface for Mobile Devices
Takashi Nagamatsu, Michiya Yamamotoand Hiroshi Sato (2012). *Cognitively Informed Intelligent Interfaces: Systems Design and Development (pp. 56-66).*
www.irma-international.org/chapter/mobigaze-gaze-interface-mobile-devices/66267

Modeling a Secure Sensor Network Using an Extended Elementary Object System
Vineela Devarashetty, Jeffrey J.P. Tsai, Lu Maand Du Zhang (2012). *Developments in Natural Intelligence Research and Knowledge Engineering: Advancing Applications (pp. 247-262).*
www.irma-international.org/chapter/modeling-secure-sensor-network-using/66452