*International Journal of Innovative Computing, Information and Control*
Volume **3**, Number **6(B)**, December **2007**

ICIC International ©2007 ISSN 1349-4198
pp. **1593–1602**

# A SYMMETRIC IMAGE ENCRYPTION SCHEME BASED ON A SIMPLE NOVEL TWO-DIMENSIONAL MAP

Feng Huang[1], Yong Feng[2] and Xinghuo Yu[3]

[1]Department of Electrical and Information Engineering
Hunan Institute of Engineering
Xiangtan, Hunan 411104, P. R. China
hf7825@gmail.com

[2]School of Electrical Engineering and Automation
Harbin Institute of Technology
Harbin 150001, P. R. China
yfeng@hit.edu.cn

[3]School of Electrical and Computer Engineering
Royal Melbourne Institute of Technology University
Melbourne, VIC 3001, Australia
x.yu@rmit.edu.au

Received October 2006; revised June 2007

Abstract. *This paper proposes a new two-dimensional map. It can encrypt images by processing image stretch-and-fold. Firstly each pixel of the first column of a square image is inserted into adjacent two pixels of the first row one by one. Then each pixel of the last column is inserted into adjacent two pixels of the last row. Repeating the process for the rest of the image, it is stretched and joins a line of pixels. Secondly the line is fold over to a new square image with the same size to the plain-image. The map is divided into the left-map permutations and the right-map permutations. The numbers of the left-map permutations and the right-map permutations can be used as the secret key in encryption. The process shuffles the positions of image pixels. Compared with the prevalent two-dimensional map, Baker map, the new map has a simpler formulation, larger key space which is more adequate for image encryption. A new image encryption scheme based on the map is developed which is composed with a simple diffusion mechanism. The deciphering process is an invertible process using the same keys. The simulation results validate the proposed image encryption scheme.*
**Keywords:** Two-dimensional map, Image encryption, Chaos

1. **Introduction.** Nowadays, how to protect the security of images is a serious problem. The encryption is an important tool to protect images from attackers. Some traditional encryption algorithms such as DES, RSA, etc were used for image encryption [1]. In order to suit the intrinsic features of images, other image encryption methods such as chaos have been explored in the recent years.

Chaos can be well applied in cryptography [5,10,11]. Chaos has many characteristics which can be connected with the "confusion" and "diffusion" property in cryptography, such as sensitive dependence on initial conditions and parameters, broadband power spectrum, randomness in the time domain, ergodicity, low-dimensional etc [6]. In fact the idea