Holograms detect digital fraud

July 5 2005

A new technique for detecting forged photographs will help newspapers and magazines check celebrity pictures that might have been doctored to make them more newsworthy, and prevent hackers from tampering with sensitive legal images including fingerprint records and medical scans used as evidence in court.

Defence agencies could also use the technique to verify the source of secret military reports, and to protect satellite images, such as aerial photographs of the Iraqi desert, from manipulation.

Developed by physicists Professor Giuseppe Schirripa Spagnolo, Carla Simonetti and Lorenzo Cozzella from the University of Roma Tre in Rome, Italy, this research was published on 21st of June in the latest issue of the Institute of Physics journal, *Journal of Optics A*.

In their system, an image, e.g. a company logo, is added to a digital photograph as an invisible “watermark”. Any subsequent attempt to alter the content of the photograph also results in damage to the watermark. Forgery can then be detected by using a computer to extract the watermark and check it for damage. In a forged picture, it can even identify the object or section which has been tampered with.

The team had to ensure that only an authorised recipient can extract the watermark, which could otherwise be added to a fraudulent image to pass it off as genuine. To counter this problem the watermark is encrypted before adding it to the image, so that only someone who knows the private key can reconstruct it. Furthermore, the encryption

makes it difficult to detect whether an image has been watermarked or not.

Before it is added to the photograph the encrypted mark is turned into a computer generated hologram (CGH). This is a simulation of the pattern of light waves that is recorded when a real hologram is made. As with all holograms, a small part of the CGH contains enough information to recreate the entire image. This means that only a small part of the watermarked image is needed to extract the watermark.

When the CGH is added to the image it replaces the image “noise”, which has been filtered out beforehand. Noise is random, high-frequency information that doesn’t contribute to the image that you see, and can be removed without damaging the picture. The CGH watermark information is in the same high-frequency band as the noise, so it is invisible to the human eye when added to the photograph.

The watermark is now embedded in the digital image file, in a separate part of the spectrum to the picture information, making it easy for the recipient to isolate and extract it. If the watermark can’t be reconstructed using the private key it means that someone has destroyed the watermark by trying to modify the image.

Testing their technique, the team demonstrated how a hologram watermark can be used to find out which part of an image has been tampered with. They changed colours in certain areas of a watermarked image and divided it into 16 parts, extracting a watermark from each. The parts where the colour change had taken place showed a significantly damaged watermark indicating that they had been modified.

“We hope that this technique can be used to improve the reliability of photographs in the media” said Dr Lorenzo Cozella, co-author of the

paper, “Digital cameras could be developed so that an invisible watermark is added when a picture is taken. A newspaper buying a photo from a freelancer could then check for a watermark to confirm that it hasn’t been tampered with to make it more newsworthy.”

The system could also protect databases of images that serve as evidence in court, for example fingerprint records or medical scans, which could be used in cases of alleged malpractice. All images in the database would be watermarked so they could be checked without having to refer to the original hard-copy. This would be especially useful for electronically stored information exposed to external users via the internet, increasing its vulnerability to fraud.

Source: Institute of Physics