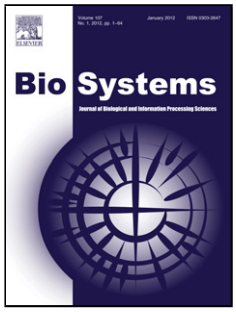

Title: Color image encryption scheme using CML and DNA sequence operations

Author: Xing-yuan Wang Hui-li Zhang Xue-mei Bao

PII: S0303-2647(16)30031-4
DOI: http://dx.doi.org/doi:10.1016/j.biosystems.2016.03.011
Reference: BIO 3647

To appear in: *BioSystems*

Received date: 20-4-2015
Revised date: 29-2-2016
Accepted date: 25-3-2016

Please cite this article as: Wang, Xing-yuan, Zhang, Hui-li, Bao, Xue-mei, Color image encryption scheme using CML and DNA sequence operations.BioSystems http://dx.doi.org/10.1016/j.biosystems.2016.03.011

Color image encryption scheme using CML and DNA sequence operations

Xing-yuan Wang*, Hui-li Zhang, Xue-mei Bao

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian, 116024, China

Abstract: In this paper, an encryption algorithm for color images using chaotic system and DNA (Deoxyribonucleic acid) sequence operations is proposed. Three components for the color plain image is employed to construct a matrix, then perform confusion operation on the pixels matrix generated by the spatiotemporal chaos system, i.e., CML (coupled map lattice). DNA encoding rules, and decoding rules are introduced in the permutation phase. The extended Hamming distance is proposed to generate new initial values for CML iteration combining color plain image. Permute the rows and columns of the DNA matrix and then get the color cipher image from this matrix. Theoretical analysis and experimental results prove the cryptosystem secure and practical, and it is suitable for encrypting color images of any size.

Key words: Chaotic image encryption; DNA coding; color image; Coupled map lattice

1. Introduction

The development of computers and the Internet has arisen the significance of information security. Image information transmission has increased rapidly and image encryption technology has drawn more attentions [1]. Image encryption is different from text encryption due to some inherent features such as bulk data capacity and high correlation among pixels. Therefore, traditional cryptographic techniques such as DES(Data encryption Standard), IDES (International Data encryption Standard) and RSA public key encryption are no longer suitable for image encryption. While a chaotic system has several significant features, such as sensitive dependence on initial conditions, pseudo-randomness, and ergodicity [2]. These properties have been used in different applications such as image fraction [3], complex network [4] and financial market forecast. Moreover, these features characterize good properties of diffusion and confusion, which are of great importance to design image encryption algorithms.

Up to now, many chaos-based image encryption algorithms have been proposed [5-10]. Wang and Teng proposed the image encryption based on the spatiotemporal chaos [5], which took advantages of pseudo-randomness of the chaos. And Ye designed the image encryption with wave transmission [6]. Besides, the self-adaptive model was proposed to encrypt images [7]. Zhou et. al designed the parametric switching chaotic system for better encryption performance [8], while Zhang and Xiao considered the bit-level operation in image encryption [9], Benyamin used only two-round diffusion in his algorithm [10], which abandoned the confusion

*Corresponding author. E-mail addresses: wangxy@dlut.edu.cn (X. Wang), zhanghui7873@foxmail.com(H. Zhang), baoxuemei1989@163.com (X. Bao).