

Rapport de synthèse

Action spécifique STIC No. 39 – CNRS

Tatouage et dissimulation de données pour les communications audiovisuelles.

—

Début de l'Action : Février 2002. Fin : Février 2003.

Contacts : Franck.Davoine@hds.utc.fr & Jean-Marc.Chassery@lis.inpg.fr

Partenaires de l'Action Spécifique :

- **HEUDIASYC** (UMR CNRS 6599), Compiègne : Franck Davoine.
- **LIS** (UMR CNRS 5083), Grenoble : Jean-Marc Chassery, Patrick Bas.
- **TEMICS, IRISA** (UMR CNRS 6074), Rennes : Stéphane Pateux.
- **LSS** (UMR CNRS 8506), Supélec, Paris : Pierre Duhamel, Claude Delpha.
- **LIFL** (ESA CNRS 8022), USTL, Lille : Caroline Fontaine.
- **LTCI** (URA CNRS 820), ENST, Paris : Nicolas Moreau, Béatrice Pesquet, Henri Maître.

Autres personnes ayant participé aux réunions de travail de l'AS :

Philippe Nguyen, Séverine Baudry (**Thales** Communication),
Jacob Löfvenberg (Université de **Linköping**, *Division of Information Theory*, Suède),
Fabien Petitcolas (**Microsoft** Research – Cambridge, U.K.).

Doctorants : Cléo Baras, ENST,
François Cayre, ENST / UCL (Belgique),
Gaëtan Le Guelvouit, IRISA,
Hussein Joumaa, HEUDIASYC,
Boris Vassaux, LIS / Thales Communication,
Alejandro Guerrero, LIS.

Table des matières

1	Introduction.....	3
2	Contexte général	4
2.1	Le tatouage pour la sécurité :	4
2.2	Le tatouage en dehors du contexte sécuritaire:	5
3	Mise en œuvre :	5
3.1	Supports :	5
3.2	Méthodes :	6
3.3	Caractéristiques :	9
3.4	Attaques :	9
4	Les domaines concernés	10
4.1	Domaines d'intérêt :	10
4.2	Domaines connexes :	10
5	Etat des recherches.....	10
6	Conclusions et perspectives	12
7	- Annexe 1 : les réunions de travail de l'AS.	14
8	- Annexe 2 : Liste des thèses françaises soutenues (●) et en cours (■).....	16
9	- Annexe 3 : Sélection de publications récentes des partenaires	17
10	- Bilan financier	19

1 Introduction

L'intégration des flux audiovisuels dans l'Internet fixe ou mobile constitue aujourd'hui un enjeu technologique majeur, qui tend à rendre la **préservation des droits de propriété** des contenus indispensable. Cette nécessité a conduit dès 1993-95 de nombreux chercheurs à se pencher sur le problème de la sécurisation des données numériques face au piratage et à la contrefaçon, par **tatouage robuste**, afin notamment de faciliter le développement économique des techniques de communication audiovisuelle en réseaux.

Il est à noter que la cryptographie et la dissimulation d'information (par tatouage, *fingerprint* ou stéganographie) traitent toutes deux de la protection de l'information, mais leurs objectifs premiers sont différents. La cryptographie offre des outils permettant d'assurer la confidentialité (chiffrement), l'intégrité¹ (hachage, signature) ou encore l'authentification (protocoles de type défi-réponse). La dissimulation d'information a quant à elle pour objectif de cacher un message utile dans un message de couverture. Selon le contexte, on distingue :

- o la **stéganographie** : il doit être impossible de distinguer si le message de couverture contient un message utile ou non ;
- o le **tatouage** : le message utile est lié à l'identité de l'ayant droit du document de couverture, et doit donc rester présent même si celui-ci subit des modifications ;
- o le **fingerprinting** : lorsqu'un document est cédé à un nouvel acquéreur, il est préalablement marqué d'un nouveau message utile. Ceci permet de tracer les fraudes.

Le tatouage robuste (aquamarquage, *watermarking*) est aujourd'hui un sujet qui dispose d'un large champ de théories et de résultats. Il consiste à enfouir au sein-même de l'**information numérique** audio (parole ou musique) ou image (fixe ou vidéo), une **signature**² indélébile et non perceptible. Dans le cas de la **protection** des informations numériques, la signature permet d'en **identifier le propriétaire** ou l'**origine**. L'information, entendue au sens large du terme, peut avoir différentes représentations : dans sa forme originelle (échantillons, pixels) ou transformée (Fourier, ondelettes, etc.), ou dans sa forme compressée (flux numérique de transport).

Les utilisations des méthodes de tatouage peuvent être triées en fonction de **contraintes d'imperceptibilité**, de **robustesse**, de **sécurité**, de **capacité** et de **complexité**. Selon l'application, la présence de la signature doit être imperceptible (voire insoupçonnable dans le cas de la stéganographie). Elle doit être retrouvée dans le document tatoué, après dégradation volontaire ou pas de ce dernier, à condition bien sûr qu'il garde une valeur commerciale suffisante. La signature doit être sûre vis-à-vis de l'attaquant (illisible, indélébile) : le schéma de tatouage doit contribuer à la sécurisation de données audiovisuelles. Enfin, la capacité correspondant à la quantité de bits dissimulés dans le document hôte doit pouvoir être importante pour satisfaire certaines applications. Ces applications englobent une **grande variété de supports** numériques tels que par exemple les images satellitaires et médicales, les cartes géographiques, les documents textuels, les logiciels et les codes informatiques, les paramètres de formes et d'animation d'objets synthétiques et d'avatars 3D, etc.

Nous voyons aujourd'hui l'émergence d'**applications nouvelles** qui font appel, comme le tatouage robuste pour la protection, à des techniques de dissimulation de données dans des documents numériques.

¹ Garantit que l'image n'est pas modifiée.

² (à ne pas confondre avec la signature cryptographique). Appelée aussi filigrane, par analogie aux filigranes qui apparaissent sur les billets de banque.

Toujours dans un **cadre sécuritaire**, ces techniques sont étudiées pour vérifier l'**intégrité** des documents ou permettre leur **authentification**. Dans le cas de la stéganographie, elles permettent de transmettre une **information** secrète de manière totalement **cachée**, non détectable, au travers de documents publics (on parle dans ce cas d'imperceptibilité statistique de la signature). Elles sont également utiles pour le **traçage** des documents circulant sur Internet, le **contrôle d'accès** ou la **protection des copies** (DVD, etc.).

Elles doivent être utiles pour le **tatouage conjoint** de sources multimodales (textes, audio et vidéo, etc.), l'**indexation**, la **correction des erreurs** de transmission, le transfert d'informations au travers de **canaux cachés** à des fins d'**augmentation des contenus**.

Le tatouage conjoint permet par exemple de synchroniser ou de rendre indissociables un visage synthétique ou naturel de son signal de parole ou d'inclure une traduction automatique directement dans une séquence audiovisuelle. La correction automatique des erreurs après transmission ou attaques est possible en incrustant dans l'image une représentation d'elle-même (on parle dans ce cas de *self-correcting images*). Enfin, les techniques de dissimulation de données (*data hiding*) doivent permettre de transmettre une information supplémentaire au travers de données porteuses telles que des images ou des sons numériques. On bénéficie dans ce cas d'un canal (caché) auxiliaire ou le contenu numérique est « augmenté » d'informations supplémentaires. Les techniques d'indexation peuvent par exemple exploiter des informations utiles qui peuvent être retrouvées à partir d'une signature dissimulée dans une image ; cette signature code l'origine de l'image, sa destination, ses usages et caractéristiques - contenu sémantique, post-traitements, etc.

2 Contexte général

2.1 Le tatouage pour la sécurité :

Nous avons vu que le tatouage des documents multimédias est motivé par la nécessité de protéger les droits d'auteurs associés aux documents numériques : un filigrane dissimulé dans le médium est le garant de l'identité de son ayant droit. Il se doit d'être imperceptible, robuste et sûr. L'algorithme d'insertion, supposé public, est paramétré par une clé secrète (associée à l'ayant droit).

Ce contexte sécuritaire s'est également élargi à d'autres types d'applications. Un premier exemple est la traçabilité des documents, afin de permettre de suivre la piste des pirates et de remonter à la source de la fraude. On doit pour ce faire pouvoir différencier les différentes versions du document qui ont été diffusées, et ces derniers doivent contenir des filigranes distincts appelés empreintes ou *fingerprints*. Un deuxième exemple est la protection de copies et le contrôle d'accès. Dans ce cas, la présence du filigrane autorise la lecture du document. Le filigrane se doit d'être fragile : si le document est modifié, le filigrane doit disparaître, et sa présence est la garantie que tout va bien. Enfin, un dernier exemple concerne le milieu médical, où il est essentiel de pouvoir remonter à l'origine d'un document (IRM, scanner, radio), c'est-à-dire au document original (assurance de l'intégrité), ainsi qu'à son auteur (authentification du praticien). Dans ce cadre encore, le filigrane se doit d'être fragile.

Si dans un premier temps les différentes contraintes du tatouage pour la protection des contenus multimédias ont été considérées comme un défi pour la communauté scientifique et industrielle (fournisseurs de contenus multimédias), les différents schémas de tatouage présentés ont rapidement été confrontés à des attaques qui peuvent parfois poser problème (cf. section 3.4).

L'un des objectifs de cette réflexion au sein du CNRS est de dégager d'autres applications du tatouage que la protection. Il nous a semblé alors logique de redéfinir un paradigme du tatouage moins restrictif.

2.2 Le tatouage en dehors du contexte sécuritaire:

La finalité première du tatouage, c'est-à-dire l'insertion d'une signature à la fois imperceptible et indélébile et permettant la protection des droits d'auteurs peut s'avérer trop restrictive au vu des différentes applications que le sujet permet d'offrir. La deuxième contrainte, l'indélébilité, est de loin la plus problématique : le fait de limiter la robustesse des schémas de tatouage à des attaques connues permet d'élargir de manière sensible le champ d'applications du tatouage. Ce dernier se rapproche alors de la stéganographie en y incluant une notion de robustesse permettant une plus grande souplesse dans l'utilisation des contenus traités.

Dans ce nouveau paradigme, le tatouage permet la création de contenus multimédias étendus, c'est à dire des contenus qui peuvent contenir des fonctionnalités non prévues lors de l'étape de normalisation initiale. L'utilisation de telles techniques peut s'avérer extrêmement utile pour étendre les fonctionnalités de formats de contenus complètement figés. Dans un tel cadre l'objectif est bien différent du premier cas ; le tatouage peut alors être vu comme l'insertion d'une information imperceptible, partiellement indélébile et aussi importante que possible. Les contraintes associées sont alors différentes :

- o Les données transmises ne sont plus supposées être sensibles, l'utilisation de clés secrètes et la robustesse au sens cryptographique n'est alors plus obligatoire.
- o L'information ajoutée doit être aussi importante que possible de manière à offrir un panel de nouvelles fonctionnalités suffisamment large.
- o La robustesse du schéma de tatouage ne sera évaluée que dans le cas d'attaques bien définies, ce qui permet de mettre des stratégies d'insertion et d'extraction efficaces dans le cadre de l'application. Les traitements à prendre en compte seront principalement ceux qui ont lieu lors de la transmission du contenu étendu : le codage source, la réception et la mise en forme du contenu. Ce nouveau paradigme peut alors être vu comme la création d'un *canal de transmission caché*.
- o Les techniques de tatouage mises en œuvre devront également être de complexité très faible afin de pouvoir être utilisées dans des applications temps réel. La complexité devra être au moins inférieure à la complexité nécessaire au décodage du contenu.

Dans la littérature, plusieurs travaux reposent sur de telles contraintes, notamment l'utilisation du tatouage pour la compression d'images couleurs, la création d'images stéréoscopiques étendues, la correction d'erreurs pour la transmission de séquences vidéo, l'insertion de clones animés s'exprimant en langage parlé complété dans des séquences télévisées, l'utilisation du tatouage pour faciliter la fouille de données ou encore l'insertion de code barres invisibles pour servir à des fins publicitaires.

3 Mise en œuvre :

3.1 Supports :

- o *Tatouage d'images*. Les méthodes de tatouage doivent prendre en compte les spécificités des images fixes en couleur de basse et haute résolutions (photographies, images médicales, satellitaires, etc.), et des normes de compression telle que JPEG2000. Celle-ci permet un codage progressif des images en qualité ou résolution, et éventuellement par régions d'intérêt, à partir d'une transformation en ondelettes découpée en blocs. La signature doit donc pouvoir être insérée localement dans l'image

et résister à ce type de compression progressive. Elle doit être retrouvée entièrement ou en partie, à l'aide de tout ou partie du train binaire compressé.

- o *Tatouage de signaux audio.* Les travaux dans ce domaine tirent partie des recherches effectuées depuis de nombreuses années sur le codage audio, et les modèles de perception auditive. Les spécificités, les dégradations et les contraintes imposées par les normes de compression à débits variables d'audio (MPEG-1 MP3, MPEG-2 AAC, MPEG-4 GA) et de parole (G.723, G.728, MPEG-4 GA) sont prises en compte. Les méthodes de tatouage considéreront une large plage d'applications incluant la communication audio sur Internet (traçage, contrôle d'accès) et la musique de très haute résolution (protection des droits d'auteurs).

- o *Tatouage de séquences vidéo.* Les méthodes de tatouage prennent en compte la dimension spatio-temporelle des séquences vidéos ainsi que les spécificités des normes de codage vidéo MPEG-2, H.263 et MPEG-4. Elles doivent également permettre de tatouer des objets vidéos caractérisés par leur forme (contours), leur texture, et leur mouvement dans la scène visuelle. Ces descripteurs multiples peuvent permettre d'augmenter la robustesse et la capacité du tatoueur. Les applications vont de la communication audiovisuelle sur Internet (*streaming* vidéo à faible résolution) aux images de très haute résolution (TVHD, médical, etc.).

- o *Tatouage conjoint multi-supports.* Exemples : Audio et vidéo. Le tatouage peut être perçu comme une approche de fusion de différents supports. Ceci peut s'illustrer dans un cadre de transmissions sur un canal où un support sert de source porteuse à laquelle les autres supports sont associés par tatouage. Les méthodes de détection permettent de séparer et régénérer les sources.

- o *Autres types de données.*

Les images et objets synthétiques 2D/3D fixes ou animés (VRML, et MPEG-4 SNHC), et audios (MIDI, et MPEG-4 Audio).

Les bandes dessinées, les dessins animés.

Les bases de données (à des fins d'indexation et de contrôle d'accès).

Les programmes (scripts et codes logiciels) et les données textuelles.

3.2 Méthodes :

Nous avons vu que la **signature** numérique utilisée par un système de marquage doit être, selon le type d'application, indélébile ou fragile, indécélabile, de longueur suffisamment variable, et/ou illisible par une personne non autorisée et par quelque moyen que ce soit. Ces conditions ne peuvent bien sûr pas être rigoureusement toutes vérifiées en même temps, et les **méthodes de tatouage** doivent donc tenir compte de l'**application visée**, des **contraintes de sécurité** et de la **nature des données** à traiter. La signature sera cachée dans des **régions** du signal aptes à la porter, sémantiquement significatives, en tenant compte de leur capacité et de leur aptitude à rendre la marque imperceptible. L'algorithme de tatouage peut en outre être connu ou plus rarement secret. La coopération entre tatouage et cryptographie est bien sûr nécessaire pour vérifier les spécifications. L'algorithme de tatouage est souvent **symétrique** dans le sens où les paramètres utilisés pour incruster (on parle de clé privée) puis extraire la signature sont identiques. Des travaux portent sur le tatouage **asymétrique**, qui utilise des paramètres différents pour l'insertion et l'extraction de la signature, et qui permet donc de la relire à l'aide d'une seule clé publique.

Les méthodes de dissimulation reposent en grandes parties sur la théorie de l'information et des **communications numériques** (capacité, codes orthogonaux, codes correcteurs, multiplexes - OFDM, partage de canaux – TDMA, FDMA et CDMA, interférences), le traitement et l'analyse du **signal** (représentations temps-échelle, transformations multirésolutions orthogonales ou redondantes, ajout d'échos, filtrage et estimation de paramètres, segmentation, détection), les **statistiques** (décision,

tests d'hypothèses, mesures de confiance, fusion, reconnaissance), et la **cryptographie** (gestion de clés publiques et privées). Leur conception implique de prendre en compte les **mécanismes psychologiques et physiologiques** qui permettent de **percevoir les dégradations** des images, des couleurs ou des sons, mais également les différents types **d'attaques**³ pouvant altérer la signature.

Les premières méthodes de tatouage proposées dès 1995 étaient **empiriques**. Elles reposaient sur des techniques de substitution, consistant par exemple à inverser une certaine propriété d'un ensemble de sites choisis dans un signal hôte \mathbf{x} , telle qu'une relation d'ordre, en fonction du bit du message \mathbf{m} à cacher (le signal hôte \mathbf{x} correspond au signal original ou à une transformation de ce dernier par DCT, ondelettes, etc.). Ces méthodes relativement simples nécessitent, pour être robustes, l'utilisation de codes correcteurs d'erreurs spécifiques, ou de répéter les substitutions plusieurs fois sur différents segments du signal hôte. La « sécurité » du tatouage est cependant ainsi diminuée.

Le tatouage s'est ensuite appuyé sur les principes théoriques de la communication numérique, sur la théorie de l'information et la théorie des jeux [3,7]. Deux grandes approches du tatouage ont été proposées, reposant sur des méthodes additives ou substitutives à base de dictionnaires (méthodes issues des travaux de Costa [4]).

Les **méthodes additives** consistent à superposer à un signal hôte \mathbf{x} un signal de référence \mathbf{w} codant le message à cacher \mathbf{m} . On trouve dans cette classe de méthodes, le tatouage par étalement de spectre qui consiste à ajouter à \mathbf{x} un signal de faible énergie (afin de ne pas dégrader \mathbf{x}), et de très haute fréquence. Le signal tatoué est ainsi donné par $\mathbf{y} = \mathbf{x} + g \mathbf{w}$ ou $\mathbf{y} = \mathbf{x} (1 + g \mathbf{w})$ où g est un paramètre scalaire appelé force d'incrustation. Cette méthode correspond à une transmission d'information très redondante (une porteuse par bit d'information) et ne permet donc d'incruster qu'un nombre très réduit de bits dans le signal hôte \mathbf{x} . L'extraction des bits du tatouage se fait à l'aide de filtres adaptés, comme dans le cas des transmissions par modulations numériques classiques.

Les **méthodes substitutives de Costa** reposent sur l'utilisation de dictionnaires structurés. Le schéma théorique a récemment été adapté au problème du tatouage qualifié d'« informé », et comparé au codage de sources distribuées.

Le signal de tatouage \mathbf{w} est transmis au travers d'un canal perturbé par l'ajout du signal hôte \mathbf{x} et par des attaques modélisées par un bruit additif \mathbf{z} (cf. figure 1). Le tatouage est ainsi souvent considéré comme un problème de codage de canal, ayant pour objectif de protéger le message incrusté dans le signal hôte. Costa montre qu'il est possible de définir un schéma de codage du message \mathbf{m} de façon à ce que le premier bruit (dû à \mathbf{x} supposé gaussien) n'ait aucune influence sur la capacité du canal de transmission, donnée par $C = \log_2 (1 + \mathbf{P}/\mathbf{N})$ (l'énergie du signal \mathbf{w} est bornée par \mathbf{P} , et le bruit centré gaussien \mathbf{z} est de variance \mathbf{N}).

Dans le cas simple basé sur l'utilisation de quantificateurs scalaires ou vectoriels, le message à transmettre \mathbf{m} n'est pas enfoui dans le signal hôte. Il définit plutôt un dictionnaire de signaux autorisés. Le signal hôte \mathbf{x} est ainsi perturbé par quantification de manière à ce qu'il appartienne au dictionnaire représentant le message à cacher \mathbf{m} souhaité : le tatouage est donc **informé** puisque le codeur profite de la connaissance du signal hôte \mathbf{x} pour créer le signal de tatouage \mathbf{w} à partir du message original, noté \mathbf{m} (\mathbf{m} est codé à l'aide de mots codes dépendant du signal \mathbf{x}).

Dans le contexte du tatouage informé, on citera les travaux de Chen [1], Cox [5], Eggers [6], Chou [2], Pateux [8] et al. qui proposent d'utiliser des dictionnaires structurés définis par des quantificateurs algébriques, des syndromes de codes correcteurs d'erreurs ou des treillis modifiés.

³ telles que la compression, la perte d'informations au cours de transmissions, les brouillages, les tatouages multiples, etc.

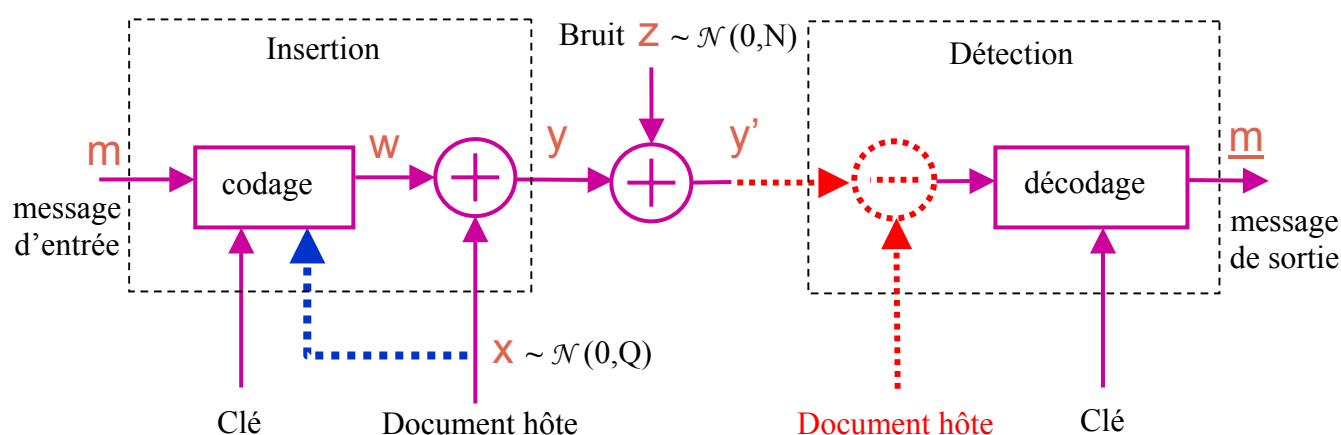


Figure 1 : Schéma général du tatouage vu comme une communication numérique avec ou sans information adjacente. Le codage du message m est informé lorsqu'il bénéficie de la connaissance du signal hôte x . Le décodage est aveugle lorsque le signal hôte x n'est pas requis. Le tatouage est symétrique lorsque la même clé permet d'insérer et de relire le tatouage.

Les méthodes de tatouage tirent également partie de modèles psychologiques et physiologiques de perception des dégradations des signaux et des images, pour pondérer le signal de tatouage w et définir des mesures perceptuelles des distorsions engendrées sur le document hôte par l'insertion et l'attaque du tatouage.

Ces méthodes de tatouage informé, lorsqu'elles utilisent la théorie des jeux, permettent de définir des limites sur les capacités atteignables en cas d'attaques optimales supposées connues de type « ajout pondéré de bruit blanc gaussien » (S-AWGN).

- [1] B. Chen and G.W. Wornell, Quantization index modulation: a class of provably good methods for digital watermarking and information embedding, IEEE Transactions on Information theory, 47(4):1423-1443, May 2001.
- [2] J. Chou, S.S. Pradhan and K. Ramchandran, On the Duality between Distributed Source Coding and Data Hiding, Conference on Signals, Systems and Computers, Asilomar, CA, 1999.
- [3] A.S. Cohen and A. Lapidoth, The gaussian watermarking game, IEEE Transactions on Information theory, 48(6):1639-1667, June 2002.
- [4] M. Costa, Writing on Dirty Paper, IEEE Transactions on Information theory, 29(3):439-441, May 1983.
- [5] I.J. Cox, M.L. Miller and J.A. Bloom, Digital watermarking, Morgan Kaufmann Publishers, 2002.
- [6] J.J. Eggers and B. Girod, Informed watermarking, Kluwer Academic Publishers, 2002.
- [7] P. Moulin and J.A. O'Sullivan, Information-theoretic analysis of information hiding, IEEE Transactions on Information Theory, 49(3), March 2003.
- [8] S. Pateux and G. Le Guelvouit, Practical watermarking scheme based on wide spread spectrum and game theory, to appear in IEEE Transactions on Image Processing, 2003.

3.3 Caractéristiques :

Le possesseur d'un document numérique tatoué possède une clé secrète qui lui permet selon le cas de vérifier la présence d'un tatouage ou d'extraire les bits du tatouage. On distinguera :

- le tatouage **symétrique** :
 - o **privé**, dans le cas où le document original, le tatouage à tester et la clé secrète ayant servi à tatouer le document sont disponibles,
 - o **semi-privé**, dans le cas où le tatouage à tester et la clé secrète sont disponibles,
 - o **aveugle**, dans le cas où seule la clé secrète est disponible.
- le tatouage **asymétrique**, dans le cas où une clé publique permet de lire le tatouage.

Le tatouage peut être :

- **robuste** lorsqu'il doit résister à un ensemble d'attaques spécifiées,
- **semi-fragile** : si le document est dégradé au-delà d'une certaine limite, le tatouage ne peut être retrouvé,
- **fragile** : si un seul pixel ou échantillons du document est modifié, le tatouage ne peut être retrouvé.

Le tatouage permet dans les deux derniers cas de contrôler l'intégrité de document numériques. Si il est en outre **effaçable**, la version originale du document tatoué peut être retrouvée.

Un tatouage **semi-robuste** des caractéristiques d'un document (ex. : version simplifiée d'une image) peut également permettre de détecter les régions du document qui ont subi des modifications, voire de les corriger partiellement.

La **capacité** d'un système de tatouage dans le contexte de la protection des droits d'auteurs n'est pas primordiale : l'insertion d'un numéro d'identification codé sur 64 bits suffit dans la plupart des applications de protection des contenus multimédias. Un seul bit est nécessaire pour la protection des copies. La capacité devra cependant être plus importante dans le cas d'applications du tatouage pour la transmission de données cachées, par exemple à des fins d'augmentation ou d'enrichissement des contenus multimédias.

Le schéma de protection par tatouage doit pouvoir être **sûr**, par exemple face à des attaques exhaustives (par force brute) ou des attaques par collusion ou recopie.

Au 19^{ème} siècle, Kerckhoffs évoque un principe affirmant que la sécurité d'un système ne doit reposer que sur la connaissance d'une clé, puisque toute méthode de chiffrement peut être connue de l'adversaire. Les cryptographes tiennent d'ailleurs essentiellement compte de la clé pour évaluer la sécurité d'un système de protection.

Dans le cas du **tatouage**, les laboratoires cherchent aujourd'hui à augmenter encore plus la robustesse des algorithmes de tatouage face à certains types d'attaques sans suffisamment prendre en compte les contraintes liés à la sécurisation d'une chaîne de transmission de données multimédias. Des efforts supplémentaires devraient porter sur les infrastructures de gestion des clés, le tatouage asymétrique, le tatouage non inversible et les notions de partage de secret ou de preuve à divulgation nulle de connaissance.

3.4 Attaques :

Le document hôte dans lequel les informations ont été cachées peut subir de nombreuses transformations. Il est important de noter que ces transformations ne sont pas nécessairement des attaques, puisqu'une compression peut être menée tout à fait honnêtement. Parmi les attaques,

certaines seront génériques et ne tiendront pas compte de la technique de tatouage utilisée, d'autres au contraire seront dédiées à certains schémas. Ceci dépendra du contexte.

On peut distinguer les désynchronisations géométriques aléatoires globales ou locales (ou les déphasages de signaux), l'utilisation de filtres optimaux (Wiener, etc.), l'ajout de bruits, les changements de format avec perte (compression, quantifications), les passages analogique / numérique (impression sur papier suivie d'une numérisation), etc.

La finalité des attaques n'est pas toujours la même. L'attaquant peut vouloir invalider la marque (par exemple dans le cadre de la protection des droits d'auteur) en lessivant le document : il altère celui-ci sans trop le dégrader. Mais l'attaquant peut également vouloir retrouver la clé secrète à l'origine du filigrane et qui est associé à l'ayant droit ou à l'auteur du document : ceci peut lui permettre ensuite de retirer tous les filigranes insérés avec cette même clé, ou encore de faussement attribuer un document au détenteur de celle-ci. Si l'attaquant désire enfin falsifier le document (par exemple dans un contexte médical), il lui faudra forger un nouveau document, valide. Une telle attaque peut être menée en estimant le filigrane contenu dans un document valide, et en l'insérant dans le faux document. Ceci peut également permettre de déjouer un lecteur n'autorisant que la lecture de documents tatoués (contrôle d'accès).

4 Les domaines concernés

4.1 Domaines d'intérêt :

- Les applications multimédias (photos, musique, audiovisuel),
- Le milieu médical, militaire, satellitaire,
- Les agences de presse, les documents officiels,
- Les musées,
- Les jeux, les logiciels.

4.2 Domaines connexes :

- Mathématiques : cryptologie, théorie des jeux, analyse statistique de données,
- Traitement du signal : compression, communications numériques,
- Sciences de la vie, SHS : psycho-perception,
- Informatique : analyse de codes, réseaux,
- Juridique, éthique,
- Economique,
- Culture.

5 Etat des recherches

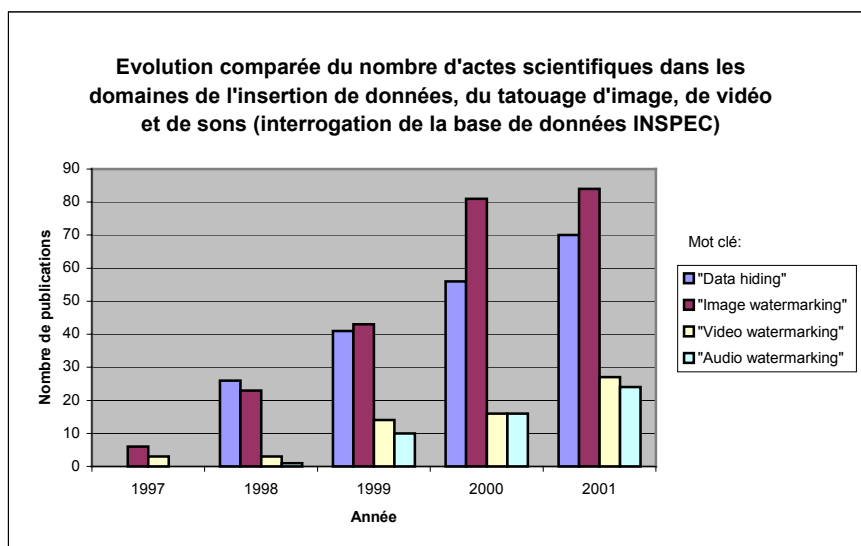
La gestion de la propriété intellectuelle et de la protection des documents audiovisuels est aujourd'hui largement prise en compte au niveau international, notamment par les groupes de **normalisation**. Nous citerons les normes JPEG2000 (codage des images fixes), MPEG-7 (description des contenus multimédias), et la future norme MPEG-21 (intégration de technologies multimédias). Ces travaux normatifs impliquent, de la part des acteurs industriels et académiques, de proposer des nouvelles méthodes de sécurisation pour la protection et d'authentification des documents multimédias, notamment des images fixes et animées, en accord avec leurs besoins.

Différents projets à caractère pré-compétitif ont déjà vu le jour en **France** et en **Europe**, notamment dans le cadre du RNRT, du CNRS ou des programmes européens RACE (ACCOPI), ACTS (TALISMAN, OKAPI, MIRADOR, OCTALIS) et IST (CERTIMARK, MIGRATOR 2000). Chacun de ces projets inclut l'utilisation de méthodes de protection par tatouage. En ce qui concerne le RNRT, nous citerons les projets :

- AQUAMARS : aquamarquage des documents audiovisuels pour leur transmission, diffusion, circulation, distribution en toute sécurité,
- AQUAFLUX : aquamarquage de flux multimédias (audio et vidéo) pour leur transmission, diffusion, circulation, distribution sur les réseaux hétérogènes de télécommunication,
- TUAMOTU : tatouage électronique sémantique de code Java,
- ARTUS : animation d'un codeur de Langage Parlé Complété virtuel par tatouage audiovisuel dans un service d'aide à la compréhension des sourds et malentendants en télédiffusion numérique,
- DIPHONET : diffusion de photographies à travers Internet,
- SEMANTIC-3D : service d'échange et de manipulation (tatouage, indexation et compression) des objets 3D.

L'enjeu est de travailler sur la conception du système de tatouage de documents audiovisuels, en considérant les besoins des utilisateurs (capacité, robustesse et perceptibilité de la signature) et les différents types de données numériques et de dégradations possibles. La prise en compte de ces contraintes évoluera au fur et à mesure des avancées des travaux de normalisation MPEG-7 et MPEG-21. Le groupe MPEG a aujourd'hui identifié le besoin d'outils de protection et de contrôle, dans le contexte des trois dernières normes : MPEG-4 (spécification des méthodes de protection et de la gestion de la propriété intellectuelle), MPEG-7 (description des conditions d'accès et d'utilisation, directement incluse dans les descripteurs et les schémas de description des contenus) et MPEG-21 (expression des droits des utilisateurs, créateurs, producteurs, propriétaires et distributeurs d'objets numériques appelés *Digital Items*).

Les premières publications dans le domaine du tatouage datent de 1993 avec une publication portant sur l'insertion de messages invisibles et robustes dans des images. En une dizaine d'années, ce domaine scientifique a connu une progression exponentielle jusqu'en 2000 (cf. graphique ci-dessous). Il s'avère que le nombre de publications scientifiques dédiées au tatouage d'images numériques est beaucoup plus important que celui des publications rattachées aux contenus vidéo ou audio (facteur de 3:1 environ). Le nombre de publications scientifiques consacrées aux maillages 3D, et plus encore aux textes et aux codes informatiques est marginal.



Le sujet principal qui est traité dans la majorité des publications concerne la robustesse des schémas de tatouage face à un type de traitement donné (compression, transformations géométriques). D'autres objectifs demeurent encore peu explorés : le tatouage d'images multi-composante (les images couleur, l'imagerie multispectrale), le tatouage conjoint au codage, l'analyse stéganographique (détection aveugle de la présence d'un message), le développement de schéma de tatouage haute-capacité, représentent autant d'axes de recherche futures.

Ce domaine très riche comporte également des points difficiles à traiter. Nous pouvons citer notamment l'évaluation d'algorithmes de tatouages destinés à des applications sensibles comme la protection des droits d'auteurs où les algorithmes sont sans cesse confrontés à de nouvelles attaques. Afin d'asseoir les bases théoriques du tatouage, il est également nécessaire de faire le lien entre les résultats obtenus en théorie de l'information et leur utilisation pratique.

Les premiers travaux sur le tatouage en France ont été initiés en 1996 (Thalès communication / Eurecom). Une communauté scientifique comprenant notamment des acteurs industriels (Thales Communication, Thomson Multimédia, NetImage) s'est rapidement rassemblée autour de ce sujet.

Au moment de la rédaction de ce document, le tatouage en France a donné lieu à une trentaine de thèses soutenues ou en cours. La communauté française est également liée à la communauté européenne via la participation à des projets européens (Certimark, Migrator 2000). La création de cette Action Spécifique offre également une structure visible pour s'insérer dans des instruments du 6^{ème} programme cadre de recherche de développement européen.

6 Conclusions et perspectives

L'action spécifique avait pour but de permettre à différents acteurs académiques nationaux de mettre en commun des compétences complémentaires, afin d'assurer une prospective de recherche sur le thème de la protection des données audiovisuelles numériques par des techniques de tatouage (marquage de la propriété de leurs ayants droit). Les partenaires de l'action se sont également intéressés aux méthodes plus générales de dissimulations de données, permettant l'authentification des documents audiovisuels et de vérifier leur intégrité. Le tatouage a été perçu comme faisant partie d'un mécanisme conjoint de compression, de sécurisation face au piratage et à la contrefaçon, d'étiquetage ou de protection des données audiovisuelles contre des dégradations volontaires ou involontaires.

Des analogies ont été établies entre la dissimulation de données par tatouage, les communications numériques et la cryptologie. **Le sujet reste cependant aujourd'hui insuffisamment traité.**

1) La notion de cryptographie asymétrique correspond à une fonctionnalité importante : la clé permettant par exemple de vérifier la signature de quelqu'un est publique, mais la signature ne peut avoir été produite qu'à l'aide d'une clé privée, connue du seul signataire. Cette fonctionnalité serait très utile en tatouage puisque l'on souhaiterait que tout le monde puisse vérifier la présence du message utile (garant de l'identité de l'ayant droit), tout en s'assurant que seul le détenteur de la clé privée (l'ayant droit) est en mesure d'enlever ce tatouage. Malheureusement, on ne connaît à l'heure actuelle aucun schéma de tatouage vérifiant cette propriété. On commence néanmoins à entrevoir des solutions spécifiques, permettant de protéger un document contre la copie en utilisant une telle dissymétrie.

2) Le problème de l'authentification cryptographique est assez proche, dans l'idée, du tatouage. En effet, l'ayant droit veut prouver qu'il est bien le propriétaire du document. On est donc tenté par la

transposition de solutions cryptographiques, au domaine du tatouage. Malheureusement, cela n'est pas si simple. En cryptographie, les protocoles d'authentification reposent souvent sur des problèmes arithmétiques (calcul d'un logarithme discret, etc.) ou de théorie des graphes (recherche d'un circuit hamiltonien dans un graphe de grande taille, etc.). Ces problèmes ne sont pas très faciles à adapter en tatouage. Prenons le cas des graphes, par exemple. Il est difficile d'associer un graphe de plusieurs milliers de points à une image, tout en s'assurant que ce graphe persistera, malgré les transformations que l'image risque de subir.

Le tatouage pour la protection vu comme une technique à la frontière entre les communications numériques et la cryptologie doit encore être approfondi.

Les outils utiles au tatouage sont également très proches de ceux issus de la théorie de l'information, de la théorie des jeux, et des communications numériques. Le tatouage peut tirer partie des connaissances acquises dans les domaines du codage conjoint source/canal, du codage de sources distribuées, du codage de données multimodales (vidéo, 3D, audio) et multicomposantes (couleur, multispectral), des représentations hiérarchiques, orthogonales ou redondantes, ainsi que des schémas de descriptions multiples des données multimédias.

La problématique du tatouage pour la protection ou l'augmentation des contenus doit être prise en compte directement au niveau de l'élaboration du schéma de communication numérique (codeurs source et canal). **Ceci reste actuellement un thème de recherche très ouvert.**

Sélection de perspectives de recherches restant ouvertes :

- Le tatouage et la cryptographie asymétrique,
 - Le tatouage et l'authentification cryptographique,
 - Le tatouage et la stéganalyse.
 - Le tatouage pour la protection des contenus et des transmissions, à la frontière entre les communications numériques et la cryptologie,
 - Le tatouage tirant partie de la théorie de l'information et de la théorie des jeux,
 - Le tatouage pour l'augmentation ou l'enrichissement des contenus (indexation multimédia, canal caché).
-

7 - Annexe 1 : les réunions de travail de l'AS.

Trois réunions ont été organisées en 2002 :

Le **19 février 2002** à l'ENST-Paris (13 personnes présentes). Chacun des six laboratoires a présenté ses travaux récents sur le tatouage d'images et des signaux audio.

Cinq sujets d'étude ont été retenus au terme de cette réunion de travail :

1. Tatouage et sécurité :
Liens entre cryptographie et tatouage, tatouage asymétrique, sécurité du tatouage, estimation du niveau de sécurité par rapport aux attaques possibles. *Fingerprinting*.
2. Tatouage : applications « hors sécurité » :
Authentification, intégrité, canal caché (*data hiding*). Applications en indexation, traçage, filtrage et augmentation des contenus.
3. Tatouage et codage canal
Protection du tatouage par codes correcteurs d'erreurs, adaptés au modèle de « canal de transmission » considéré.
4. Perception du tatouage et capacité
Etudes des modèles de perception dans les domaines « image, vidéo et audio » pour l'insertion du tatouage. Estimation de la capacité des images.
5. Méthodes de tatouage
Recensement, évaluation et comparaison des principales méthodes déjà proposées. Protocoles et approche système.

Un site Internet a été créé, afin de permettre de présenter les objectifs de l'Action Spécifique, et de permettre aux chercheurs désireux de participer aux travaux de l'action de nous rejoindre :

<http://www.hds.utc.fr/~fdavoine/astatouage/>

Le **31 mai 2002** à l'ENST-Paris (15 personnes présentes). Les partenaires de l'AS ont présenté le résultat de leurs recherches concernant un ou plusieurs des cinq thèmes sélectionnés.

- 10:15 – 10:30 : Introduction, présentations.
- 10h30 – 11h15 : Caroline Fontaine, LIFL.
Introduction to cryptography, relations between cryptography / watermarking.
- 11h15 – 12h00 : Stéphane Pateux, IRISA.
Watermarking, the Costa scheme, and channel coding.
- 12h00 – 13h00 : Open short presentations from other partners.
- 14h00 – 14h45 : Jacob Löfvenberg – **Linköping** University, Division of Information Theory.
Introduction to fingerprinting, and codes for fingerprinting.
- 14h45 – 15h30 : Fabien Petitcolas, **Microsoft** Research – Cambridge.
Watermarking attacks and Stirmark advances.
- 15h30 – 16h15 : Research perspectives in the field of Watermarking.
Next meetings of the *Action Spécifique*.

16h15 – 17h00 : Watermarking in the next EU's framework programme ?

Le **3 octobre 2002** à l'ENST-Paris (14 personnes présentes) dont le programme était :

- 10 h 30 : Hussein Joumaa, HEUDIASYC :
Quelques méthodes de tatouage vidéo.
- 10 h 50 : Béatrice Pesquet-Popescu, ENST :
Capacité du canal de tatouage pour des sources gaussiennes,
et adaptation au signal vidéo.
- 11 h 10 : Nicolas Moreau, ENST :
Adaptation aux signaux audio.
- 11 h 30 : Patrick Bas, LIS :
Le tatouage pour des applications autres que la sécurité.
- 12 h 00 : Franck Davoine, HEUDIASYC :
Authentification d'images par tatouage.
- 12 h 20 : Discussions
- 14 h : Sous-groupes de travail :
- Tatouage et sécurité
- Tatouage : applications hors sécurité
- Tatouage et codage correcteur d'erreur
- Perception et capacité du tatouage
- Méthodes de tatouage
- 15 h : Synthèses et réactions.
- 16 h 30 : Perspectives de l'action spécifique, etc.

Avant la fin février 2003 : écriture collective du présent rapport.

Les avancées de l'AS ont également été présentées :

Le **18 juin 2002** : journées scientifiques de présentation des Actions Spécifiques du département STIC, Paris.

Le **17 décembre 2002** : Michel Riguidel (RTP 13), journées scientifiques de présentation des Réseaux Thématiques Pluridisciplinaires du département STIC, CAP 15, Paris.

Le **17 janvier 2003** : Réunion du comité de pilotage du RTP 13 « Sécurité des accès, des échanges et des contenus », ENST, Paris.

8 - Annexe 2 : Liste des thèses françaises soutenues (●) et en cours (■) portant sur le tatouage et ses applications

- Stéphane Roche, Eurecom,
Mécanismes de sécurité liés à la diffusion des images : tatouage d'image, 18 mai 1999.
 - Christian Rey, Eurecom,
Tatouage d'image : gain en robustesse et intégrité des images, 14 février 2003.
 - Florent Autrusseau, Ircsyn,
Tatouage d'image basé sur la modélisation du système visuel humain, 7 novembre 2002.
 - Anne Manoury, Ircsyn,
Tatouage d'images numériques par paquets d'ondelettes, 21 décembre 2001.
 - Patrick Bas, LIS,
Méthodes de tatouages d'images fondées sur le contenu, 5 octobre 2000.
 - Gouenou Coatrieux, ENST,
Contribution à la sécurité d'images médicales par tatouage, 6 novembre 2002.
 - Teddy Furon, Thomson Multimedia / ENST,
Application du tatouage numérique à la protection de copie, 22 mars 2002.
 - Séverine Baudry, ENST / Thalès Communication,
Stratégies de codage canal pour le tatouage vidéo, 12 novembre 2001.
 - Leandro de Campos Teixeira Gomes, Paris V / ENST,
Tatouage de signaux audio, 5 juillet 2002.
 - Julien Stern, LRI / UCL,
Contribution à la théorie de la protection de l'information, 23 mars 2001.
 - Caroline Fontaine, INRIA Rocquencourt,
Contribution à la recherche de fonctions booléennes hautement non linéaires, et au marquage d'images en vue de la protection des droits d'auteur, 13 novembre 1998.
 - F. Raynal, INRIA Rocquencourt,
Etude d'outils pour la dissimulation d'information : approches fractales, protocoles d'évaluation et protocoles cryptographiques, 1 mars 2002
 - Teddy Voinson, CRAN,
Quantification vectorielle algébrique avec zone morte : application à la compression d'images à bas débit et au tatouage d'images, 7 mars 2003.
- | | |
|---|--|
| <ul style="list-style-type: none"> ■ Cléo Baras, ENST, tatouage audio. ■ Ilaria Venturini, ENST, authentification audio. ■ François Cayre, ENST / UCL, tatouage 3D. ■ Sonia Larbi, ENIT / ENST, tatouage audio. ■ Hussein Joumaa, HEUDIASYC, tatouage vidéo. ■ Yann Bodo, FTRD, tatouage audio. ■ Jonathan Delhumeau, IRISA, tatouage vidéo. | <ul style="list-style-type: none"> ■ Gaëtan Le Guelvouit, IRISA, tatouage d'images. ■ Alejandro Guerrero, LIS, tatouage audio. ■ Boris Vassaux, LIS / Thalès, tatouage vidéo. ■ J.-P. Boyer, DGA / LSS. ■ M. Haddad, FTRD / L2S / ENST. ■ A. Zaidi, LSS. ■ Gael Chareyron, LIGIV. |
|---|--|

9 - Annexe 3 : Sélection de publications récentes des partenaires

Différents travaux théoriques et applicatifs ont été menés conjointement par plusieurs partenaires et ont donné lieu à des publications :

F. Cayre, F. Davoine, "Vers un tatouage d'images mou", *Traitement du Signal*, Vol. 18, No. 4, déc. 2001.

F. Davoine, S. Baudry and P. Nguyen, Data hiding and digital watermarking, in *Eurasip News Letter*, Vol. 13, No. 1, 2002.

F. Davoine et S. Pateux (Eds.), "Tatouage de documents audiovisuels numériques", *Ouvrage du traité IC2*, Hermès Science. A paraître en 2003.

H. Joumaa, F. Davoine, "Tatouage substitutif d'images intégrant un masque de pondération psychovisuelle", *Actes de CORESA*, Lyon, France, pp. 249-252, 16-17 janvier 2003.

F. Raynal, F.A. Petitcolas and C. Fontaine, « Évaluation automatique des méthodes de tatouage », *Traitement du Signal*, 2002.

C. Fontaine, F. Raynal, « About the links between cryptography and information hiding », in *Proc. of IS&T/SPIE International Symposium on Electronic Imaging 2002: Security and Watermarking of Multimedia Contents IV*, SPIE, Vol. 4675, January 2002.

S. Baudry, P. Nguyen and H. Maître, "Optimal decoding for watermarks subject to geometrical attacks", in *Signal processing: Image communication*, 18, pp. 297-307, 2003.

F. Cayre, P. Rondao-Alface, F. Schmitt, B. Macq and H. Maître, "Application of spectral decomposition to compression and watermarking of 3D triangle mesh geometry", in *Signal processing: Image communication*, 18, pp. 297-307, 2003.

S. Baudry, P. Nguyen and H. Maître, "Use of synchronisation patterns to estimate geometric distortions in digital watermarking", in *Proc. of Eusipco*, Toulouse, France, Oct. 2002.

S. Baudry, P. Nguyen and H. Maître, "Estimation of geometric Distorsions in digital watermarking", in *Proc. of IEEE-ICIP*, Rochester, USA, 2002.

S. Baudry, J.-F. Delaigle, B. Sankur, B. Macq and H. Maitre, "Analyses of Error correction Strategies for Typical communication channels in Watermarking", *Signal Processing*, Vol. 81, n° 6, June 2001, pp.1239-1250.

Q. Chen, H. Maître and B. Pesquet-Popescu, "Oblivious image watermarking combined with JPEG compression", in *Proc. of IS&T/SPIE International Symposium on Electronic Imaging 2002: Security and Watermarking of Multimedia Contents IV*, SPIE, Vol. 5020, January. 2003.

F. Cayre and B. Macq, « Data hiding on 3D triangle meshes », *IEEE Transactions on Signal Processing*, Special Issue on Signal Processing for Data Hiding in Digital Media & Secure Content Delivery, à paraître en avril 2003.

P. Bas, J-M Chassery and Benoît Macq, "Image Watermarking: an evolution to content based approaches", *Pattern Recognition, Special Issue on Image/Video Communication* edited by D. Aboutajdine, 2002, pp. 545-561.

P. Bas et Benoît Macq, "Tatouage d'objets vidéos résistant aux manipulations", *Traitement du Signal* 2001 numéro spécial volume 18 N° 4, pp. 249-257.

P. Bas, J-M Chassery and Benoît Macq, "Geometrically Invariant Watermarking Using Feature Points ", *IEEE Transactions on Image Processing* , September 2002

P. Bas et Benoît Macq, "Méthode de tatouage fondée sur le contenu", *Traitement du Signal* 2002, vol 19, num1 pp. 11-18.

G. Le Guelvouit and S. Pateux, "Wide spread spectrum watermarking with side information and interference cancellation", *Proc. SPIE*, Santa Clara, CA, Janvier, 2003.

S. Pateux and G. Le Guelvouit, "Practical watermarking scheme based on wide spread spectrum and game theory", to appear in *IEEE Transactions on Image Processing*, 2003.

J. Delhumeau and T. Furon and N. Hurley and G. Silvestre, "Improved Polynomial Detectors for Side-Informed Watermarking", *Proc. SPIE*, Santa Clara, CA, Janvier, 2003.

G. Le Guelvouit and S. Pateux and C. Guillemot, "Information-theoretic resolution of perceptual WSS watermarking of non i.i.d. Gaussian signals", *Proc. Eur. Signal Processing Conf.*, vol. 1, pp. 454-457, Toulouse, France, Septembre, 2002.

G. Le Guelvouit and S. Pateux and C. Guillemot, "Perceptual watermarking of non i.i.d. signals based on wide spread spectrum using side information", *Proc. Int. Conf. on Image Processing*, Rochester, NY, Septembre, 2002.

T. Furon, N. Moreau and P. Duhamel, "Audio public key watermarking technique," in *Proceedings of the Int. Conf. on Audio Speech and Sig. Proc.*, 2000.

L. de C.T. Gomes, E. Gomez, N. Moreau, "Resynchronization methods for audio watermarking", 110th Convention of Audio Engineering Society, New York, September 2001.

L. de C.T. Gomes, E. Gomez, M. Bonnet, N. Moreau, "Méthodes de resynchronisation pour le tatouage audio", Dix-huitième Colloque GRETSI, Toulouse, Septembre 2001

L. de C.T. Gomes, M. Mboup, M. Bonnet, N. Moreau, "Cyclostationarity-based audio watermarking with private and public hidden data", 109th Convention of Audio Engineering Society Los Angeles, September 2000

10 - Bilan financier

Budget prévu: 45 735 Euros.

Budget alloué à l'AS: 30 487 Euros. Chaque laboratoire partenaire a reçu une somme de 4573 Euros.

Des missions ont été effectuées en France, correspondant à des déplacements ponctuels entre laboratoires, et sur des lieux de conférences. Certains partenaires ont assisté à des soutenances de thèse organisées en France. Chaque partenaire a utilisé la somme qui lui a été allouée pour des dépenses de fonctionnement, missions et/ou matériels utilisés dans le cadre de l'AS.

Le laboratoire Heudiasyc a reçu en plus des 4573 Euros une somme de 3049 Euros pour financer les déplacements des chercheurs internationaux, spécialistes du tatouage, invités à participer aux réunions de travail de l'Action.