Computers and Electrical Engineering 000 (2015) 1–13

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A chaos-based image encryption algorithm with simple logical functions☆

Erdem Yavuz[a], Rifat Yazıcı[a], Mustafa Cem Kasapbaşı[a,*], Ezgi Yamaç[b]

[a] *Department of Computer Engineering, Istanbul Commerce University, Kucukyali E5 Kavsagi Inonu Cad. No: 4 Istanbul, 34840/Kucukyali, Turkey*
[b] *Department of Computer Engineering, Istanbul University Avcılar Istanbul, Turkey*

ARTICLE INFO

Article history:
Received 29 December 2014
Revised 9 October 2015
Accepted 6 November 2015
Available online xxx

Keywords:
Image encryption
Chaos
Low entropy
Security analysis

ABSTRACT

This paper proposes an effective chaos-based encryption algorithm specialised for images. A system of two independent chaotic functions with high sensitivity to initial states, is utilised to sufficiently apply confusion and diffusion principles for images with any entropy. One of the functions is used for shuffling pixel positions while the other for changing the values of pixels. In the resulting new pixel organisation, adjacent pixels with naturally close values will take on considerably different values, making it difficult to crack the encrypted image. To increase resistance of the system to differential attacks, some logical operations such as exclusive-or and circular rotation are used to spread the effect of a slight change in single pixel intensity of plain image over many pixels in cipher-image. A variety of analyses and tests has been carried out to prove the security and the validity of the algorithm. Even with low entropy images the proposed algorithm has been proved to be more secure and faster than the previous algorithms.

1. Introduction

Since there has been a rapid advance in computing technology, developing effective techniques for secure storing and transmitting digital image data has become an important issue for researches. Applications especially for secure image storage and communication require image data production against unauthorised users. Whenever an image has to be employed in an application, image security becomes a crucial concept. In the last decade, many different encryption algorithms relied on diverse principles have been published in the literature [1]. Due to the specific characteristics of chaotic systems, chaos based encryption methods seem to be more efficient for practical use regarding reasonable speed, high security and complexity [2].

It is expected from an ideal cipher to fulfill some fundamental cryptographic requirements as confusion, diffusion, and randomness. Chaotic systems offer advantages of random behaviour and greater sensitivity to initial conditions, so introduce very large space to resist brute force attacks. Since digital images inherently have redundant data, high similarity for neighbouring pixels, and less sensitivity to a tiny change in pixel attribute, the security requirements of digital images increase the importance of chaos based encryption methods [3,5].

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. E. Cabal-Yepez.

* Corresponding author. Tel.: +905335447486.
E-mail addresses: eyavuz@ticaret.edu.tr (E. Yavuz), ryazici@ticaret.edu.tr (R. Yazıcı), mckasapbasi@ticaret.edu.tr, mckasap@gmail.com (M.C. Kasapbaşı), ezgi.yamac@ogr.iu.edu.tr (E. Yamaç).

http://dx.doi.org/10.1016/j.compeleceng.2015.11.008
0045-7906/

Based on the above discussion, an enhanced chaotic system with two Logistic Maps is proposed in this paper. The first Logistic Map is used to scramble the plain image for reducing correlation between adjacent pixels. So, statistical analysis becomes difficult to crack the cipher image. The purpose of the second Logistic Map is to further increase the confusion by changing the pixels' values (i.e. decreasing the relationship between the plain image and the cipher image). In addition, the second Logistic Map makes it possible for the image data with any entropy structure to be securely encrypted. In order to reflect the influence of slight change in single pixel intensity of plain image on larger number of pixels in cipher-image, some logical operations such as XOR and circular rotation are exploited with the proposed algorithm.

The main improvements of this paper can be summed up as: (1) to better shuffle the plain image for encryption, only two chaotic Logistic Maps are used together with some logical operations, (2) to get more uniform histogram for low entropy images, disruption of plain image is achieved in only a few rounds, (3) to resist differential attacks, the influence of one bit change in single pixel is spread over many pixels with the logical operations mentioned above.

1.1. Related works

Chaotic systems have attracted attention of many researchers due to their inherent features such as ergodicity and pseudo-randomness, sensitivity to initial conditions and control parameters. Chaos-based encryption algorithms have been widely used for image encryption [1,2,4–9,11] because they are easy to be realised compared with traditional crypto-systems such as AES, DES etc. [12].

One of the most cited image encryption schemes is offered by [13] which proposes permutation and diffusion processes governed by 2D map and 1D chaotic maps respectively. In the study Fridrich first discretized Baker-map, then extended it to three dimensions and composed it with a simple diffusion mechanism. Subsequent proposed works in the field [10,11] are highly influenced by this work .

In [10] it is proposed a chaos-based image encryption algorithm with variable control parameters derived from plain-image in order to improve resistance to all known attacks. They used three maps namely Standard map, Cat map and Baker map in the permutation stage of their algorithm to compare performances of each map. Their work resulted in higher security and faster encryption speed for practical applications.

In [7] it is proposed chaos based symmetric block cipher composed of a confusion process based on chaotic standard map, a diffusion function and a key generator for encrypting large volume data sets. Their algorithm reportedly has satisfactory security level and short run times.

In [5] a new symmetric chaotic encryption based on bit level permutation was proposed by using Logistic Map. This study has achieved required security level consecutively running many rounds of diffusion and confusion processes, but resulting in longer processing time and heavy computational load.

In this paper, inspired by the [5] a novel chaotic image encryption scheme with two Logistic Maps is proposed. The proposed scheme performs diffusion process faster and more effectively by figuring on the previously encrypted byte for the encryption of next byte and rotating the resulting byte to get more complex disruption on the pixel. So a slight change in plain-image results in substantially different cipher image in much shorter time.

The paper is organized as follows: Section 2 introduces the proposed encryption system including description of encryption/decryption algorithm. In Section 3, security analysis, speed performance, complexity analyses of the proposed algorithm and the results of these analyses are given in detail. Section 3 finally concludes the paper.

2. The proposed encryption system

The proposed scheme uses an iterative process to encrypt a sequence of bytes which is the 1D transformed version of the 2D original image. Two independent chaotic functions are used as given in Eqs. (2) and (3). One of them is used to permute pixel positions while the other used to change intensity values of pixels. These functions together ensure confusion and diffusion operations required for encryption. The algorithm is also supported with some logical operations to further increase security and to decrease encryption time.

2.1. Chaotic behaviour of the Logistic Map

In the present study, a chaotic function known as Logistic Map is used:

$$f(x) = \lambda x(1-x), 3.57 < \lambda < 4. \quad (1)$$

Chaotic behaviour of the function depends entirely on the value of λ, which is constrained to the range of (3.99,4) to make the function operate in the most chaotic region. Bifurcation diagram of the Logistic Map is given in Fig. 1. It can be seen from Fig. 1 that as the value of λ approaches to 4, the output of the function takes on more distinct values ranging from 0 to 1. Discrete form of the chaotic function used is given in Eqs. (2) and (3). Our aim for using Logistic Map is to benefit from its well-known chaotic behaviour to perform more complex pixel permutation, namely better diffusion operation. One of the functions is used to find new positions of the pixels while the other operates to modify their intensities.

2.2. Encryption/decryption algorithm

In the presented crypto-system, two separate Logistic Maps are utilised for both encryption and decryption processes. The Logistic Maps are given in Eqs. (2) and (3) where x_{i+1} and y_{i+1} are state values with $i = 0, 1, 2, \ldots$; $\lambda_1$and λ_2 are the parameters

Please cite this article as: E. Yavuz et al., A chaos-based image encryption algorithm with simple logical functions, Computers and Electrical Engineering (2015), http://dx.doi.org/10.1016/j.compeleceng.2015.11.008