

## Le watermarking trouve ses marques

### Un espion indétectable

Le principe de cette technologie de tatouage numérique est de rajouter dans un contenu audio et vidéo une marque invisible et inaudible qui puisse être identifiée ultérieurement. Une des fonctionnalités associées consiste à lutter contre le piratage : identifier la source à partir de laquelle a été copié un contenu est en effet devenu primordial pour les majors et autres éditeurs de contenus.

Rappelons que l'une des principales sources de piratage des studios est la duplication des films directement dans les salles de cinéma avec l'aide de caméras numériques. Ces contenus sont ensuite distribués parallèlement sur des DVDs ou sur Internet. Dans ce contexte, le Watermarking, qui rajoute une marque spécifique pour chaque salle de cinéma, permet de remonter à la salle responsable de la fuite.

Jusqu'à présent, les solutions de WaterMarking étaient utilisées essentiellement dans des solutions 'Business to Business', c'est-à-dire pour la protection des échanges entre professionnels. Aujourd'hui elles se démocratisent.

### Le terminal numérique : la nouvelle cache

Les nouvelles technologies dont disposent les équipements de l'électronique grand public permettent depuis quelques années de réaliser des enregistrements, voire de les distribuer (soit par des sorties adaptées, de type USB, soit par des dispositifs de gravage directement intégrés). Si les technologies d'Accès Conditionnel sont particulièrement bien adaptées pour protéger le contenu en 'live', il n'en est pas de même pour les contenus persistants, pour lesquels de nouvelles solutions de type DRM sont mises en œuvre.

Or au-delà des protections DRM qui empêchent la copie par exemple, la

solution complémentaire consiste à utiliser les technologies de WaterMarking dans les terminaux numériques. Cette fois, l'idée est d'insérer, à la volée et en temps réel, une marque dans le contenu décodé. Toutes les sorties possibles du terminal numérique (analogique ou numérique, y compris les moyens de stockage) véhiculeront ainsi le contenu auquel est rajouté cette marque. Et cette fois, la marque permet d'identifier sans ambiguïté le numéro du terminal ou de la carte à puce de l'abonné.

Dans le cas où ce contenu marqué serait retrouvé par la suite sur Internet ou sur le marché parallèle des DVDs, ces outils permettraient de retrouver la marque, et remonter ainsi à la source de la fuite afin de mener éventuellement des actions judiciaires.

tionnel avec le Watermarking proposé par Thomson Security. La démonstration que nous avons vue sur le stand de Thomson Security reprenait justement la solution intégrée avec Viaccess. Dans ce cadre, c'est un identifiant contenu dans la Carte à Puce de l'abonné qui est marqué dans le contenu. Verimatrix, en toute logique, intègre directement sa solution de Watermarking avec sa propre solution d'Accès Conditionnel.

En somme, le WaterMarking, qui peut être également utilisé sans Accès Conditionnel pour des contenus non embrouillés et non protégés par Accès Conditionnel, s'introduit partout.

### Certes, mais quelles performances pour ces solutions ?

Sur un salon, il est peu aisé de tester la

## Les méthodes du Watermarking

La stéganographie, largement utilisée pour le Watermarking, est l'art de cacher un message dans un document au contenu visiblement anodin, de façon à ce que le message reste secret.

De nombreuses anecdotes historiques illustrent cette technique, comme les encres invisibles. Au

IV<sup>ème</sup> siècle av JC, Hérodote raconte qu'à la cour de Perse, un certain Histiée, qui voulait communiquer avec son gendre le tyran Aritagoras de Millet, choisit un serviteur dévoué, lui rasa le crâne et y tatoua son message. Puis il attendit la repousse de ses cheveux avant de l'envoyer avec instruction de se raser une fois présenté à Aristogoras.

### A vos marques !

Thomson Security, Cinea (société du groupe Dolby) ou encore Philips présentent leur solution de Watermarking intégrée directement dans les chipsets des terminaux numériques. Thomson est pour le moment intégré avec ST, Philips avec ST, Broadcom et Texas Instruments. Verimatrix intègre sa propre technologie directement dans les chipsets. Mais que font les fournisseurs d'Accès Conditionnel ?

Viaccess et Irdeto annoncent l'intégration de leur technologie d'accès condi-

robustesse et la fiabilité des solutions présentées. Les grandes questions à se poser pour évaluer une solution de WaterMarking sont les suivantes :

- La marque est elle réellement invisible ou inaudible ?
- L'algorithme de mise en place de la marque est-il suffisamment sûr ?
- La marque ne peut-elle pas, par traitements successifs, être retirée du contenu ?

Autant de problématiques qui permettront de comparer les solutions utilisées et intégrées.