ELECTRONIQUE GRAND PUBLIC I Films, clips musicaux, matchs de foot... Copiés, les contenus vidéos se répandent sur internet dès leur diffusion. Un manque à gagner pour les ayants droit qui explorent plusieurs pistes pour protéger leurs programmes originaux. ■ LUC MATHIEU

Vidéos cherchent protections

Des sommes colossales en jeu

PLUS DE 6 MILLIARDS DE DOLLARS. C'est ce qu'a coûté le piratage aux principaux studios américains en 2005, selon la Motion Pictures Association of America.

A ELLE SEULE, LA DIFFUSION illégale de copies de films sur Internet représente un manque à gagner de **2,3 milliards de dollars**, contre 1,4 milliard pour la duplication de faux DVD.

Les studios américains rendront leur verdict d'ici à la fin juin. Depuis plusieurs mois, ils testent les dernières technologies pour repérer les copies illicites de leurs films qui circulent sur internet. Une douzaine de solutions, développées aussi bien par des grands groupes que par des start-up, sont examinées. «Les studios ne veulent pas subir le sort des maisons de disques, qui n'ont pas réussi à juguler le piratage», explique Jean-Luc Moullet, le vice-président de Thomson chargé des technologies.

Ils ne sont pas les seuls. Viacom, la maison mère de MTV, réclame un milliard de dollars à Google, propriétaire du site de partage de vidéos YouTube, pour «violation massive et intentionnelle des droits d'auteurs». Une preuve que les technologies de protection ne suffisent pas? Pas forcément. Car si aucun procédé ne peut garantir une sécurité parfaite, plusieurs permettent tout de même de limiter les risques.

Première piste, les technologies dites de DRM (Digital Right Management). Leur principe : le cryptage des contenus, accessibles seulement par ceux qui les auront payés. Le distributeur ou le possesseur des droits d'une vidéo, par exemple un studio ou une chaîne de télé, commence donc par la crypter à l'aide d'un algorithme dit AES (Advanced Encryption Standard), dont la clé compte 128 ou 256 bits. «C'est suffisamment long pour décourager une attaque brute, qui testerait toutes les combinaisons possibles», indique Jean-Luc Moullet.

Deuxième étape, la clé de cryptage de l'acheteur est elle-même... cryptée. Celui qui achète une vidéo sur internet est identifié et reçoit une nouvelle clé, d'une longueur minimale de 1024 bits qui décrypte la première. Autre particularité de ces solutions, telle celle de Microsoft, elles incluent les conditions d'utilisation des contenus acquis. «On peut, par exemple, fixer le nombre de copies autorisées une fois la vidéo achetée», explique Erwan Bigan, le directeur des technologies chez Viaccess.

UN SYSTÈME DE FILTRAGE

Pour autant, aucun système de cryptage n'est inviolable. Le système de protection des DVD a été cassé en 1999 par un Norvégien de seize ans. En outre, le DRM n'a d'intérêt que s'il est appliqué à la source, avant toute distribution. Ainsi un match de foot peut être enregistré lors de sa diffusion, copié et redistribué sur un site de partage tel YouTube. Dès lors, la chaîne de télé n'a d'autres recours que de scruter internet pour y repérer les vidéos frauduleuses. Un travail systématique impossible à mettre en œuvre. Sur le seul site YouTube, 65 000 nouvelles vidéos sont postées chaque jour. Seule solution : automatiser les recherches.

C'est précisément ce qu'autorisent les technologies «d'empreintes numériques» («fingerprinting», en anglais). A l'inverse des DRM, l'idée n'est pas de crypter un contenu mais de lui associer une signature qui l'identifiera. Plusieurs start-up, telles l'américaine Audible Magic et la française Advestigo, se sont lancées. Chaque solution fait l'objet de plusieurs dépôts de brevets, mais leur principe est similaire.

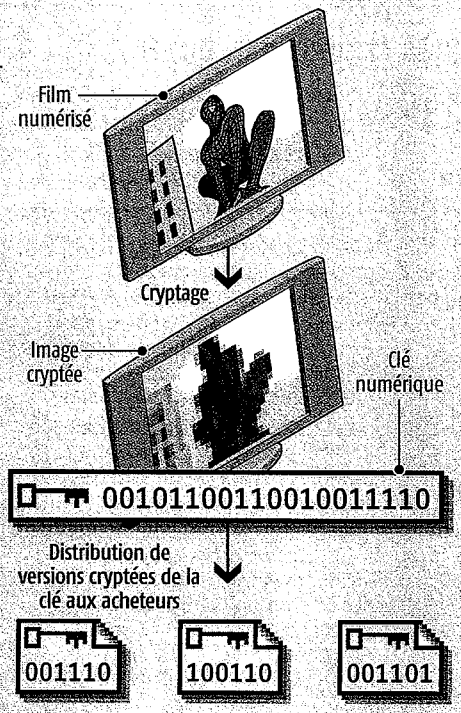
Il faut d'abord trouver des séquences de la vidéo qui constitueront sa signature. «On choisit des scènes signifiantes, avec des images qui changent brutalement. Par exemple, une séquence où un personnage nouveau apparaît d'un seul coup», explique Christophe Tilmont, le vice-président marketing d'Advestigo. Pour un film de 90 minutes, entre 200 et 2 000 séquences clés seront extraites. Ensuite, codées et mises bout à bout, elles formeront une empreinte d'environ un mégaoctet.

ÉGALEMENT DANS CETTE PARTIE
56 | La cellule solaire prend de la hauteur
57 | La fonderie à modèle perdu s'affranchit du problème des inserts
58 | La semaine en bref

Trois technologies en lice

1 LE CRYPTAGE

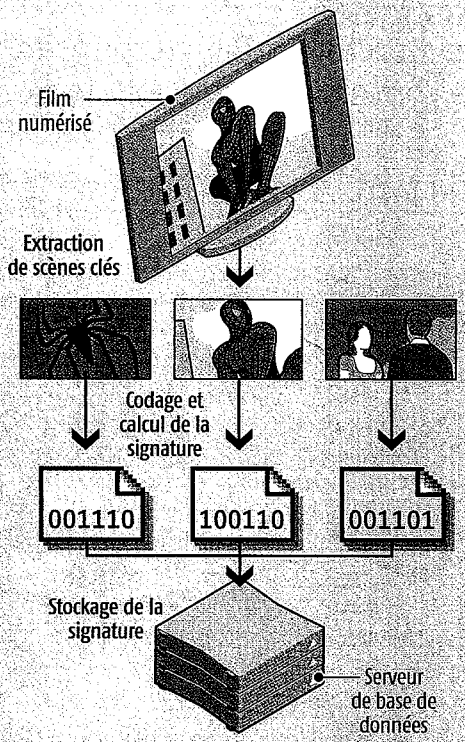
Chaque acheteur se voit confier une clé unique. Seule celle-ci lui permettra de décoder la clé qui a servi à crypter la vidéo.



AVANTAGE	INCONVÉNIENT
Contenu protégé.	Ne permet pas de trouver l'origine du piratage.

2 L'EMPREINTE NUMÉRIQUE

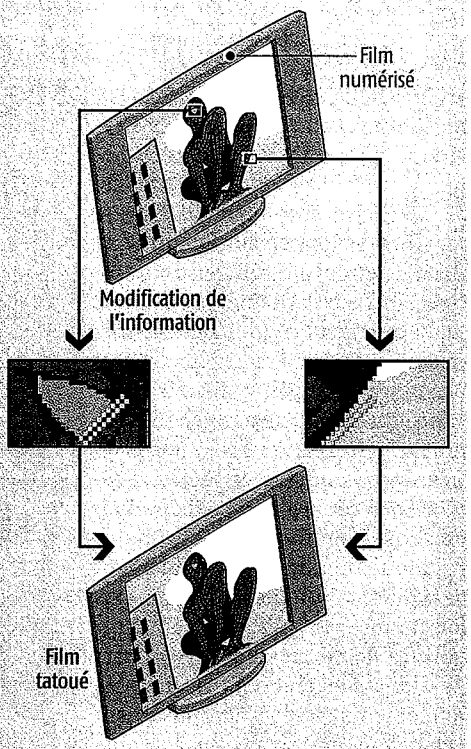
Pour déterminer si une vidéo circulant sur internet lui appartient, un studio peut calculer sa signature et vérifier si elle figure dans sa base de données.



AVANTAGE	INCONVÉNIENT
S'applique à n'importe quelle vidéo en circulation.	Ne protège pas la vidéo elle-même.

3 LE TATOUAGE

En appliquant un tatouage différent à chaque copie d'un film, un studio peut, par exemple, déterminer dans quelle salle il a été piraté.



AVANTAGE	INCONVÉNIENT
Permet de retrouver l'origine de la fraude.	Doit être appliqué avant diffusion.

Les studios, chaînes de télévision et autres producteurs peuvent ainsi se constituer des bases de données regroupant les signatures de leurs œuvres. De leur côté, les sites de partage peuvent calculer les empreintes des vidéos reçues et vérifier qu'elles ne figurent pas dans ces bases. Dans le cas contraire, le clip peut être refusé et l'ayant droit prévenu. Un filtrage que le site Dailymotion mettra en œuvre dans les prochains mois pour les fichiers musicaux.

Reste qu'en cas de détection de contenu piraté, le studio n'a aucun moyen de déterminer qui est à l'origine de la fraude. La vidéo envoyée sur YouTube peut provenir aussi bien d'une diffusion télé que d'un enregistrement réalisé dans un cinéma. La seule solution pour repérer son origine est de tatouer la vidéo avant sa diffusion. Développé notamment par Philips et Thomson, le «watermarking» revient à graver sur chaque copie d'un film un numéro de série unique. Si une copie illégale atterrit sur internet, il suffit de lire le tatouage pour déterminer sa provenance.

DES TATOUAGES DISSIMULÉS

Concrètement, les technologies de tatouage reposent sur un algorithme qui dissémine une série d'informations dans la vidéo elle-même. «L'idée est de cacher dans le signal vidéo des petits bouts de signaux quasiment imperceptibles», explique Henri Maître, professeur à Télécom Paris. Les derniers algorithmes, brevetés, dissimulent les tatouages dans des détails de l'image. «Cela peut avoir une incidence sur le contraste ou le placement de quelques cheveux d'un acteur», explique Henri Maître. Pour choisir un algorithme, les grands studios emploient des testeurs, dits «golden eyes» («yeux d'or»), qui scrutent des films tatoués et s'assurent que les défauts ajoutés ne sont pas visibles.

Séduites, les majors américaines réfléchissent à un moyen de coupler tatouage et cryptage. «Les deux technologies sont complémentaires, explique Erwan Bigan. La première permet de retrouver l'origine de la fraude. L'autre tente de la limiter.» Un double verrou qui fait office pour l'instant de protection quasi parfaite.