http://tarjomebazar.com
09372121085 Telegram
026-33219077
درخواست
ترجمه کردن
این مقاله
ترجمه بازار

2015 IEEE International Conference on Computational Intelligence & Communication Technology

# Design of a chaos-based digitlal image encryption algorithm in time domain

JiaYan Wang
GuangZhou Power Supply CO.,LTD, Guangzhou, China
wangjy_power@163.com

Geng Chen
Faculty of Automation, GuangDong University of technology
alex.chen@techyc.com

***Abstract*—In this paper a chaos-based digital image encryption scheme by a permutation-substitution structure is proposed. Its design and implement have been detailed discussed and tested. The results of simulation and analysis show that the proposed image encryption scheme provides a secure way for image encryption.**

***Keywords-encryption; decryption;permutation; substitution;***

## I. INTRODUCTION

With the rapid development of the network communication, digital image encryption has becoming a field that has drawn much attention in the latest years. Digital image data have some particular characteristics such as bulk capacity, high redundancy and high correlation among image pixels. Traditional encryption technologies, such as DES, AES, IDEA, regard digital image data as common data without considering their special characteristics, thus they are unsuitable in protecting digital image data any more.

One of the most effective approaches for image encryption recently is to use chaos maps owning to their non-periodic, non-convergent, sensitivity to initial conditions and ergodicity properties. Chaotic system has interesting and close relationship with cryptography. They are considered the favorable tradeoff of the digital image encryption between the security and the speed. We can find a brief description of relationship between chaos and cryptography in [1, 2]. Fridrich [1] proposes an image encryption scheme based on two-dimensional discrete chaotic baker maps. To fulfill the request of Shannon’s theory, the architecture of the scheme is composed of the confusion and diffusion criteria, which is regarded as the basic structure for chaos-based image encryption algorithms. Afterwards, various algorithms based on chaotic maps [3-15] have been proposed for securing image applications.

In this paper a chaotic cipher for gray images by a permutation-substitution structure is proposed. Chaotic maps with random initial conditions and parameters are used to generate random sequences with high sensitivity. Two of the sequences are produced from 2D chaotic map then used to design a two dimensional permutation. The initial values are derived from 1D Logistic map. Then elements of other two sequences are used to confuse pixel values by combined bit exclusive-OR and cyclic bit-shift operations.

Other sections of this paper are organized as follows. In the next section, a brief discussion of chaotic map is introduced. The proposed algorithm is put forward and discussed in section III. Simulation results and security analysis are described in section IV. Section V is a conclusion.

## II. CHAOTIC SYSTEM

1D Logistic map is a simple chaotic map and has been widely used in many image encryption algorithms. It is defined by:

$$f(x)=\mu x(1-x), \qquad x\in(0,1). \tag{1}$$

Research shows that the system is in chaotic state under the condition that $3.99465<\mu\le 4$. However, it may lead to insecure encryption algorithm due to its small key space and simple structure. Therefore high-dimensional chaotic systems which possess large key space will provide better security. For example, 2D discrete Super-chaotic map[3] is given by following equation.

$$\begin{cases} x_{n+1}=ay_n+by_n^2 \\ y_{n+1}=cy_n+dx_n \end{cases} \tag{2}$$

If we let $a=1.55, b=-1.3, c=0.1, d=-1.1$, the map will exhibit a chaotic state.

The Lyapunov exponents are usually be employed to measure the exponential rates of divergence and convergence of nearby trajectories in state space. For the above Super-chaotic map, it has two positive Lyapunov exponents, 0.238 and 0.166.

## III. THE DESIGN OF IMAGE ENCRYPTION ALGORITHM

Let $I$ denotes a gray scale image with size $M\times N$. Denotes $I(i,j)$ the gray scale value of the pixel at position $0\le i\le M-1$ and $0\le j\le N-1$. The proposed algorithm is a symmetrical image encryption method based on chaotic maps. The algorithm is composed of two processes, permutation and substitution, to fulfill the Shannon’s criteria, confusion and diffusion.

978-1-4799-6023-1/15 $31.00 © 2015 IEEE
DOI 10.1109/CICT.2015.23