Editorial

Special Issue on Image security: secure imaging—is it necessary?

In the mathematical model of Shannon, "the fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point". The pioneering papers of Shannon described also cryptographic coding for ensuring confidentiality. Efficient, confidential, authentic and reliable coding of digital sources is nowadays an issue for which a number of solutions exist both in multimedia communications and contents delivery. However a media is not always used in its digital representation. For example, in the case of image communication, the source is at the endpoint transformed into light through a display mechanism. The ultimate question arises: how can one ensure security of an image transformed into light?

One solution would be to link intimately the image with a mark tracing the path of its distribution. Such a mark would be a trace of the process indicating the validity or integrity of a visual content but also revealing the source of illegal manipulation or re-distribution. The ideal mark should be invisible and not erasable. These are the well-known requirements for watermarking. Some security requirements are passive (unremovable and invisible traces in the visual contents), and some more active (watermarks for copy control). The conclusions of the secure digital music initiative (SDMI) have shown the major difficulties in an active watermarking approach. But on the other hand, long years of practice have shown the usefulness of watermarks for protecting printed documents against forgery. Even, if the domain still needs improvements, sole cryptography is not useful to protect the light from a displayed image. One can then explore the use of alternatives such as watermarks for that purpose.

This special issue has gathered five papers which have been initially discussed during the special sessions of the SPIE Annual Meeting on Imaging Security in 2001 and 2002. They cover hot topics in this field and are constituting one step among many others to recent progresses in image security and watermarking.

The two first papers are complementary overview papers. The first, co-authored by A. Eskicioglu, J. Town and E. Delp, reviews the mechanisms to be deployed for securing the delivery of multimedia contents. The second, co-authored by G. Doërr and J.-L. Dugelay, provides a guided tour of potential usages of watermarking in video.

The third paper, from S. Pateux and G. Le Guelvouit, is a contribution to a better mathematical modelling of spread-spectrum watermarking techniques in the light of the information theory. The watermarking is viewed, as proposed by P. Moulin, as a game between desired robustness and accepted distortion.

The fourth paper presents an original contribution to make watermark decoding resistant against geometric attacks. Such attacks are among the most efficient ways to attempt to flaw watermark decoding.

The last paper presents an original contribution to the watermarking of 3-D meshes. The contribution relies on new spectral decomposition of meshes based on overlapped patches.

This issue reflects examples of ongoing research in this field and illustrates new usages of such technologies, demonstrating an emerging maturity of imaging security.

Touradj Ebrahimi[a]
[a] *Ecole Polytechnique Fédérale de Lausanne,*
Switzerland
E-mail address: Ebrahimi@epfl.ch

Benoit Macq[b]
[b] *Université catholique de Louvain,*
Belgium
E-mail address: macq@tele.ucl.ac.be