

Image Encryption Scheme Based on Dynamics System

Liang Zhao

Graduate School of Information Science and Electrical Engineering
Kyushu University, Fukuoka, Japan 819-0395

e-mail: zhaoliang@itslab.csce.kyushu-u.ac.jp

website: <http://itslab.csce.kyushu-u.ac.jp/~zhaoliang/index.htm>

Abstract

Multimedia security is already one of the most crucial problems in information science. Many researchers have introduced and analyzed some protection methods for multimedia data, such as the encryption, watermarking and steganography. In particular, the encryption scheme is considered as a direct and effective method for the multimedia data. Digital image, which is one of the most important multimedia information, is seen as the most effective carrier for people to obtain the outside information. Each person can achieve the useful information directly by viewing an image on Internet. Therefore, the security protection on the digital image is an urgent and crucial problem.

Some typical methods for encrypting the image data include the traditional symmetry cryptography, such as DES and AES, image permutation method and Substitution-Permutation Networks (SPN). Recently, image encryption based on dynamics system attracts the interest of many researchers studying the image security. Specially, Introduction of chaos system in image encryption scheme is considered as a promising direction. This is due to the fact that chaotic systems possess several properties which make them be suitable for constructing image cryptosystems, such as randomness, sensitivity, simplicity and ergodicity. For example, Chen et al. [1] introduced an image encryption algorithm based on 3D Arnold's cat map. Lian et al. [2] proposed an image encryption scheme which makes use of the standard map.

In the present article, an especial image encryption structure, named Partitioning Substitution and Diffusion-Integration Substitution Network Structure, is proposed, which is different from the traditional ones [3]. According to this proposed structure, a detailed image encryption scheme is presented, and some analyses about the proposal are also introduced.

References

- [1] Chen G., Mao Y., Chui C., Symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals* 21(3), pp.749–61, 2004.
- [2] Lian S., Shun J., Wang Z., A block cipher based on a suitable use of the chaotic standard map. *Chaos, Solitons & Fractals* 26(1), pp.117–29, 2005.
- [3] Zhao L., Xiao D., Sakurai K., Image Encryption Design Based on Multi-Dimensional Matrix Map and Partitioning Substitution and Diffusion-Integration Substitution Network Structure. *International Conference on Information Science and Applications (ICISA)*, pp.1–8, 21–23 April 2010.