Chapter 2

A Review on Chaos–Based Image Encryption Using Fractal Function

Anandkumar R.
Pondicherry Engineering College, India

Kalpana R.
Pondicherry Engineering College, India

ABSTRACT

The tremendous development in the field of telecommunication and computer technologies leads to the preference of transferring information as a digital data. In this transformation of information, cryptography helps in encrypting/decrypting digital data, so that intruders will not be able to sniff the highly confidential information. Most information is transferred as a digital image, where image encryption is done by scrambling the original pixels of the image, and hence, the correlation between the original pixel and scrambled pixel differs leading to confusion to unauthorized accesses. Chaotic image encryption is one of the recent technologies in cryptosystems, where a pseudorandom and irregular key is used for encryption/decryption, as the key suffers a great change if some initial conditions are altered, leading to highly secured transmission in the network. In this chapter, a detailed survey is conducted on chaotic image encryption using fractal function, in which fractal key is used for encryption and decryption of an image.

DOI: 10.4018/978-1-7998-0066-8.ch002

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
INTRODUCTION

Encryption of images transferred through an open medium, can be very easily hacked by unauthorized users and is vulnerable to unexpected changes in the image leading to the breech of confidential information. Various procedures are being proposed till now, in order to protect the confidentiality of the image-based information from intruders. All techniques encompass the vital criteria mentioned in the following section:

- **Low Correlation**: The original image and the encrypted image should not correlate can be preferably so zero, so that the attackers will not be able to predict the encrypted image (Kumari et al., 2017).
- **Large Key Size**: The larger the key size, there will be very less probability for brute force attack (Kumari et al., 2017).
- **Key Sensitivity**: When an intruder tries to manipulate the image pixel in order to decrypt the confidential image, that activity or any minute change, should lead to a completely different encrypted image (Kumari et al., 2017).
- **Less Time-Complexity**: The whole image encryption/decryption methodology should consume very less time, as the performance may degrade if the methodology has higher time (Kumari et al., 2017).
- There are more than 15 image encryption techniques, which preserves the image from unintended users as well as, encompassing the above discussed criteria. The following are the image-based encryption algorithm:
  - Vigene`re Cipher
  - Data Encryption Standard (DES)
  - International Data Encryption Algorithm (IDEA)
  - Blowfish
  - Visual Cryptography
  - RC4, RC5, RC6
  - Triple Data Encryption Standard (TDES)
  - Advanced Encryption Standard (AES)
  - Scheme Based on Intertwining Chaotic Maps
  - Scheme Based on Chaotic Function Using Linear Congruence’s
  - Scheme Based on Mixed Transform Logistic Maps
  - Scheme Based on Peter De Jong Chaotic Map and RC4 Stream Cipher
  - Scheme Based on Chaotic Map and Vigene`re Scheme
Related Content

Efficient Data Access Control for Cloud Computing With Large Universe and Traceable Attribute-Based Encryption

An Efficient Time Series Forecasting Method Exploiting Fuzziness and Turbulences in Data
Application of Artificial Intelligence Techniques to Handle the Uncertainty in the Chemical Process for Environmental Protection
www.igi-global.com/chapter/application-of-artificial-intelligence-techniques-to-handle-the-uncertainty-in-the-chemical-process-for-environmental-protection/123088?camid=4v1a

A Review of Contemporary Image Compression Techniques and Standards
www.igi-global.com/chapter/a-review-of-contemporary-image-compression-techniques-and-standards/236824?camid=4v1a