Available online at www.sciencedirect.com

ScienceDirect

Chaos, Solitons and Fractals 38 (2008) 213–220

CHAOS
SOLITONS & FRACTALS

www.elsevier.com/locate/chaos

Image encryption based on a new total shuffling algorithm

Tiegang Gao [a,*], Zengqiang Chen [b]

[a] *College of Software, Nankai University, Tianjin 300070, PR China*
[b] *Department of Automation, Nankai University, Tianjin 300070, PR China*

Accepted 10 November 2006

Communicated by Prof. M.S. El Naschie

Abstract

This paper presents image encryption scheme, which employs a new image total shuffling matrix to shuffle the positions of image pixels and then uses the states combination of two chaotic systems to confuse the relationship between the plain-image and the cipher-image. The experimental results demonstrate that the new image total shuffling algorithm has a low time complexity and the suggested encryption algorithm of image has the advantages of large key space and high security, and moreover, the distribution of grey values of the encrypted image has a random-like behavior.
© 2006 Elsevier Ltd. All rights reserved.

1. Introduction

With the rapid developments in digital image processing and network communication, electronic publishing and widespread dissemination of digital multimedia data over the Internet, protection of digital information against illegal copying and distribution has become extremely important. To meet this challenge, many new encryption schemes have been proposed [1–4]. Among them, chaos-based algorithms has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption, and it has been proved that in many aspects chaotic maps have analogous but different characteristics as compared with conventional encryption algorithms [5–9].

The chaos-based encryption was first proposed in 1989 [10], since then, many researchers have proposed and analyzed a lot of chaos-based encryption algorithms, these work all have been motivated by the chaotic properties such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity. While classical encryption algorithms are sensitive to keys, so some elaborated constructions are need to achieve satisfying and safer chaos-based encryption.

It is well known a good encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible [11]. Recently, in [12], a fast chaotic cryptographic scheme based on iterating a logistic map was proposed, and no random numbers need to be generated and the look-up table used in the cryptographic process is updated dynamically. In [13], a two-dimensional chaotic cat map is generalized to 3D

[*] Corresponding author.
E-mail address: gaotiegang@nankai.edu.cn (T. Gao).

0960-0779/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chaos.2006.11.009

for designing a real-time secure symmetric encryption scheme, which employs the 3D cat map to confuse the relationship between the cipher-image and the plain-image. Also recently, the authors in [14] thought that the algorithm for encoding binary images using one-dimensional chaotic map [15] is not secure enough, and there is the same problem with the algorithm proposed in [16], to overcome the drawbacks such as small key space and weak security of one-dimensional chaotic map, a nonlinear chaos algorithm is proposed in [17], which shows high-level security and acceptable efficiency.

A new image encryption scheme is suggested in this paper, different from the 2D or 3D chaotic map that is used to shuffle the pixel positions of the plain-image, a new image total shuffling matrix is used to shuffle the position of the pixels and the states combination of two chaos are used to change the grey values of the plain-image in our method. The rest of this paper is organized as follows. Section 2 presents the proposed image total shuffling algorithm and image encryption algorithm through combination of states of chaotic systems. Section 3 describes some simulation outcomes, some security analysis are given in Section 4. Finally, Section 5 concludes the paper.

2. The proposed encryption algorithm

2.1. Generation of image total shuffling matrix

Image data have strong correlations among adjacent pixels, in order to disturb the high correlation among pixels; an image total shuffling matrix is used to shuffle the position of the plain-image. Without loss of generality, we assume that the dimension of the plain-image $N \times M$, the position matrix of pixels is $P_{i,j}$, $i = 0, 1, \ldots, M-1$; $j = 0, 1, \ldots, N-1$ the procedure of generation for shuffling matrix is described as follows:

(1) For Logistic map $x_{n+1} = 4x_n(1 - x_n)$ and a given x_0, after do some iterations, a new x_0 is derived, then let

$$l = \mathrm{mod}(x_0 \times 10^{13}, M) \tag{1}$$

Obviously, $l \in [0, M-1]$.

(2) Continue to do the iteration of Logistic map and do (1) until we get M different data which are all between 0 and $M-1$, these data can be recorder in the form of $\{h_i, i = 1, 2, \ldots, M\}$, where $h_i \neq h_j$ if $i \neq j$. Then rearrange the row of matrix $P_{i,j}$ according to $\{h_i, i = 1, 2, \ldots, M\}$, that is, move the h_1 row to the first row, h_2 row to the second row, thus a new position matrix $P^h_{i,j}$ is generated based on the transformation.

For the new matrix $P^h_{i,j}$, we will produce column shuffling matrix column by column. The process is presented next.

(1) Use the present x_0 to do the iteration of Logistic map and then let

$$l = \mathrm{mod}(x_0 \times 10^{13}, N) \tag{2}$$

It is easily can be seen, $l \in [0, N-1]$.

(2) Continue to do the iteration of Logistic map and do (2) until we get N different data which are all between 0 and $N-1$, these data can be expressed $\{l_i, i = 1, 2, \ldots, N\}$, where $l_i \neq l_j$ if $i \neq j$. Then rearrange the data of every column for the first row of matrix $P_{i,j}$ according to $\{l_i\}$, that is, move the l_1 column to the first column, l_2 column to the second column, thus a new column transformation of the first row of matrix $P^h_{i,j}$ is generated.

(3) From the second row till the last row of matrix $P^h_{i,j}$, do the same column transformation in the same way as the second step, thus a new image total shuffling matrix $P^{hl}_{i,j}$ is given, and if N and M are not very big, the algorithm have lower time complexity, which can be summarized in Table 1.

Table 1
Time complexity of *image total shuffling algorithm*

Size of the image	The average number of iteration needed to accomplish a row transformation
32×32	80
64×64	300
128×128	520
256×256	1600