Abstract

The PhD Thesis *Cryptographic methods and techniques using chaos theory and statistics* is featuring an important issue of nowadays life, security of data. It is structured in six chapters from which the first one places this work in the larger domain it belongs to and the last one concludes the original contributions proposed by its author and traces new directions to be investigated. *Chapter 2* presents a statistical mean test on the autocorrelation function of the chaotic maps and how it relates to the statistical independence sampling distance. The influence of the working numerical precision on the obtained results is also analysed in this chapter. *Chapter 3* presents a pseudo-random number generator (pRNG) based on some three-dimensional chaotic maps. It is built in such a way that it enables the pseudo-randomness whether the parameters of the map engender chaotic behavior or not, by dynamically changing the evolution of the underlying system. The statistical analysis of a matrix issued by chaotic maps is presented in *Chapter 4*. The aim is to estimate the secret key used to generate the pseudo-random enciphering matrix used for encryption. Public knowledge is the way the matrix is built, but not the secret parameters the transmitter used for its generation. Several statistical methods and techniques - Smirnov test, histograms, autocorrelation function, successive iterations - are used for this estimation and their results are compared. *Chapter 5* evaluates the possibility of using wavelet packets together with chaotic maps in cryptographic algorithms and the benefits of this approach. Conclusions and some perspectives in this area are presented in *Chapter 6*, alongside with highlighting the main contributions brought by the present work.