Encrypting images chaotically

August 13 2020, by David Bradley

Credit: CC0 Public Domain

An artificial neural network approach to image encryption offers many advantages over conventional encryption methods suggests a review published in the *International Journal of Services Operations and Informatics*. Shaimaa Abbas Fahdel Al-Abaidy of the University of Baghdad in Iraq explains that exploiting what is colloquially known as the "butterfly effect" in chaos theory can be even more effective.

Mobile computing and communications devices are almost ubiquitous now. We rely heavily on mobile phones, tablets, laptops, smartwatches, fitness trackers, smart TVs, and other such devices. They almost all rely on being constantly connected with the internet either through a cellphone network or via Wi-Fi for their many different functions. However, the transfer of data to and from such devices can often be vulnerable to third-party intrusion.

There are some instances where this is not particularly problematic, but there are other cases, such as sharing personal images where the sender and recipient, a student and educator, patient and doctor, employee and executive, may not wish other people to have access to those images. This is where encryption becomes a critical part of the communication.

There are many different approaches to encryption some are very secure but have high overheads, particularly when the files being encrypted are themselves relatively large, such as is the case with high-resolution photographs, for instance. Encryption needs to be smoother, faster, and preclude overpowering the encrypting and decrypting device as well as not adding to the data transfer costs in terms of the connecting network capacity.

The new approach discussed by Al-Abaidy offers protection against the integrity of the encrypted and decrypted image file and protection

against common attacks such as a cipher attack, plaintext attack, and brute force attack.

More information: Artificial neural network based image encryption technique, *Int. J. Services Operations and Informatics*, Vol. 10, No. 3, pp.181–189.

Provided by Inderscience