Resenha

Texto

Nardo, L. G., Lima, A. M., Nepomuceno, E. G., Arias-Garcia, J. (2018). Image Encryption Algorithm Using Natural Interval Extensions.

Comentários

Cada vez mais métodos de criptografia vem sendo desenvolvidos para suprir a necessidade, que também vem crescendo, de obter controle ao acesso de informações. Uma parte desses métodos utiliza sistemas caóticos, que mostram-se muito convenientes na criptografia de dados devido suas principais características (transitividade, sensibilidade à condições iniciais e a geração de órbitas pseudo-aleatórias). Este artigo propõe um método de criptografia de imagens usando extensões intervalares naturais.

A sequência pseudo-aleatória é gerada a partir da simulação do circuito de Chua, usando o método de Range-Kutta de quarta ordem e as duas extensões intervalares naturais representados em (1).

$$C_1\frac{dv_{C_1}}{dt} = \frac{v_{C_2} - v_{C_1}}{R} - i_R(v_{c_1}), \qquad C_1\frac{dv_{C_1}}{dt} = \frac{v_{C_2}}{R} - \frac{v_{C_1}}{R} - i_R(v_{c_1}) \tag{1}$$

A pesquisa é realizada de modo que primeiramente simula-se as extensões intervalares excluindo os 2000 primeiros pontos, que por serem muito próximos nas duas pseudo-órbitas, tornam o sistema menos seguro. Após isso realiza-se o logaritmo do lower bound error, gerando assim uma só sequência que passa por um processo de normalização. Para finalizar o processo de criptografia, faz-se a operação XOR entre a imagem e a chave (sequência gerada).

Realizando o método acima chega-se a um histograma da imagem criptografada com uma distribuição uniforme, gerando uma imagem ilegível. Além disso, a entropia calculada e os coeficientes de correlação são relativamente próximos aqueles encontrados na literatura. A descriptografia também é facilmente implementada com o processo oposto. Esse método mostrou-se eficiente para sua proposta, já que gerou uma sequência pseudo-aleatória com boas propriedades criptográficas.

Autor: Dyulia Rossi Fiorio, 15/09/2019.