Image encryption algorithm based on chaotic color mixing

Massimiliano Zanin
Universidad Autónoma de Madrid
28049 Cantoblanco, Madrid, Spain

E-MAIL: massimiliano.zanin@hotmail.com

COLABORADORES: A. N. Pisarchik (Centro de Investigaciones en Optica, Guanajuato, Mexico)

In the last years, cryptography has become a field of great interest in many areas, such as secure data storage, Internet transaction or communication channels; in particular, chaos based encryption schemes have been studied ([2], [3]), due to the high sensitivity of those systems to initial conditions, that assures strong resistance against any statistical attacks. Recently one of us [1] proposed an algorithm for image encryption, based on multiple chaotic logistic maps, one-way coupled by initial conditions, with good cryptographic properties like high sensitivity to secret keys and absence of patterns in the encoded data.

In the present work, we go further in developing a strong chaos-based algorithm for image encryption; moreover, the problem of real-time communication is taken into account, that implies an extremely short encryption /decryption time (EDT), and tolerance to random noise. The basic idea is to convert a $M \times N$ image to a linear array $\mathbf{P}$ of $h = 3MN$ items, each of which represents a single color component of every pixel, with integer values between 0 and 255. The encryption algorithm consists in mixing the components in this array by a chaotic way to obtain a new array of the same length, that can be represented back as an image. More specifically, an uni-dimensional chaotic iterative map

$$x_{n+1} = Q(a, x_n), \tag{1}$$

is defined, where Q is a nonlinear map function, x_n is the system state after n iterations, and a is the map parameter that acts as a secret key of the system. By this way, we can define the mixing function $F : \mathbf{P} \rightarrow \mathbf{S}$ such that

$$\mathbf{S} = F(p_j, p_k) mod(255), \tag{2}$$

where

$$k = round[Q_j(x_0)h]. \tag{3}$$

We carried out computer experiments using the well-known logistic map (LM) as the map function Q with a variety of color images. It is easy to show that the most dangerous attack, the known-plaintext attack, is unfeasible, because information is mixed and distributed over whole image in a complex strategy that dissolves any pattern in the original data. To estimate EDT, calculations were made with a standard PC, resulting in about 28 images per second, for an image size of 720 x 480 pixels (standard NTSC television dimension). Moreover, the algorithm demonstrates a good tolerance to noise. When a pixel is modified due to disturbance while transmitting a codified image, color components of the decrypted image are modified; nevertheless, for small noise, only isolated components are affected and hence the overall information to the human eye is maintained. Thanks to that, this algorithm can be successfully used in encrypted real-time communications, without any special hardware codec.

Bibliografía

[1] A. N. Pisarchik *et al.*, *Encryption and decryption of images with chaotic map lattices*, Chaos **16**, 033118 (2006).

[2] K. Kaneko *et al.*, *Complex Systems: Chaos and Beyond: A Constructive Approach with Applications in Life Sciences*, Springer-Verlag, Berlin (2001).

[3] S. Wang *et al.*, Phys. Rev. E **66**, 065202(R) (2002).

Justificación de interdisciplinariedad: Chaos theory, specially non-linear maps, have been an important instrument for a variety of fields, from electrical circuits to heart diseases control, since the original works of E. N. Lorenz in the '60. By applying chaotic maps to image encryption, a wide field of application is opened, that includes real-time communication for pay-per-view contents, secure data storage, and, as a goal for future works, 3D images (holograms) cryptography.