A Novel Approach for Designing Dynamical S-Boxes Using Hyperchaotic System

Jun Peng, Chongqing University of Science and Technology, China
Du Zhang, California State University, Sacramento, USA
Xiaofeng Liao, Chongqing University, China

ABSTRACT

In the information security field, the substitution boxes (S-boxes) have been extensively used in many cryptographic systems. This paper presents a novel approach for generating dynamically cryptographically S-boxes using a four-dimensional hyperchaotic Lorenz system. Within the algorithm, the initial condition is employed to drive the hyper-chaotic system to generate a chaotic sequence which is used to construct a chaotic key-dependent S-box. With different system initial conditions, many of distinct S-boxes can be obtained dynamically. Some cryptographic properties for a good S-box such as bijection, nonlinearity, SAC (Strict Avalanche Criterion), BIC (Bit Independence Criterion), and differential approximation probability are found to hold in the obtained S-boxes. The analytic results indicated that all the criteria for designing strong S-boxes can be achieved. The comparison of the proposed method for generating S-boxes with other chaos-based schemes indicates that our S-boxes have a better performance with respect to some properties. Finally, the authors give an example of a digital image encryption algorithm using their S-box and the results of image statistical analysis show that the algorithm has the desirable cryptographic properties.

Keywords: Bit Independence Criterion, Chaos, Cryptography, Hyperchaotic Lorenz System, Information Security, Strict Avalanche Criterion, Substitution Box

INTRODUCTION

In the information security field, the substitution boxes (S-boxes) have been extensively used in most of cryptographic systems, such as DES, IDEA and AES. S-boxes are core component of the DES-like cryptosystems and the only nonlinear component of these ciphers. The security of a cryptographic system primarily depends on the cryptographic strength of the S-box (Feng, 2000). In block ciphers, they are typically used to obscure the relationship between the secret key and the ciphertext’s Shannon property of confusion. In many cases, the S-boxes are care-
fully chosen to provide the cryptosystem with abilities of resisting cryptanalysis. Therefore, the construction of cryptographically strong S-boxes is an important task. Mathematically, an $n \times m$ S-box is a nonlinear mapping (or substitution) from $V_n$ to $V_m$, where $V_n$ and $V_m$ represent the vector spaces of $n$ and $m$ tuples of elements from $GF(2)$, respectively.

As chaotic sequences have many significant properties favorable to the information security, such as random-like and extreme sensitivity to the initial condition and control parameters, the study on using chaos theory in information security has attracted great attentions, such as cryptographic ciphers (Yang, 1997; Fridrich, 1998; Kocarev, 2001), image encryption systems (Chen, 2004; Rhouma, 2009), and chaos-based hash functions (Xiao, 2008; Peng, 2008; Li, 2012). Recent research shows that it is a promising direction to use the distinct properties of chaos to design S-boxes, and there are many methodologies and design criteria for constructing chaos-based S-boxes in the literature. Jakimoski and Kocarev presented a map $f : \{1, 2, \ldots, m - 1\} \rightarrow \{1, 2, \ldots, m - 1\} (m = 256)$ from chaotic Logistic map, in which map $f$ actually can be viewed as an S-box (Jakimoski, 2001). Tang and Liao (2005) and Tang, Liao, and Chen (2005) proposed a new method for obtaining cryptographically strong dynamic S-boxes based on the iterating discretized chaotic map. Later, Chen et al. presented a scheme to construct S-box by employing a three-dimensional chaotic Baker map, which has more intensive chaotic characters than the two-dimensional one (Chen, 2007). Recently, Wang et al. proposed a method for designing S-box based on chaotic neural network (Wang, 2010). After that, Wang et al. studied a novel method to design S-box using chaotic map and genetic algorithm (Wang, 2012), where the problem of constructing S-box was transformed to a Traveling Salesman Problem. Obviously, these research achievements are very useful to the later studies on the construction algorithms of S-boxes using chaotic map.

As we know, a hyperchaotic system has a strong spatiotemporal complexity and mixture due to owning more than one positive Lyapunov exponent. In this paper, a novel approach for generating dynamically cryptographically strong S-boxes based on iterating a four-dimensional hyperchaotic system is presented. One of the main motivations for using hyperchaos is that we want to achieve a more sophisticated chaotic sequence to generate an S-box. Since S-box plays a pivotal role in 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 (Wang, 2003, 2007, 2009, 2010; Wang et al., 2009; Wang & Kinsner, 2006; Wang, Kinsner, & Zhang, 2009).

The remaining part of the paper is organized as follows. Several cryptographic properties that are required to design a “good” $n \times n$ bits S-box are firstly described. Then, an approach for generating dynamical S-boxes is presented in detail. Following that, the performance analysis and comparison are provided respectively. Finally, conclusions are drawn.

**CRYPTOGRAPHIC PROPERTIES OF S-BOXES**

Adams and Tavares (1990) proposed a design procedure for the s-boxes of private key cryptosystems constructed as substitution-permutation networks (DES-like cryptosystems). Furthermore, Jakimoski and Kocarev described how to select the important properties required for the design of a cryptographically strong S-Box (Jakimoski, 1991). In general, the following cryptographic properties are required for “good” S-boxes. These properties can be used as our evaluation criteria and to guide the construction of S-box.
Metaphore, Self-Reflection, and the Nature of Mind
[www.igi-global.com/chapter/metaphore-self-reflection-nature-mind/31018?camid=4v1a](www.igi-global.com/chapter/metaphore-self-reflection-nature-mind/31018?camid=4v1a)

The Motivation/Attitude-Driven Behavior (MADB) Model in E-Learning and the Effects on Mouse Dynamics