La stéganographie : une solution pour enrichir le contenu des vidéos numériques

François Merciol, Sébastien Lefèvre

Laboratoire VALORIA – équipe SEASIDE
IUT Vannes – département informatique
Université de Bretagne Sud
8, rue Montaigne, 56 000 Vannes

Francois.Merciol@univ-ubs.fr ; Sebastien.Lefevre@univ-ubs.fr ;

Sections de rattachement : 27,
Secteur : Secondaire

RÉSUMÉ. Après une présentation des concepts en sécurité de l'information, cet article montre par des illustrations que la stéganographie peut servir à la transmission d'informations non confidentielles. Nous présenterons ensuite quelques techniques stéganographiques adaptées au média vidéo. Dans ce contexte, la stéganographie présente l'avantage de conserver une compatibilité ascendante avec tous les lecteurs multimédia existants. Cependant nous montrerons que les solutions actuelles n'offrent pas une indépendance aux traitements pouvant être effectués sur les vidéos (telles les compressions).

MOTS-CLÉS : Stéganographie, Vidéo, Métadonnées embarquées, Compatibilité ascendante

1. Introduction : un potentiel profondément enraciné

La stéganographie est l'art d'incorporer une information (masquée) dans une autre (une couverture). L'élément incorporé de façon masquée doit être plus court que la couverture pour éviter de trop la détériorer. L'objectif est que l'attention soit captée par la couverture pour empêcher de remarquer, en première analyse, ce qui doit être masqué. Malheureusement, en cas d'analyse poussée, l'information masquée ne dispose d'aucune autre protection que sa discrétion : au contraire de la cryptographie dont l'objet est justement de rendre illisible une information.

Si l'on trouve des traces cryptographiques deux mille ans avant Jésus-Christ, celles de la stéganographie n'apparaissent qu'environ cinq cents ans avant Jésus-Christ (un écart comparable à l'ère chrétienne qui suivra !) [Singh 1999]. Son usage fut à l'origine motivé par la protection des informations du regard des tiers. Notons que cacher une

information ne peut se faire que sur des supports utilisés par le plus grand nombre : si les agents de renseignements ne communiquaient que via des systèmes spécifiques, ils seraient facilement repérés. L'information masquée a des vocations multiples puisqu'elle peut servir à nuire, à défendre voire à protéger. Initialement pratiquée dans un contexte guerrier, l'usage de la stéganographie s'est diversifié jusqu'aux échanges épistolaires privés. Par la suite, d'autres pratiques sont apparues, comme celle de chercher à masquer une information parfaitement connue de tous, mais qu'il est préférable de cacher dans un premier temps. C'est le cas lorsque l'on souhaite enrichir une technique sur laquelle un investissement lourd a été consacré. L'illustration la plus simple est celle du Télétexte, qui permet d'ajouter de l'écrit dans une transmission vidéo analogique sans modifier l'ensemble du parc de téléviseurs. Nous souhaitons exploiter et généraliser cette approche de diffusion d'informations non confidentielles par stéganographie.

Aujourd'hui, le média vidéo s'est imposé comme un des canaux majeurs d'information (cent millions de vidéos consultées par jour pour le seul opérateur YouTube). Régulièrement de nouveaux services apparaissent pour personnaliser et enrichir ce média. Dans ce contexte nous pensons que la stéganographie est un moyen naturel pour y parvenir. Cet article a plus précisément pour but d'illustrer la stéganographie comme moyen d'enrichissement de l'information et de dresser un panorama de ses mises en œuvre dans le domaine de la vidéo.

Pour ce faire, nous commencerons par rappeler un vocabulaire cryptographique (section 2), dans un univers par nature obscur. Nous présenterons des usages où, par essence même, l'information masquée n'est pas confidentielle (section 3). Nous énumèrerons quelques techniques stéganographiques dans le domaine vidéo (section 4). Puis nous conclurons en indiquant les pistes à suivre pour pouvoir enrichir le média vidéo à l'aide de la stéganographie

2. Riche et varié en concepts

Rappelons quelques notions pour éclaircir le paysage du traitement de l'information qui, d'ordinaire, cherche à demeurer ésotérique. Bien évidemment, ces notions s'appliquent à toute information quelle qu'en soit la nature : texte, son, image, vidéo, programme informatique … Nous devons clairement séparer le fait de rendre illisible une information (cryptographie) et celui d'ajouter une information nouvelle (stéganographie) à un support existant [Cheddad 2010] (cf figure 1).

Rendre illisible une information relève de la cryptographie (du grec *kruptos* : caché et *graphein* : écrire). Dans ce cas, il n'y a pas d'ajout d'information pertinente. Certains algorithmes cryptographiques peuvent introduire une perturbation (du bruit) et allonger artificiellement la taille des données. Ce faisant, ils cherchent à contrer une cryptanalyse[1] fondée sur l'analyse des fréquences. Cependant, nous savons [Singh 1999]

[1] Cryptanalyse : attaque visant à révéler le texte d'origine

que pour être efficace, il faut au contraire chercher à supprimer toutes formes de redondances. Les actions cryptographiques sont (cf tableau 2) :

- **chiffrer** : rendre obscur un texte clair à partir d'une clef (notre secret),
- **déchiffrer** : rendre clair un texte obscur à partir d'une clef (notre secret),
- **décrypter** : rendre clair un texte obscur sans connaître la clef (secret des autres),
- **forger** : fabriquer un message obscur alors que l'on n'est pas censé connaître la clef (secret des autres).

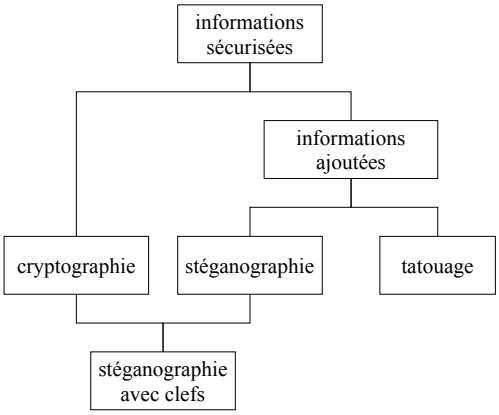

Figure 1 . *taxonomie*

	Rendre illisible	**Rendre lisible**
Propriétaire	Chiffrer	Déchiffrer
Usurpateur	Forger	Décrypter

Tableau 2 . *actions*

La cryptographie est souvent utilisée en complément de la stéganographie, mais nous ne décrirons pas ici les notions de clefs secrètes, ni de clefs publiques et privées [Menezes 2001].

A l'origine, seule la stéganographie servait à cacher des informations. De nos jours, il faut distinguer l'ajout d'informations masquées (la stéganographie) et l'ajout d'informations visibles (le tatouage). Ils ont toutefois en commun le fait de dégrader la couverture qu'ils exploitent.

Écartons le tatouage (ou marques d'eau, *watermark* en anglais) [Yamada 2010] trop visible. Il sert à ajouter une empreinte, une « signature » (comme l'incrustation en coin du logo d'une chaîne). Strictement parlant, ces marques détériorent visiblement la couverture. La « surface » détériorée n'est pas récupérable. L'inconvénient d'une telle approche est qu'il est aisé de supprimer ou remplacer le tatouage. Cependant, certains tatouages servent de preuve de droit de propriété et font intervenir des informations qui ne doivent pas être supprimées. En ce sens, ils rejoignent alors la stéganographie.

Enfin, la stéganographie (du grec *steganos* : couvrir, *graphein* : écrire) est la discipline qui nous intéresse. Nous en avons déjà donné une définition en introduction et rappelons que la stéganographie a essentiellement pour but de transmettre une information confidentielle.

Nous partons du principe que l'information est ajoutée en clair, car c'est le procédé qui est secret. La stricte stéganographie ne fait intervenir aucune clef. Ceci contrevient aux principes de Kerckhoffs [Singh 1999], qui veulent que : *la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef*. Nous pouvons dire qu'une technique cryptographique est par nature faible (ou non sûre). Toutefois, combiner stéganographie et cryptographie permet d'y ajouter de la sûreté.

Les procédés stéganographiques se distinguent par leurs capacités à résister à la stéganalyse[2]. On peut vouloir renforcer le caractère :

- enfoui dans une couverture (être indétectable),
- indélébile de la couverture (non effaçable).

Les besoins pouvant être contradictoires, il n'y a pas de procédé idéal. Si on utilise un canal de transmission (sûr mais non fiable) qui dégrade systématiquement la qualité de service par des compressions avec pertes et changements de formats, on préfèrera un procédé indélébile. Si on utilise un canal de transmission (fiable mais non sûr) de bonne qualité mais visible de tous, on souhaitera que les copies faites du message puissent être dégradées le plus rapidement possible.

3. Efficace même sans secret

Comme indiqué dans l'introduction, notre objectif est de montrer que la stéganographie permet également d'enrichir des informations numériques. Pour illustrer notre propos, nous présentons différents exemples :

- Celui du « passager clandestin », en utilisant un canal qui n'est pas prévu à cet effet. En 1850, pour envoyer une lettre, il fallait acquitter une taxe d'environ un shilling tous les cent miles (montant prohibitif pour la plupart des britanniques) [Singh 1999], alors même que l'envoi de journaux était dispensé de taxe. Il y avait donc une motivation financière à reprendre une technique consistant à piquer un journal avec une épingle sous les caractères du texte à rédiger, dans l'ordre de lecture du texte à transmettre. Il ne restait plus qu'à envoyer un journal et non une lettre.
- Celui de l'esthétisme. Ne pouvant supprimer une information légale, des fabricants préfèrent parfois en ajouter autour pour la noyer. Ainsi des fabricants avaient ajouté de la décoration à la bande verte désignant les

[2] Stéganalyse : attaque visant à révéler l'information masquée

produits dangereux. D'autres proposent aux producteurs de décorer les codes à barres de leurs produits[3]. La Poste a déposé un brevet [Merciol 2002] pour intégrer des informations numériques introduisant de nouveaux services postaux dans des timbres.

- Celui de contraindre, d'influencer ou manipuler nos comportements. Nous connaissons tous les images subliminales [Fullerton 2009] où l'information est banale : l'envie de consommer, d'opter pour des opinions politiques, ...
- Celui de pérenniser un investissement financier. Les postes de télévision intègrent un décodeur télétexte [Bailly 2007]. Même si l'information est publique, il s'agit bien de stéganographie puisque les informations sont introduites dans une couverture dont les caractéristiques techniques n'ont pas évolué. Le but est que les anciens postes ne disposant pas du décodeur continuent à fonctionner normalement.

4. Pour la vidéo, quelles techniques ?

Nous n'avons aucune prétention de fournir une liste exhaustive des procédés, même limitée à la vidéo. Notre but est ici de montrer la diversité des techniques existantes.

Un système stéganographique est généralement découpé en couches fonctionnelles [Wu 2003] (tableau 3). Pour ne pas entrer dans les détails et montrer la diversité des procédés, nous allons particulièrement nous intéresser aux couches inférieures d'enfouissement de chaque technique.

Couches supérieures	Compression et codage
	Sûreté
	Fiabilité (correction d'erreur)
	Homogénéité d'enfouissement
Couches inférieures	Plusieurs bits
	Un bit

Tableau 3 . *couches fonctionnelles*

Les images numériques sont apparues avant les vidéos et certains formats de vidéo (MPEG-2) s'appuient sur des formats d'images (JPEG). Il est donc naturel que des procédés stéganographiques vidéos reprennent historiquement ceux de l'image dans leurs principes. En fait, nous pouvons ajouter des informations dans tous les composants d'un flux vidéo compressé :

[3] http://www.d-barcode.com/

- les images, de grandes tailles servant à resynchroniser en cas d'erreur,
- les informations intermédiaires de déplacement de région de pixels,
- les informations intermédiaires de prédiction de modifications de pixels,
- les informations autres que visuelles (son, sous-titre, ...).

4.1. Modification d'images

Pour les images, la méthode la plus rapide et la plus discrète (pour nos yeux) est de manipuler les bits de poids faibles des pixels (LSB des pixels). Un pixel d'image (RGB) est souvent codé sur trois octets (24 bits) ce qui donne 16,8 millions de couleurs. Notre œil est loin de pouvoir distinguer deux couleurs adjacentes dans cette masse. Il est facile d'agir sur la parité des pixels pour coder des 0 et des 1. Par hasard, c'est la couleur bleu qui est concernée [Chastagnol 2009] (car située à droite de notre représentation numérique), mais les autres couleurs conviennent tout autant. Nous éviterons d'agir sur les 3 en même temps car cela implique d'autres perturbations (luminosité, contraste).

En théorie, en utilisant 1 bit par pixel, nous pourrions coder pour des images de 640x480 pixels : 307 200 bits, soit pour 25 images par seconde un débit utile de : 937,5 Ko par seconde. Mais cette limite ne peut être exploitée pour deux raisons :

- Al-Kindi [Singh 1999] nous a appris dès le 9e siècle, qu'il était possible de retrouver un message par analyse statistique. Il faut prendre garde que modifier un 24e des données (1 bits sur 24) aura une incidence statistique.
- Les nuances non significatives d'une image ne résistent pas aux algorithmes de compression avec perte, qui commenceront par les supprimer (puisque justement nous ne les voyons pas).

4.2. Modification de déplacement de pixels

Dans une vidéo, nous pouvons également utiliser des propriétés de mouvement qui dépendent du format de codage. Là où l'on utilisait les éléments les moins significatifs d'une image, ici, on utilisera ceux des vecteurs de déplacement de région de pixels entre deux images. Par exemple dans [Nguyen 2006], le schéma proposé dépend du format H.264 et sélectionne les vecteurs de mouvement (horizontal et vertical pour un bloc de pixels). Le procédé commence par éliminer les mouvements trop faibles ou les blocs qui disparaissent. Les mouvements sont indiqués en demi pixel. On arrondira au nombre pair ou impair en fonction du bit à coder (0 ou 1). Par exemple, au lieu d'un déplacement horizontal de 3,5 pixels, on appliquera un déplacement de 3 pixels ou de 4 pixels pour obtenir le codage d'un 0 ou d'un 1. Les images de resynchronisation ne sont

pas altérées pour que les dégradations ne se propagent pas. En revanche, les mécanismes de prédiction doivent être modifiés en cohérence.

4.3. Modification de prédiction de modification

C'est une approche symétrique de la précédente pour la sélection des zones où cacher des données. Elle a l'inconvénient d'être de nouveau dépendante du format vidéo. Pour réduire la redondance spatiale, le format H.264 met en place un calcul de prédiction du contenu des blocs de coefficients IT [Hu 2007]. Un drapeau (0 ou 1) est positionné pour indiquer qu'un bloc est correctement prédit. Suivant la texture d'une image (sa complexité), les drapeaux seront majoritairement à 0 (image complexe) ou à 1 (image unie). Une image complexe est un bon candidat pour l'enfouissement de l'information, alors qu'une image unie ferait apparaître des anomalies trop visibles.

4.4. Modification autre que visuelle

Enfin, dans un flux vidéo, il n'y a pas que des informations visuelles. Nous pouvons agir sur le son, les sous-titres, …. Comme pour la vision, nos sens sont limités. L'oreille humaine est incapable de percevoir des changements de phase dans le spectre sonore. Il ne reste plus qu'à définir un codage particulier. En représentant un signal sonore sous forme sinusoïdale, nous pouvons déphaser le signal (le plier au passage à l'axe) sans que nous puissions entendre une différence dans la modulation [Das 2008].

Toutes les combinaisons précédentes sont envisageables, y compris celles qui consisteraient à alterner les flux ou la nature des données servant à enfouir l'information.

5. Conclusion : une solution à améliorer

La stéganographie ajoute de l'information soit par augmentation de la taille de la couverture (la vidéo) soit en dégradant son contenu, avec dans les deux cas le risque de révéler la présence d'information cachée. Cet inconvénient disparaît dès lors que l'information cachée n'est plus confidentielle. La stéganographie semble donc une solution intéressante pour garantir une indépendance vis-à-vis des formats de codage et donc des lecteurs qui les supportent.

Cependant, les techniques présentées sont souvent liées à un format vidéo et utilisent les bits de poids faibles de différentes représentations, qui supportent mal les traitements (conversion, compression). Or, nous souhaitons un mécanisme indépendant des formats et de la compression. Il nous semble possible d'agir à un niveau d'abstraction suffisant

de représentation, pour nous affranchir des formats sous-jacents. Dans le cas d'ajout de métadonnées dans un flux vidéo, nous allons privilégier la fiabilité des procédés stéganographiques, qui garantissent une meilleure pérennité face aux transformations de format et une parfaite indépendance vis-à-vis des formats.

Bibliographie

G. Bailly et al., « *ARTUS: synthesis and audiovisual watermarking of the movements of a virtual agent interpreting subtitling using cued speech for deaf televiewers. »*, AMSE - Advances in Modelling, vol. 67, 2007, p. 177-187

C. Chastagnol, *Stéganographie en domaine vidéo compressé*, Mémoire de fin d'étude de l'École Centrale de Lyon, 2009.

A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, « *Digital image steganography: Survey and analysis of current methods* », Signal Processing, vol. 90, n°3, 2010, p. 727-752

S. Das, S. Das, B. Bandyopadhyay, S. Sanyal, « *Steganography and Steganalysis; different approches* », International Journal of Computers, Information Technology and Engineering, vol. 2, n° 1, 2008.

R. Fullerton, « *"A virtual social H-bomb": the late 1950s controversy over subliminal advertising* », Journal of Historical Research in Marketing, vol. 2, n°2, 2010, p. 166-173

Y. Hu, C. Zhang, Y.Su, « *Information Hiding Based on Intra Prediction Modes for H.264/AVC* », IEEE International Conference on Multimedia ans Expo, 2007, p. 1231-1234

I. Maitra, S. Nag, B. Datta, « *Digital Steganalysis: Review on Recent Approaches* », Journal of Global Research in Computer Science, vol. 2, n°1, 2011

A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.

F. Merciol, La Poste, « *Electronic franking seal or stamp and corresponding electronic seal or stamp issuing system* », Patent WO/2002/045027, 2002

C.-V. Nguyen, D.B.H. Tay, G. Deng, « *A Fast Watermarking System for H.264/AVC Vidéo* », IEEE Asia Pacific Conference on Circuit and System, 2006, p. 81-84

S. Singh, *The Code Book* (*Histoire des codes secrets)*, JC Lattès, 1999.

M. Wu, B. Liu. « *Data Hiding in Image and Video - Fundamental Issues and Solutions »,* IEEE Transactions on Image Processing, vol. 12, n°6, 2003.

T. Yamada Y. Takahashi, R. Ebisawa, I. Echizen, H. Yoshiura, « *Experiment on video watermark detection system using degraded original images* », IEEE International Conference on Industrial Informatics, 2010, pp 454-459