Color image encryption using an improved version of stream cipher and chaos

September 16 2022, by David Bradley

Credit: Pixabay/CC0 Public Domain

Chaos theory can be used to encrypt, with computational efficiency, a color image, according to work published in the *International Journal of*

Ad Hoc and Ubiquitous Computing. The non-linear approach described performs far better than conventional encryption algorithms for such digital assets.

Subhrajyoti Deb of the ICFAI University Tripura, Bubu Bhuyan of North-Eastern Hill University in Shillong, Nirmalya Kar of the National Institute of Technology in Agartala, K. Sudheer Reddy of Anurag University, in Hyderabad, India, explain how strong encryption is essential for a wide range of digital assets, not least color images. Traditional encryption tools can treat a file that encodes for a color image as if it were a text document but that approach is very inefficient given the different qualities of a displayed image when compared with a text document.

As such, there is considerable waste in terms of time and computing resources when encrypting an image using encryption algorithms designed to encrypt text. Moreover, such an approach, not being optimized for an image also makes them susceptible to decryption by a third party because of the characteristics of the encrypted file, wherein it might contain excessive redundancy because of long strings with the same pixel values. Various researchers have suggested alternative approaches such as using chaos theory, cellular automata, or quantum theory, to make encryption of images more efficient and less prone to attack. Fundamentally, there is a need to randomize the pixels encoded by the image file in a reversible way that is efficient and next-to-impossible to breach without the encryption key.

The team has used a modified version of the Grain-128 cipher to address the issues facing those who need to encrypt color images. The result is an encrypted file that has a satisfactory key space, low correlation and high randomness. The encrypted image has the appearance of random, color noise when displayed on a screen. Overall, the improvements over traditional text encryption approaches gives the team an efficient and

essentially uncrackable encrypted file that cannot be breached using standard occlusion, rotation, and noise attacks.

More information: Nirmalya Kar et al, Color image encryption using an improved version of stream cipher and chaos, *International Journal of Ad Hoc and Ubiquitous Computing* (2022). DOI: 10.1504/IJAHUC.2022.10045645

Provided by Inderscience