## Une équipe de l'EPFL a mis au point une signature numérique infalsifiable

Ce procédé révolutionnaire permet ainsi à l'auteur d'images fixes ou vidéo de faire valoir ses droits.

I ly a quelques années, un industriel est venu consulter le Laboratoire de traitement des signaux (LTS) du professeur Murat Kunt à l'EPFL afin de mettre au point un système empêchant la reproduction d'un document, par exemple un billet de banque, à l'aide d'une photo-

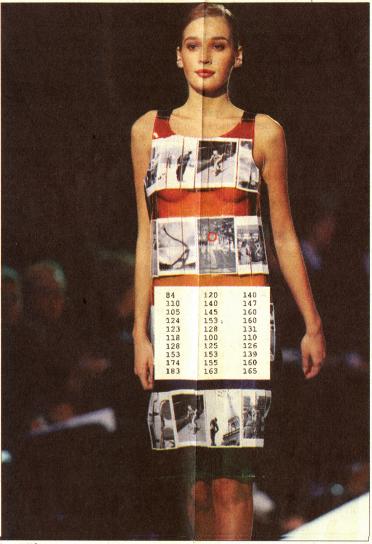


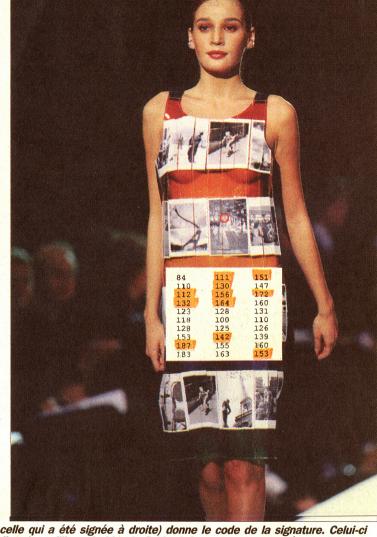
PAR Nicolas WILLEMIN

copieuse numérique couleur. «On a ainsi pu déposer un brevet, mais notre système n'est pas utilisé, explique le professeur Kunt. Sur les billets de banque figure en effet désormais un hologramme qui empêche déjà toute photocopie. Mais grâce à ce travail, nous avons commencé à travailler dans le domaine de la signature numérique des images.»

Avec le développement d'Internet, ce domaine est devenu très important: comment protéger les droits d'auteurs pour toutes les images présentes sur les dizaines de milliers de serveurs aujourd'hui disponibles sur le Web? L'équipe de Murat Kunt et de son premier assistant Touradj Ebrahimi a ainsi réussi à cacher une signature de l'auteur dans une image en modifiant la valeur d'une couleur numérique (qui va de 0, le noir, à 255, le blanc) en un point précis de l'image. Le système travaille dans le bleu, la couleur la plus courante, mais la modification est invisible à l'œil nu. Ce programme, disponible sur le serveur Web du LTS, a été mis au point par les assistants Frédéric Jordan et Martin Kutter. Son nom, JK-PGS; JK pour ses auteurs et PGS pour «Pretty Good Signature»

La signature, qui se répète plusieurs milliers de fois dans l'image, ne peut pas être modifiée, même si l'on soumet l'image à plusieurs retraitements graphiques. L'algorithme de codage est en effet extrêmement complexe, d'où la robustesse de la signature. L'équipe du LTS a même réussi à retrouver la signature dans une image scannée, puis imprimée. Ce système permet plusieurs applications: définir l'auteur d'une image (watermarking), voir si le document n'a pas été intercepté





La différence des chiffres entre les deux images (l'originale à gauche et celle qui a été signée à droite) donne le code de la signature. Celui-ci n'est en effet pas visible à l'œil nu. Il ne consiste qu'en une modification d'un des millions de bits du fichier informatique que représente l'image.

et modifié (hashing), découvrir si quelqu'un a copié le document (fingerprinting).

## Images fixes ou vidéo

Le procédé développé par l'équipe lausannoise peut être utilisé pour des images fixes ou pour des films vidéo (qui ne sont qu'une succession d'images fixes). Il ne sert pas uniquement à prouver les droits d'auteur d'un document dans le cas d'une utilisation abusive ou malhonnête. Dans ce cas-là, le propriétaire des droits est le seul à connaître la clé informatique qui fera apparaître la signature. On peut également l'employer pour signer une image et permettre ainsi, à tout un chacun qui disposerait du programme de reconnaissance ad hoc de la voir. Là, la clé informatique sera puIl ne faut pas en effet croire que tous ceux qui «captent» des images sur Internet ont de mauvaises intentions. Certains aimeraient ainsi bien savoir à qui appartiennent les droits d'un document. Une signature publique leur simplifierait bien la tâche.

N. W. [

La première version du programme JK-PGS (pour stations de travail) est disponible sur le Web du LTS à l'adresse http://ltswww.epfl.ch/jordan/watermarking.html. Une version Windows NT sera prévue pour bientôt.

## Spécialiste de la télévision numérique

e Laboratoire de traitement des signaux (LTS) de l'EPFL, un des plus importants de la haute école lausannoise, a acquis, sous la direction du professeur Kunt, une renommée internationale dans les domaine des images numériques. Télévision haute définition, compression numérique, contrôle d'accès, signature numérique, les différents domaines étudiés serviront bientôt à la plupart des consommateurs. Les travaux du

LTS seront ainsi utilisés pour la mise au point de la future norme mondiale du multimédia MPEG-4. Cette norme, qui sera opérationnelle en 1998, servira à de nombreuses applications grand public d'ici à l'an 2000. Economiquement, entre le marché de la télévision numérique et celui d'Internet, les enjeux sont considérables. Le professeur Kunt et son équipe travaille également sur la nouvelle JPEG 2000, qui touche les images

fixes. Il s'occupe aussi de réalité virtuelle et d'imagerie en trois et même en quatre dimensions.

Mais le LTS ne travaille pas uniquement pour le multimédia. Dans le domaine médical, il collabore également, en matière de traitement des signaux, avec le CHUV, et, plus récemment, avec la firme américaine Medtronic, le fabricant de pacemakers qui vient de s'installer dans le canton de Vaud.

N. W. □