A fast and robust chaos-based cryptosystem for transmitted data

Safwan EL ASSAD, Hassan NOURA, & Daniel CARAGATA

École d'ingénieurs de l'université de Nantes Site de la Chantrerie -Rue Christian Pauc B.P 50609 - 44306 NANTES CEDEX 3 - France
safwan.elassad@univ-nantes.fr

In this paper, a fast and robust chaos-based image encryption/decryption system is presented. The proposed cryptosystem includes a new perturbed chaotic generator using 32-bits finite precision with integer representation to facilitate hardware implementation and uses a variable block cipher length with different modes. The proposed chaotic generator is composed of two nonlinear digital IIR filters, connected in parallel. The non linear function used is the integer skew tent map. In the block encryption/decryption algorithms, a 2D cat-map with chaotic control parameters is used to shuffle the image pixel positions. Then, multiple rounds of substitution (confusion) and permutation (diffusion) operations, based on two of the proposed chaotic generators, are performed on every block. The perturbing orbit technique improves the dynamical statistical properties of generated chaotic sequences. This technique increases also the orbit cycle length. The problem of error propagation in various cipher block modes: Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter mode (CTR) is presented. The dependence between input and output error probability of the modes is studied. The obtained simulation results demonstrate that the proposed cryptosystem including OFB, or CTR modes, is suitable to transmit encrypted data over a corrupted digital channel. To quantify the security level of the proposed cryptosystem, we analyze the global dynamical properties of the chaotic generator using the NIST (National Institute of Standards and Technology) test, and we show that, the algorithm can resist the statistical and differential attacks; it also passed the key sensitivity test. Moreover, the algorithm has a large key space. The experimental results indicate that the scheme is secure, efficient, and faster than conventional advanced encryption standard (AES).

Keywords : Chaos-based Crypto-system, chaotic generator, chaotic permutation, Security analysis

References C. Vladeanu, S. El Assad, J-C. Carlach, R. Quere. "Chaotic digital encoding for trellis-coded modulation", IEEE Trans on Circuits and Systems II, Vol. 56, No. 6, June 2009, pp. 509-513. Impact factor: 1.436 S. El Assad, H. Noura, I. Taralova. "Design and analyses of efficient chaotic generators for crypto-systems", Advances in Electrical and Electronics Engineering- IAENG Special Edition of the World Congress on Engineering and Computer Science 2008, vol. I, pp. 3-12, ISBN: 978-0-7695-3555-5. H. Noura, S. Henaf, I. Taralova, S. El Assad. "Efficient Cascaded 1-D and 2-D Chaotic Generators", 2nd IFAC conference on analysis and control of chaotic systems, TB2 Communication, London, UK, June 2009, 6 pages. A. Awad, S. El Assad, D. Carragata. "A Robust Cryptosystem Based Chaos for Secure Data", IEEE, ISIVC Conference On, Image/Video Communications over fixed and mobile networks, Bilbao Spain, July 2008, 4 pages.