Cryptography System using Efficient Chaos Based Feedback Stream Cipher

Myo Min Thein, Win Win Zaw

University of Computer Studies, Yangon

myominthein46@gmail.com, comwwzawucsy@gmail.com

Abstract

Today. More and more information has been transmitted over the World. The information is not only text, but also audio, image, and other multimedia Images have been widely used in our daily life. This paper presents on efficient chaos based feedback stream cipher (ECBSFC) for image cryptosystems. The proposed stream cipher is based on the use of ac chaotic logistic map and an external secret key of 256-bit. The initial conditions for the chaotic logistic map are derived using the external secret key by providing weight age to its bits corresponding to their position in the key. Further, new features of the proposed stream cipher include the heavy use of data-independent iterations, data-dependent inputs, and the inclusion of three independent feedback mechanisms. These proposed features are verified to provide high security level. A complete specification for the proposed ECBFSC is given.