BẢO MẬT ẢNH DỰA TRÊN HỘP THAY THẾ VÀ LÝ THUYẾT HỖN ĐỘN

IMAGE ENCRYPTION BASED S-BOX AND MULTI CHAOS

Nguyễn Anh Dũng[1,*], Ngô Văn Huấn

TÓM TẮT

Bài báo đề xuất thiết kế hộp thay thế S-box mới sử dụng Triangle-Chaotic (TCM), Logistic 1D cải tiến. Đề xuất phương án bảo mật ảnh dùng hàm Chaos 2D cross để xáo trộn vị trí điểm ảnh, thay đổi giá trị điểm ảnh sử dụng S-box và Logistic 1D. Sử dụng các tiêu chuẩn đánh giá chất lượng ảnh bảo mật để kiểm tra phương án đề xuất, kết quả chỉ ra phương án đề xuất đảm bảo yêu cầu.

Từ khóa: *Chaos, S-box, Logistic, Triangle-Chaotic(TCM), bảo mật ảnh, hộp thay thế.*

ABSTRACT

In this paper, a new S-box is proposed base on combination Triangular Chaotic Map (TCM) and improved 1D Logistic Chaos. Then the shuffled image is used by 2D cross Chaos, diffusion of image pixel using S-box and Logistic 1D. After analysis and test, the algorithm satisfies the requirments of safety image encryption.

Keywords: *image encryption, S-box, 2D cross map, Triangular Chaotic Map (TCM), 2D Cat, Improved 1D Logistic.*

[1]Khoa Điện tử, Trường Đại học Công nghiệp Hà Nội
[2]Khoa Điện tử, Học viện Kỹ thuật Quân sự
**Email: anhdung0412@gmail.com*
Ngày nhận bài: 28/12/2017
Ngày nhận bài sửa sau phản biện: 27/3/2018
Ngày chấp nhận đăng: 21/8/2018