Signal Processing: *Image Communication* 28 (2013) 1548–1559

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

journal homepage: www.elsevier.com/locate/image

A family of new complex number chaotic maps based image encryption algorithm

Yang Liu [a], Xiaojun Tong [a,*], Shicheng Hu [b]

[a] School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China
[b] School of Economics and Management, Harbin Institute of Technology, Weihai 264209, China

ARTICLE INFO

Article history:
Received 11 March 2013
Received in revised form
13 June 2013
Accepted 28 July 2013
Available online 8 August 2013

Keywords:
Image encryption
Chaotic map
Complex number

ABSTRACT

A family of new complex number chaotic maps based image encryption algorithm is proposed in the paper. A family of maps is constructed and proved to be chaotic in the complex number field, and its characteristics are analyzed. Two maps are selected from the chaotic maps family and are utilized to construct pseudorandom keystream sequence. In the proposed encryption algorithm, the pseudorandom keystream sequences are used to scramble and diffuse the plain image data and two entropy coding methods are used to reduce the correlation among the signals. Both theoretical analysis and experimental tests show that the proposed algorithm is secure and efficient.

© 2013 Elsevier B.V. All rights reserved.

1. Introduction

With the rapid development of network technology, a lot of image data are transmitted over the network. In the transmission, one of the major issues is the security of digital images. So image encryption technology has drawn more attention.

Due to the random-like behaviors of chaos [1] and the sensitivity of chaotic trajectories to the initial conditions, many chaos based image encryption algorithms [2–15] have been proposed in recent years. Wang et al. [2] utilized the chaotic system to encrypt the R,G,B components of a color image at the same time to reduce the correlation within the signals and increase the security of the algorithm. Kumar et al. [3] proposed an extended substitution–diffusion based image cipher, which utilized chaotic standard map and linear feedback shift register to add nonlinearity. Patidar et al. [4] proposed a loss-less symmetric block cipher, which was a chaos-based pseudorandom permutation–substitution scheme for image encryption. Gao et al. [5] employed an image total shuffling matrix to shuffle the positions of image pixels and used a hyper-chaotic system to confuse the relationship between the plain-image and the cipher-image. Rhouma et al. [6] proposed an OCML-based color image encryption scheme with a stream cipher structure. Mirzaei et al. [8] proposed a total shuffling and parallel encryption algorithm. Fu et al. [9] proposed an improved diffusion strategy to promote the efficiency of the most widely investigated permutation–diffusion type image cipher. Huang et al. [10] utilized the multi-chaotic systems to get unpredictable sequence and combined four different chaotic systems and pixel shuffling to banish the outlines of the original image. Seyedzadeh et al. [11] encrypted color images with a coupled two-dimensional piecewise nonlinear chaotic map and a masking process. Ye et al. [12] proposed a permutation–diffusion algorithm, in which the yielded gray value sequences were not only sensitive to the control parameters and initial conditions, but also dependent on the plain image processed. Tong et al. [14] designed a new two-dimensional chaotic function using two one-dimensional chaotic functions, and utilized the compound chaotic functions to encrypt the image. Wang et al. [15] proposed a delayed fractional-order chaotic logistic system

* Corresponding author.
E-mail addresses: liuyang@hitwh.edu.cn (Y. Liu), tong_xiaojun@163.com (X. Tong).

0923-5965/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.image.2013.07.009

based image encryption scheme. The time-varying delay and fractional derivative were embedded into the scheme to improve the security. In these algorithms, the maps used are conventional chaotic maps [2–7], combination of several chaotic maps [8–10], the transformation of conventional chaotic maps [11,12] or some new chaotic maps [13,14]. These chaotic maps are all defined in the real number field.

In recent years, many complex analysis theories [16] are used for studying chaos. For example, Mahmoud et al. [17,18] introduced several chaotic systems with complex variables and analyzed their chaotic behaviors. Moreover, there are many nonlinear dynamical systems in which the main variables are complex. They are related to physical magnitudes that naturally possess real and imaginary parts. Secure communication to complex-variable chaotic systems, which can increase the number of state variables, can further enhance the security of private communications. Complex-variable chaotic systems have many potential applications [19]. At present, most researches about complex-variable chaotic systems aim at performance analysis [17,18] and chaos synchronization [19–21]. There are few researches about applying complex-variable chaotic systems to produce pseudorandom sequences and encrypt images [22]. We think that using the complex number based chaotic map in pseudorandom number generation and image encryption is a new idea. In this paper, we prove a family of complex number maps chaotic and propose new pseudorandom number generation and image encryption algorithms based on this chaotic maps family. It is a generalization from the real number field to the complex number field.

The rest of this paper is organized as follows. Section 2 proves a family of maps to be chaotic in the complex number field. Section 3 describes the generation and performance analysis of pseudorandom keystream based on the proposed chaotic maps. Section 4 presents the proposed cryptosystem and Section 5 shows its performance and security analysis. Finally, the conclusions are drawn in Section 6.

2. A family of new complex number chaotic maps

In this section, a family of maps is proved to be chaotic in the complex number field and its characteristics are analyzed.

2.1. Proof of complex number chaotic maps family

First, we will prove a lemma.

Lemma 1. *In the complex field C, the chaotic area of the squaring map*

$$h(x)=x^2 \tag{1}$$

is the unit circle.

Proof: we express the squaring map with iteration form $z_{n+1}=z_n^2$. Let z_0 be an arbitrary point in C.

If $|z_0|<1$, then there is

$$|z_{n+1}|=|z_n{}^2|=|z_n|^2=|z_{n-1}{}^2|^2 =|z_{n-1}|^4=\ldots=|z_0|^{2^{n+1}}\underset{n\to\infty}{\to}0$$

If $|z_0|>1$, then there is

$$|z_{n+1}|=|z_n{}^2|=|z_n|^2=|z_{n-1}{}^2|^2 =|z_{n-1}|^4=\ldots=|z_0|^{2^{n+1}}\underset{n\to\infty}{\to}\infty$$

If $|z_0|=1$, then z_0 belongs to the unit circle in the complex field. Let S denote the unit circle in the complex field. The point on S expressed by polar coordinates is $e^{i\theta}$ (i is the imaginary unit), then the squaring map (1) can be represented by

$$h(e^{i\theta})=e^{2i\theta} \tag{2}$$

If we denote the point on S with radian number, then Eq. (2) is turned into

$$h(\theta)=2\theta \tag{3}$$

while $h(\theta)=2\theta$ is chaotic on the unit circle [1]. Consequently, the squaring map (1) is chaotic on the unit circle.

Now we prove that a family of maps is chaotic in the complex field.

Proposition 1. *Let l be a straight line passing through the original point in the complex plane, the angle between l and the positive horizontal axis be θ ($\theta\in[0,\pi)$), then the map*

$$x_{n+1}=\frac{2e^{(\pi+2\theta)i}x_n}{e^{(\pi+2\theta)i}+x_n^2} \tag{4}$$

is chaotic on l.

Proof. First, let us represent this straight line l with a formula. We divide the complex plane into two parts: I={the part above the horizontal axis}∪{the positive horizontal axis}∪{the original point}, II={the part below the horizontal axis}∪{the negative horizontal axis}. Let x be an arbitrary point on l, the distance from x to the original point is $\rho(\rho\geq 0)$. Then l can be expressed by

$$x=\begin{cases}\rho e^{i\theta}, & x\in \mathrm{I}\\ \rho e^{i(\theta+\pi)}, & x\in \mathrm{II}\end{cases} \tag{5}$$

where i is the imaginary unit. Since $\rho e^{i(\theta+\pi)}=-\rho e^{i\theta}$, then there is

$$x=\begin{cases}\rho e^{i\theta}, & x\in \mathrm{I}\\ -\rho e^{i\theta}, & x\in \mathrm{II}\end{cases} \tag{6}$$

For simplicity, let $\rho\in(-\infty,+\infty)$, then l can be expressed by

$$x=\rho e^{i\theta},\quad \rho\in(-\infty,+\infty),\quad \theta\in[0,\pi) \tag{7}$$

while $|\rho|$ expresses the distance from x to the original point. When $\rho\geq 0$, $x\in$ I, and when $\rho<0$, $x\in$ II. With trigonometric representation of complex number, Eq. (7) can be expressed by

$$x=\rho(\cos\theta+i\sin\theta),\quad \rho\in(-\infty,+\infty),\quad \theta\in[0,\pi) \tag{8}$$

In the following, we will utilize Eqs. (7) and (8) to express the straight line l passing through the original point in the complex plane. Obviously, for an arbitrary point $x_0=\rho_0(\cos\theta+i\sin\theta)$, there is $\rho_0\sin\theta/\rho_0\cos\theta=\tan\theta$.

Download English Version:

https://daneshyari.com/en/article/537629

Download Persian Version:

https://daneshyari.com/article/537629

Daneshyari.com