Chaotic map-embedded Blowfish algorithm for security enhancement of colour image encryption. (English) Zbl 1348.94007

Summary: The quest for achieving an accurate and efficient algorithm in enhancing the security of colour image encryption is never-ending. We enhance the security level of conventional Blowfish algorithm (BA) for colour image encryption by modifying it with new F-function. The dynamic S-box and XOR operator are generated from the F-function via four-dimensional hyper-chaotic map, and the number of iterations is dramatically reduced from sixteen to four to simplify the processing complexity. The block secret keys of varying space size are randomly created. The computation is performed using Matlab R2008a codes on eight images of size $512 \times 512$ pixels obtained from standard USC-SIPI Image Database. The security of the proposed method exhibits notable enhancement with increasing block size. Performance analyses reveal a correlation coefficient less than $-0.0016$ and entropy greater than 7.9993. Furthermore, the distribution of RGB channel for image Lena displays sizeable security improvements. Correlation between image pixels is significantly decreased with higher entropy. In comparison with previous works, the proposed algorithm is found to exhibit superior performance for colour image encryption than the conventional BA.

MSC:
94A08 Image processing (compression, reconstruction, etc.) in information and communication theory
94A60 Cryptography
37D45 Strange attractors, chaotic dynamics of systems with hyperbolic behavior

Keywords:
colour image encryption; Blowfish algorithm; chaotic map; image entropy; block image encryption correlation

Software:
Blowfish; Matlab

Full Text: DOI

References:

Parameshachari, BD; Sojyuadh, KMS; Chaitanyakumar, MV, A study on different techniques for security of an image, Int. J. Recent Technol. Eng., 1, 14-19, (2013)


Norouzi, B; Mirzakouchaki, S; Seyedzadeh, SM; Mosavi, MR, A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process, Multimed. Tools Appl., 61, 1-29, (2012)


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.