Encrypting images with chaos

4 June 2020, by David Bradley

Standard "Lenna" test image and how a chaotically encrypted version looks. Credit: University Batna

Research published in the *International Journal of Information and Computer Security* details a way to encode an image using a chaotic cryptosystem that makes it harder for someone to illicitly break the encryption by boosting the size of the key space to 180 bits. The system, its authors write, is both robust and highly efficient based on their key space, statistical, and sensitivity analyses.

Assia Merzoug of the Laboratory of Coding and Security of Information at the University Batna and Adda Ali-Pacha and Naima Hadj-Said of the Laboratory of Coding and Security of Information at the University of Oran of Sciences and Technology in Algeria, explain how information security is primarily based on calculation algorithms. The level of security depends on the number of binary digits, bits, used by the system to define the cryptographic key that is employed by legitimate users to unlock the encryption. Too few bits in the key make it easier for a third party to crack the code. Conversely, if the key is too complex, i.e. a very high number of bits then it will require a lot of computer power from legitimate users on both sides to encrypt and decrypt the information.

One way around this need for inordinate computer resources for simple encryption might involve exploiting chaos theory, so that a complex key coding the information with an adequate number of bits might be generated that is difficult to crack. The team has brought together the Hénon attractor and a logistics map from chaos theory to construction their cryptosystem.

The chaotic data can be spliced into a normal image file to produce an encrypted image that will be very difficult to crack. Indeed, the test image once encrypted looks like simple noise to the casual observed with a flat histogram of pixel values. The whole process uses a very low level of computing resources but nevertheless produces an encrypted image this is very difficult to crack with a bruteforce attack.

More information: Assia Merzoug et al. New chaotic cryptosystem for the image encryption, *International Journal of Information and Computer Security* (2020). DOI: 10.1504/IJICS.2020.107452

Provided by Inderscience

APA citation: Encrypting images with chaos (2020, June 4) retrieved 16 January 2022 from https://techxplore.com/news/2020-06-encrypting-images-chaos.html