

Encrypting medical photos with chaos

12 October 2016

Chaos and confusion could be used to encrypt colour photos and protect them from prying eyes, according to computer scientists in Algeria. Writing in the *International Journal of Information and Computer Security*, the team describe a new algorithm that generates pseudo-random sequences that change a plain image into a ciphered image in a single step leading to a file that cannot be cracked.

Provided by Inderscience

Assia Beloucif, Oussama Noui and Lemnouar Noui of the University of Batna, explain how increasing concerns about personal data and privacy, particularly in medicine and other sensitive areas mean there is a growing need for easy to implement but tough to crack [encryption technology](#) that can protect images, such as medical scans, business plans, even just family snapshots. There are already powerful encryption tools for converting text documents but these are not the best choice for colour photos because there is a strong correlation between the data in the original image and an encrypted one, particularly in terms of bulk data volume.

As such, the team explains [encryption techniques](#) that exploit confusion or diffusion can remove redundancies to reduce file sizes and spread pixel values so that it becomes more difficult to extract parts of the original image using data recovery and cracking tools. In addition, there is the potential of using chaos theory to further blur the correlation between original and encrypted image. Their algorithm uses a chain of "tweaks" that are spread randomly from pixel to pixel in the conversion by the [encryption key](#). This approach, the team reports, beats other image encryption approaches in tests despite only requiring this single process to convert the original into an encrypted image.

More information: Design of a tweakable image encryption algorithm using chaos based schema.

[DOI: 10.1504/IJICS.2016.079183](https://doi.org/10.1504/IJICS.2016.079183)

APA citation: Encrypting medical photos with chaos (2016, October 12) retrieved 21 January 2021 from <https://phys.org/news/2016-10-encrypting-medical-photos-chaos.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.