A novel image encryption algorithm based on chaos maps with Markov properties.


Summary: In order to construct high complexity, secure and low cost image encryption algorithm, a class of chaos with Markov properties was researched and such algorithm was also proposed. The kind of chaos has higher complexity than the Logistic map and Tent map, which keeps the uniformity and low autocorrelation. An improved couple map lattice based on the chaos with Markov properties is also employed to cover the phase space of the chaos and enlarge the key space, which has better performance than the original one. A novel image encryption algorithm is constructed on the new couple map lattice, which is used as a key stream generator. A true random number is used to disturb the key which can dynamically change the permutation matrix and the key stream. From the experiments, it is known that the key stream can pass SP800-22 test. The novel image encryption can resist CPA and CCA attack and differential attack. The algorithm is sensitive to the initial key and can change the distribution the pixel values of the image. The correlation of the adjacent pixels can also be eliminated. When compared with the algorithm based on Logistic map, it has higher complexity and better uniformity, which is nearer to the true random number. It is also efficient to realize which showed its value in common use.

Keywords: chaos; Markov; complexity; cipher

doi:10.1016/j.cnsns.2014.06.005