Weakness analysis and performance improvement of an image encryption algorithm based on chaotic system crossing a cylinder

Zhao Chaofeng*, **Ren haipeng***

**Shaanxi Key Laboratory of Complex System Control and Intelligent Information Processing, Xi'an University of Technology, Xi'an 710048, P.R.China*

Abstract. We analyze and improve a typical class of chaotic image encryption algorithms which have no valid diffusion operation. The image encryption algorithm [1] based on chaotic system crossing a cylinder is analyzed, and several security weaknesses due to inadequate diffusion are pointed out. Using chosen plain-text attacks, the equivalent keys of the cryptosystem are cracked, so that the target encrypted image can be decrypted. An improved image encryption algorithm is proposed based on the original algorithm. A connection between plain-text images and security keys is created, therefore, the improved algorithm remedies the missing of diffusion and resists against chosen plain-text attacks. The security analysis and extensive tests of the improved algorithm show that the proposed algorithm significantly increases the security while keeps all merits of the original algorithm, and achieves better performance as compared to some existing algorithms.

Introduction

Due to the attracting features, such as the extreme sensitivity to initial conditions and system parameters, ergodicity and random like behaviors, chaos is considered as one of ideal tools for image encryption[2]. However, the image encryption algorithm [1] based on chaotic system crossing a cylinder is proved to be lack of effective diffusion operation. The present paper analyses and evaluates the security performance of the algorithm in [1] to show its weaknesses, including: (1) the key sensitivity analysis is not given; (2) the key is not related to the plain-text image; (3) it can't resist chosen plain-text attack and differential attack. To deal with the weaknesses, an improved image encryption algorithm (as shown in Fig.1(a)) is proposed by adding the diffusion operation and creating a connection between plain-text images and security keys in order to remedy the missing of diffusion and to resist chosen plain-text attack and differential attack.

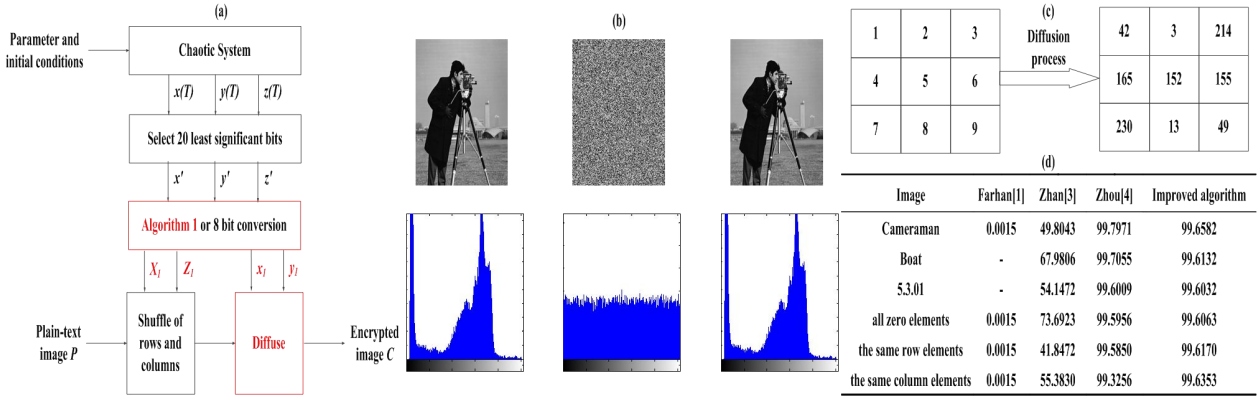

Image	Farhan[1]	Zhan[3]	Zhou[4]	Improved algorithm
Cameraman	0.0015	49.8043	99.7971	99.6582
Boat	-	67.9806	99.7055	99.6132
5.3.01	-	54.1472	99.6009	99.6032
all zero elements	0.0015	73.6923	99.5956	99.6063
the same row elements	0.0015	41.8472	99.5850	99.6170
the same column elements	0.0015	55.3830	99.3256	99.6353

Figure 1: (a) The flowchart of the improved algorithm; (b) Statistical performance; (c) Diffusion; (d) NPCR results.

Results and discussion

First, using chosen plain-text attacks, the target encrypted image by Farhan's algorithm is found to be easily decrypted, and two commonly indices NPCR and UACI, which were far away from ideal values 99.6094% and 33.4635%, respectively, are used to show that Farhan's algorithm cannot resist differential attack. Meanwhile, it is found that Farhan's algorithm is not fit for different size of image. Second, the improved image encryption algorithm based on the basic structure of Farhan's algorithm is proposed by introducing diffusion operation (as shown by Fig.1(c)) and creating a connection between plain-text images and security keys. In particular, for diffusion operation, the encrypted pixel value is not only related to the corresponding plain-text pixel value and the security key, but also related to the former plain-text pixel values and former encrypted pixel values. Meanwhile, the proposed algorithm can adapt to different image size. Third, the performance analysis show that the improved algorithm has very competitive performance in key sensitivity, statistical performance (as shown by Fig.1(b)), differential analysis (as shown by Fig.1(d)), chosen plain-text attack resistance, robustness to partial data loss, efficiency, etc. Meanwhile, it also shows that the improved algorithm significantly improves the security of encryption images while still keeps all the merits of the original Farhan's algorithm, thus shows a better potential for application. Finally, compared with some existing image encryption algorithms based on chaos [1,3,4], the improved image encryption algorithm has better performance.

References

[1] Farhan, A. K., Al-Saidi, N. M. G., Maolood, A. T. (2019) Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder. *Entropy* **21**: 958.

[2] Zhao, C. F., Ren, H. P. (2020) Image encryption based on hyper-chaotic multi-attractors. *Nonlinear Dynam* **100**: 679-698.

[3] Zhan, K., Wei, D. (2017) Cross-utilizing hyper chaotic and DNA sequences for image encryption. *J. Electron. Imaging* **26**: 0130221.

[4] Zhou, Y. C., Bao, L., Chen, C. L. P. (2014) A new 1D chaotic system for image encryption. *Signal Process* **97**:172-182.