Image Encryption Using Lorenz's Attractor and Fractional Fourier Transform

Ökkeş Erdem TEKEREK
Kahramanmaraş Fen Lisesi,
Kahramanmaraş, Turkey
okkeserdemt@gmail.com
ORCID:0000-0001-7281-9486

Adem TEKEREK
Computer Engineering Department,
Technology Faculty, Gazi University
Ankara, Turkey
atekerek@gazi.edu.tr
ORCID:0000-0002-0880-7955

Abstract— In this study, a new image encryption and decoding algorithm is developed using fractional fourier transform, lorenz attractor and masking. In the proposed algorithm, firstly, the image is masked with a randomly generated mask and fractional fourier transform is applied to the masked image. These two processes were applied 3 times in a row, making the image more complex. The resulting image was then decomposed into 256 parts. 16 chaotic outputs were obtained from lorenz attractor. These outputs are calculated in base 256. The parts with the same index number as the output were selected and mixed among themselves. The scrambled image parts are combined and the encryption process is completed. The degree of the function applied in the algorithm is a rational number. The use of lorenz attractor provides chaotic outputs. These 2 features make the algorithm resistant to attacks. The use of a chaotic set of differential equations is reduced the probability of finding the scrambled method by an analytical approach and the linear predictability of the method for attacks on the scrambled image. The analysis of chaotically generated random numbers was made and produced successful results. The algorithm is confidential and usable against most common attacks such as brute force. The data contained in the key is encrypted using the RSA algorithm.

Keywords— *Fractional Fourier Transform, cryptology, chaos*