

Numerical methods and chaotic maps

Léa Cot, LATTIS-INSA, Université de Toulouse

Danièle Fournier-Prunaret, LATTIS-INSA, Université de Toulouse

Mots-clés : Dynamical systems, cryptosystem, chaotic signals, parameter estimation, Gauss-Newton, Extended Kalman Filter

A comparative study of the Gauss-Newton and Kalman filter methods has been carried out to test the robustness of a digital chaos-based cryptosystem against potential attack.

Many chaotic cryptosystems have been developed to improve the security of transmissions. Indeed, chaotic signals may be generated by determinist models but they are similar to random noise. So, they may be used to conceal information and encipher transmission by mixing them with the message in an appropriate manner.

Our study uses nonlinear chaotic maps depending on parameters. Because of the high sensitivity of chaos to initial conditions, by slightly modifying the initial conditions, sequences with similar distributions can be generated, but will never take the same values. We suppose that the chaotic map is known but not the parameters nor the initial conditions. Because these exact values are unknown, a hacker cannot reconstruct the chaotic sequences and decipher the message. He may therefore try to estimate the map parameters from which the chaotic signals result.

The two methods, Gauss-Newton and Extended Kalman Filter (EKF), are considered to estimate the map parameters knowing only sequences generated by this map. First, the sequences generated by chaotic maps are used. Then, an index shift of sequence terms is made so that no transmission of consecutive terms occurs and the complexity in estimation of parameter values is increased.

Various two-dimensional chaotic maps are tested in exactly the same conditions with the Gauss-Newton method and the EKF method.

For all the maps and for various values of the parameters, the error of estimated parameters is studied in terms of the initial error on the parameters. We show that for low initial precisions and for an index shift below five, we obtain estimated parameters that enable the transmitted sequence to be returned. We can see that the magnitude of error on the estimated parameters is that of the transmitted sequence. The impact of the shift value is then studied for all the maps, by gradually increasing it for various parameter values, initial error on the parameters and initial conditions until the algorithm diverges. The absolute error related to the estimated parameters obtained (i.e. the absolute discrepancy between the result and the exact value of parameters) is analyzed. We obtain a maximum shift, different in each case, from which it is not possible to estimate the parameters.

In most cases, the Gauss-Newton algorithm converges for a range of values of the maximum shift higher than the EKF method. In many cases, the Gauss Newton method seems to be more robust and efficient than the EKF method. However, we are continuing our studies to improve the EKF method.

Comparative tests of the Gauss-Newton method between our program in Matlab and the one using the predefined Matlab function (`lsqnonlin`) have been done. This algorithm has the advantage of using the Levenberg-Marquardt method in the case of ill-conditioned problems. Although the results provided by both programs are of the same order of magnitude, the estimated parameters with our program are more accurates and the value of maximum shift obtained is generally higher.

With the Gauss-Newton method, we have also done tests on the impact of the number of observations on the estimated parameters precision and the maximum shift. We gradually increase the number of observations and we show that the maximum shift decreases strongly. Accumulated rounding errors in calculations appear to cause a loss of accuracy on the estimated parameters and consequently a more rapid divergence.

Références

- [1] V. GUGLIELMI, H. POONITH, D. FOURNIER-PRUNARET, A.TAHA, *Security performances of a chaotic cryptosystem*, IEEE ISIE'04, 2004.
- [2] D. P. BERTSEKAS, *Incremental least squares methods and the Extended Kalman Filter*, IEEE Conference on Decision and Control, 1994.