

Digital watermarking to prevent fraud: From medical images to fake news

June 27 2024, by Laura Rodríguez



Credit: CC0 Public Domain

We expose ourselves to data manipulation every time we send information over the internet. A recent study led by researcher Tanya Koohpayeh Araghi from the Interdisciplinary Internet Institute (IN3) of

the Universitat Oberta de Catalunya (UOC) has developed a new tool to protect digital data in a secure and cost-effective way.

The study focuses on medical images and offers significant advances in protection through an innovative technique involving digital watermarking, a kind of imperceptible digital watermark and a [digital signature](#) embedded in these files. Applications range from medical images -X-rays, CT scans, MRI-, and telemedicine reports to protect [multimedia content](#) in order to prevent the spread of fake news.

The new method, [published](#) in [open access](#) in *Multimedia Tools and Applications*, combines two [mathematical techniques](#) commonly used to create digital watermarks: discrete wavelet transform (DWT) and singular value decomposition (SVD). It also tests the effects of a deeper level of SVD, as if performing a second decomposition. This makes it easier to create digital watermarks that are highly resistant to filtering, [digital signal processing](#) and geometric attacks.

Preventing medical data tampering

"Our research is all about developing improved digital watermarking techniques," explained Koohpayeh, a researcher in the K-ryptography and Information Security for Open Networks (KISON) group. "They not only improve imperceptibility and robustness, but also reduce the computational burden, making them more efficient and accessible."

These results, which the researchers tested on medical images, are particularly relevant.

Whenever doctors use the internet to transfer images or make diagnoses, the data are vulnerable to attack. Therefore, some form of protection must be in place to ensure the accuracy and confidentiality of the images. "Digital watermarks need to be embedded in all types of [medical](#)

[images](#), whether they are X-rays, CT scans or MRIs," said Koohpayeh. "This is how we guarantee the authenticity and integrity of health data.

A tool to combat fake news

Watermarking and digital security tools have numerous other use cases, such as protecting devices connected to the internet of things, securing cryptocurrency transactions and preventing the spread of fake news.

It is the fight against misinformation where Koohpayeh and her team are now focusing their efforts. Their goal is to provide techniques for tracing fake news to its source, identifying legitimate information and detecting manipulation.

"It's important for the public to understand the risks of fake news, as the slightest manipulations in images or videos can have serious consequences on [public perception](#) and decision-making," Koohpayeh said.

Koohpayeh and her team's research is currently focused on video and images, but could be applied to other media. It also uses tools such as blockchain and [artificial intelligence](#) to detect the subtlest of fakes.

However, digital watermarking remains their main area of research. By embedding imperceptible information into content without adding a large computational burden, their solution offers a versatile tool. Robust watermarks can be used to identify the origin of content (for example, if it is from a trusted media outlet), while fragile and semi-fragile watermarks are effective in detecting any kind of tampering (for example, retouching in an official photograph).

Taking heed of our digital vulnerability

At a time when deepfakes (an artificial intelligence technique used to create fake videos of people that appear to be real) and other spurious content have taken hold in the digital world, the public also needs to be made aware of the importance of these tools to protect their own well-being. Our images and data are increasingly vulnerable, even if we don't realize it.

Koohpayeh said, "It's important for the public to understand the risks of sharing images online and to take steps to protect their own information. By recognizing the importance of verifying the authenticity of digital content, we can work together to combat misinformation and protect the integrity of information online."

More information: Tanya Koohpayeh Araghi et al, Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking, *Multimedia Tools and Applications* (2023). [DOI: 10.1007/s11042-023-15554-z](https://doi.org/10.1007/s11042-023-15554-z)

Provided by Open University of Catalonia

Citation: Digital watermarking to prevent fraud: From medical images to fake news (2024, June 27) retrieved 10 September 2024 from <https://techxplore.com/news/2024-06-digital-watermarking-fraud-medical-images.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.