# Tatouage informé basé sur un treillis : application à la vidéo.

Hussein JOUMAA, Franck DAVOINE

Laboratoire Heudiasyc, CNRS, Université de Technologie de Compiègne
BP 20529, 60205 Compiègne Cedex.
Joumaahu@hds.utc.fr, Franck.Davoine@hds.utc.fr

**Résumé –** Le tatouage informé est basé sur la construction d'un dictionnaire de codage partitionné en des sous-dictionnaires correspondants aux différents messages à insérer. Dans ce cadre, l'utilisation des codes correcteurs d'erreurs permet d'effectuer une recherche efficace dans le dictionnaire et d'assurer une distance importante entre les mots de code du dictionnaire. Miller et al. [11] ont proposé un système de tatouage informé basé sur la modification du treillis d'un code convolutif. Après une introduction des principales méthodes proposées en tatouage informé, nous utilisons le système de Miller et al. dans le cadre de tatouage des séquences vidéos : nous étendons le tatouage sur plusieurs images. Ce qui permet d'améliorer les performances de la méthode en terme de qualité du document tatoué. Le système ainsi proposé assure un niveau de robustesse important face à des attaques de traitement de signal, ainsi qu'une capacité d'insertion intéressante pour les applications d'augmentation de contenu.

**Abstract –** Informed watermarking is essentially based on a structured codebook : each message is associated to a sub-codebook. Error correcting codes are used to design the codebook because they can provide an efficient structuration of it, and an important distance between codewords. Miller et al. [11] have proposed an informed watermarking scheme based on the modification of a convolutionnel code trellis. After an introduction of the principal methods proposed on informed watermarking, we apply the scheme of Miller et al. on video watermarking : the host signal is extracted from several images. A gain on the quality of watermarked images is obtained. An important watermark robustness against signal processing attacks is also observed. Finally, the embedding capacity is adapted for watermarking applications such as hidden auxiliary channel or labelling.

## 1 Introduction

Le tatouage est souvent vu sous la forme d'une chaîne de communication numérique : un message codé $\mathbf{w}$ est transmis au travers d'un canal bruité par le signal hôte $\mathbf{x}$ ainsi que par un bruit additif $\mathbf{v}$. Le tatouage est dit "informé" lorsque le codeur profite de la connaissance du signal hôte $\mathbf{x}$ pour créer $\mathbf{w}$ à partir du message original, noté $\mathbf{m}$ : le tatouage devient donc un problème de communication numérique avec information adjacente au codeur. Dans le contexte du tatouage informé, on citera les travaux de Chen [2], Cox et al. [6], Eggers et al. [8], Chou et al. [3], Moulin et al. [12].
Dans la deuxième partie de cet article, nous rappellerons la notion de tatouage informé ainsi que les principales implémentations proposées dans la littérature, à base de quantification, ou de codes correcteurs d'erreurs. Dans la troisième partie, nous nous intéresserons à une implémentation d'un codeur informé utilisant le treillis d'un code convolutif et proposée récemment par Miller et al. [11]. Nous utiliserons cette approche pour le tatouage robuste et à forte capacité de séquences vidéos. L'article se terminera par la fourniture de résultats montrant les intérêts et les inconvénients de l'approche testée.

## 2 Tatouage informé

Considérons un système de tatouage visant à insérer un message $\mathbf{m}$ dans un signal hôte $\mathbf{x} = [x_1,x_2,\ldots,x_n]$. Le message $\mathbf{m}$ est codé par un vecteur $\mathbf{w} = [w_1,w_2,\ldots,w_n]$. Le signal tatoué est donné par $\mathbf{s} = \mathbf{w} + \mathbf{x}$. Le décodeur reçoit le vecteur $\mathbf{y} = \mathbf{s} + \mathbf{v}$ où $\mathbf{v} = [v_1,v_2,\ldots,v_n]$ est un vecteur représentant une attaque. Ce système de tatouage est décrit par la figure 1.

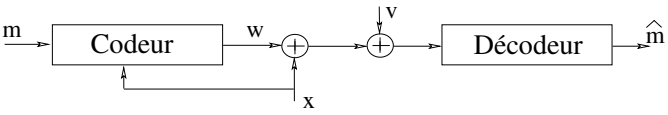


FIG. 1 – *Tatouage : problème de communication avec information adjacente au codeur*

Le tatouage est vu comme un codage de canal avec information adjacente au codeur (le signal $\mathbf{x}$). Dans le cas d'une communication à puissance limitée ($\frac{1}{n}\sum w_i^2 \leq P_w$) et de signaux $\mathbf{x}$ et $\mathbf{v}$ de composantes $i.i.d$, représentées respectivement par les deux variables aléatoires $X \sim \mathcal{N}(0,Q_x)$ et $V \sim \mathcal{N}(0,Q_v)$, Costa [5] a montré que la capacité d'un tel canal est donnée par $C = \frac{1}{2}\log(1 + \frac{P_w}{Q_v})$.
La capacité est ainsi indépendante du signal hôte $\mathbf{x}$, et est égale à la capacité d'un canal classique à bruit additif blanc gaussien. Le débit de la transmission au travers du canal est donc le même, que le décodeur ait accès à l'information adjacente ou pas.
Le résultat est obtenu en construisant un dictionnaire de codage $CB$ (*Code Book*) disponible au codeur et au décodeur, formé de $2^{nI(U,S)}$ mots de code $\mathbf{u}$, où $S$ est une variable aléatoire qui module $\mathbf{s} = \mathbf{w} + \mathbf{x}$. Le $CB$ est ensuite décomposé en des sous-dictionnaires de codage $CB_{\mathbf{m}}$ (*Bins*) : on associe à chaque message un sous-dictionnaire formé de $2^{nI(U,X)}$ mots de code. Au codeur, on veut transmettre le message $\mathbf{m}$.

Egalement, on dispose de la liste des mots de code du sous-dictionnaire correspondant à $\mathbf{m}$. Parmi cette liste, on choisit le mot de code $\mathbf{u}$ le plus approprié par rapport à l'état de canal partiellement connu du codeur (présence de $\mathbf{x}$). Ensuite, le signal $\mathbf{w} = \mathbf{u} - \alpha\mathbf{x}$ est envoyé à travers le canal. En général, on peut envoyer $\mathbf{w} = \mathbf{g}(\mathbf{u},\mathbf{x})$ : la fonction $\mathbf{g}$ permet d'effectuer une combinaison de $\mathbf{u}$ et $\mathbf{x}$ en respectant la contrainte d'énergie bornée de $\mathbf{w}$. Au décodeur, on reçoit $\mathbf{y} = \mathbf{w}+\mathbf{x}+\mathbf{v}$. Le vecteur $\mathbf{y}$ est décodé en un mot de code $\widehat{\mathbf{u}}$ en utilisant le dictionnaire principal CB. $\widehat{\mathbf{u}}$ appartient à un seul sous-dictionnaire $CB_{\widehat{\mathbf{m}}}$, ce qui permet d'estimer le message $\widehat{\mathbf{m}}$.
Le signal hôte est considéré comme un bruit disponible au codeur. Cependant, il ne peut pas être considéré comme un signal gaussien. Les attaques, en pratique, sont également de types très variés, et elles sont plus néfastes que des simples bruits gaussiens. Les travaux de Costa ont mis en évidence le gain résultant de l'exploitation de la présence du signal hôte au codeur.
D'autre part, la méthode présentée par Costa est basée sur un dictionnaire de mots de code pseudo-aléatoires : pour trouver un mot de code, il faut effectuer une recherche exhaustive dans ce dictionnaire. Il est important de construire un dictionnaire structuré $CB$ qui permet d'une part d'effectuer une recherche rapide et efficace des mots de code, et d'autre part de constituer un bon code de canal, ce qui se traduit par des contraintes sur les distances qui séparent deux mots de code de deux sous-dictionnaires $CB_{\mathbf{i}}$ et $CB_{\mathbf{j}}$ et deux mots d'un même sous dictionnaire $CB_{\mathbf{m}}$. Les premières implémentations du tatouage informé se sont basées sur des mots codes répartis sur le réseau régulier de points d'un quantificateur scalaire ou vectoriel : méthodes QIM, DM, SCS [2, 7, 10]. Dans ce cas, le problème du tatouage informé consiste à rechercher un système de quantification adéquat. Le principal avantage d'un tel système est qu'il permet d'assurer une recherche rapide dans $CB$. Les contraintes de distance imposées sur un codage informé restent plus difficiles à remplir.
Plusieurs chercheurs [4] [11] [9] associent à un dictionnaire de codage un code correcteur d'erreur : ils utilisent essentiellement un code convolutif, représenté par un treillis. En effet, un code correcteur d'erreur permet d'assurer les contraintes de distance et de structurer le schéma de codage de Costa. Le premier système de tatouage informé basé sur un code correcteur d'erreur a été présenté par Chou et al. [3] qui ont montré la propriété de dualité entre le codage informé avec information adjacente au codeur et le codage informé avec information adjacente au décodeur. Le tatouage constitue une application du premier problème. Quant au deuxième, il est principalement utilisé dans le problème de compression de sources distribuées qui consiste à compresser des sources corrélées, mais distantes et ne pouvant pas communiquer. Pradhan et al. [13] ont proposé une solution à ce problème, qui est basée sur l'utilisation du syndrome d'un code correcteur pour indexer les sous-dictionnaires de codage d'un schéma structuré. Chou et al. [4] ont appliqué la méthode proposée par Pradhan et al. au problème de tatouage, en utilisant une concaténation de deux codes convolutifs. Dans ce système de codes concaténés, les syndromes du premier code convolutif indexent les sous dictionnaires de codage $CB_{\mathbf{m}}$. Le deuxième code convolutif permet d'effectuer une recherche dans le dictionnaire de codage $CB$ au décodeur. Le choix d'un mot de code particulier d'un sous-dictionnaire se fait à partir de la connaissance de l'information adjacente $\mathbf{x}$, à l'aide d'une version modifiée de l'algorithme de Viterbi [4].
Le Guelvouit et Pateux [9] ont présenté une méthode basée sur un code correcteur d'erreurs qui consiste à ajouter au message à insérer un index identifiant les mots de code du sous-dictionnaire associé à ce message. La recherche dans le dictionnaire ainsi construit est assuré en utilisant un code convolutif : un sous-dictionnaire est balayé en effectuant un décodage a priori (on fixe la valeur des bits correspondant au message à insérer et on détermine l'index correspondant à un mot de code particulier du sous-dictionnaire actif). Un poinçonnage du code est effectué pour résoudre le problème de la variation de la longueur des mots de code selon le signal hôte.
Miller et al. [11] ont proposé d'utiliser des sous-dictionnaires construits par modification du treillis d'un code convolutif. Dans la partie suivante, nous présentons leur méthode avec plus de détails.

# 3 Tatouage informé basé sur le treillis modifié d'un code convolutif

Dans cette partie, nous présentons le système de tatouage informé proposé par Miller et al. [11]. Ce système repose sur le treillis pleinement connecté d'un code convolutif qui constitue le dictionnaire principal. Les sous-dictionnaires sont ensuite construits en élaguant le treillis en fonction du message à insérer. Dans la suite, nous introduisons la notion de treillis pleinement connecté ainsi que la méthode avec laquelle il est partitionné en des sous-dictionnaires de codage. Pour se faire, nous partons des notions d'un treillis classique. Dans le cas d'un code convolutif traditionnel, représenté par un treillis [1], un message $\mathbf{m}$ (de $k$ bits) est associé à un chemin particulier du treillis : $\mathbf{m}$ est ainsi codé par une suite de $k$ branches du treillis. Dans le treillis, deux branches sont issues de chaque nœud : la première correspond à un bit 0 de $\mathbf{m}$ et la seconde à un bit 1. Si on associe à chaque branche un vecteur pseudo-aléatoire de longueur $n_b$, $\mathbf{m}$ serait codé par un vecteur $\mathbf{w}$ de taille $k \times n_b$ (code de rendement $\frac{1}{n_b}$). On peut ajouter $\mathbf{w}$ à $\mathbf{x}$ et obtenir un schéma de tatouage par étalement de spectre.
Pour construire un tatoueur informé à partir du système précédent, Miller et al. [11] ont associé à un message $\mathbf{m}$ plusieurs chemins du treillis. Ces associations définissent un sous-dictionnaire. Elles s'effectuent en commençant par construire un treillis pleinement connecté $T$ : chaque nœud est connecté à tous les nœuds qui le précèdent et qui le suivent immédiatement. La moitié des branches porte un bit 0, l'autre un bit 1. Un message particulier $\mathbf{m}$ est ainsi représenté par plusieurs chemins dans le treillis : ces chemins constituent un treillis $T_{\mathbf{m}}$ correspondant au sous-dictionnaire $CB_{\mathbf{m}}$. Le treillis pleinement connecté $T$ est constitué de l'union des treillis $T_{\mathbf{m}}$ : $T$ joue le rôle du dictionnaire principal $CB$. La figure 2 illustre un exemple des treillis utilisés dans cette méthode.
On a ainsi construit un système structuré de tatouage informé. Au codeur, en utilisant l'algorithme de Viterbi appliqué sur le treillis $T_{\mathbf{m}}$, $\mathbf{x}$ est décodé pour trouver le vecteur $\mathbf{u} \in CB_{\mathbf{m}}$ le plus proche. Le message est ensuite codé par $\mathbf{w} = \alpha\mathbf{u}$. $\mathbf{w}$ est ensuite ajouté au signal hôte $\mathbf{x}$. Au décodeur, on reçoit le signal $\mathbf{y}$. En utilisant l'algorithme de Viterbi appliqué sur le

treillis $T$ pleinement connecté, $\mathbf{y}$ est décodé pour trouver le vecteur $\widehat{\mathbf{u}} \in CB_{\widehat{\mathbf{m}}}$ le plus proche. Le message $\widehat{\mathbf{m}}$ correspondant à $CB_{\widehat{\mathbf{m}}}$ est ainsi estimé. Le système ainsi présenté peut être considéré comme un système de tatouage par étalement de spectre, informé. Il permet d'assurer une robustesse qui dépasse celle obtenue par les systèmes de tatouage informé basés sur une quantification. Ce système semble intéressant dans une application de tatouage sur les séquences vidéo : il permet d'insérer un message de grande taille, tout en gardant une robustesse importante. On a ainsi appliqué le système sur des groupes d'images (GOP) de séquences vidéo. Dans la partie suivante, nous présentons la structure de l'algorithme proposé.

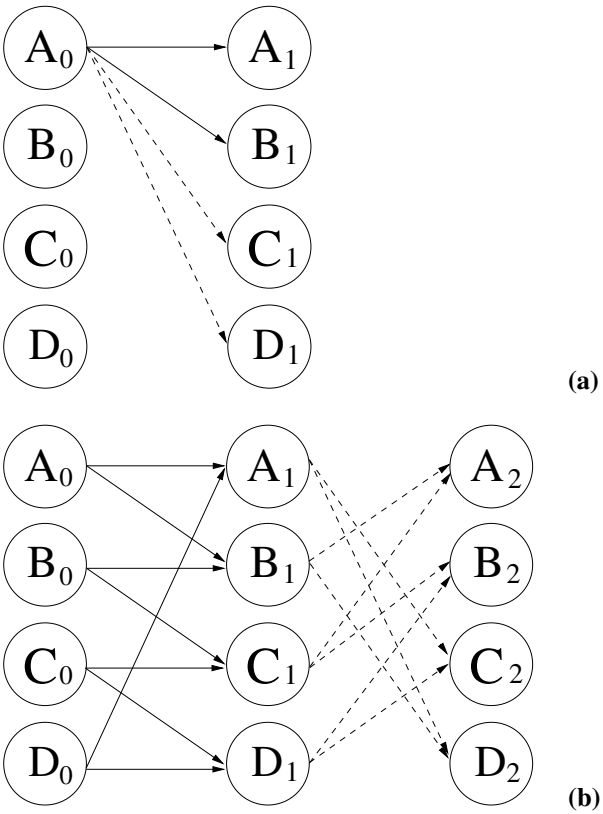


**FIG. 2 –** *Treillis utilisé par Miller et al. :*
*La figure (a) représente un exemple de treillis pleinement connecté à 4 états. De chaque état sont issues 4 branches : 2 branches (complètes) représentent un bit 0, les deux autres (pointillées) représentent un bit 1. Nous représentons seulement les branches issues de l'état* $A_0$.
*La figure (b) représente le treillis correspondant au message (01) : on ne garde que les branches correspondantes aux bits du message, on construit ainsi le sous-dictionnaire correspondant à (01).*

# 4 Tatouage appliqué aux séquences vidéo

Dans cette partie, nous présentons l'implémentation de l'algorithme sur une séquence vidéo. Le signal hôte est extrait d'un groupe d'images. Si on considère que la séquence va être soumise à une compression MPEG, le groupe d'images sera un GOP (*Group of Pictures*) de MPEG : l'insertion s'effectue sur les images I et P seulement (*Intra, Predicted Frames*). Il est nécessaire donc de séparer les images portant le même message d'une distance qu'on fixe en fonction de l'application. Un exemple d'un message réparti sur les images d'un GOP est présenté dans la figure 3.

On considère maintenant la structure adoptée par rapport à chaque image. On effectue un partitionnement des images à tatouer en des blocs $8 \times 8$ transformés par DCT. On extrait de chaque bloc $n_1$ coefficients de moyennes fréquences. Il nous est ainsi possible, en raccourcissant si besoin le vecteur $\mathbf{x}$, de ne conserver que $k \times n_b$ coefficients, afin d'insérer $k$ bits dans un groupe d'images (cf. section 3). On décode ensuite $\mathbf{x}$ en appliquant l'algorithme de Viterbi sur le treillis $T_{\mathbf{m}}$ correspondant au message, pour trouver parmi les configurations possibles, le vecteur $\mathbf{w}$ le plus proche de $\mathbf{x}$. Le décodage de Viterbi considère une mesure de corrélation pour trouver le chemin le plus vraisemblable. $\mathbf{w}$ est ensuite ajouté à $\mathbf{x}$ avec une pondération $\alpha$ : $\mathbf{s} = \mathbf{x} + \alpha\mathbf{w}$.
Au décodeur, on applique l'algorithme de Viterbi sur le treillis $T$ pleinement connecté, pour décoder le vecteur $\mathbf{y}$ extrait d'un groupe d'images de la séquence reçue.

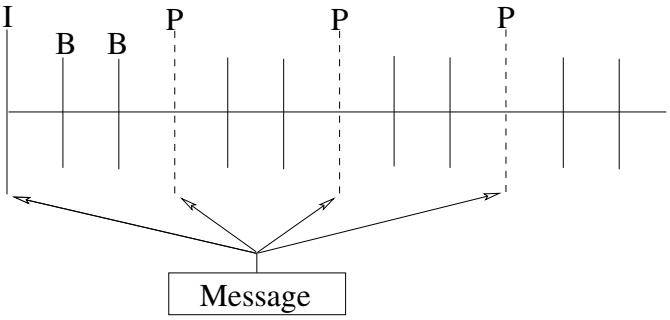


FIG. 3 – *Exemple d'un message inséré dans les images I et P d'un GOP de* 12 *images.*

# 5 Résultats

Nous avons effectué une série de tests, pour évaluer la performance du système face à des attaques de type traitement de signal. Nous présentons des tests effectués sur la séquence *Foreman* composée de 150 images de $176 \times 144$ pixels. Un groupe d'images est constitué de 12 images : nous choisissons d'insérer un message de longueur 37 bits étendu sur 4 images du groupe, séparées l'une de l'autre par 2 images non tatouées (cela correspond à une structure $MPEG-2$ très utilisée en pratique, qui a un $GOP$ de 12 images, et qui code 2 images B entre 2 images P).
Nous avons effectué le décodage suite à une perturbation due à une compression de type $MPEG-2$. La figure 4 représente le pourcentage moyen de bits erronés ($BER$ moyen) au décodeur en fonction du taux de compression, pour des forces de tatouage différentes. La force de tatouage correspond à une qualité visuelle moyenne $Q$ des images tatouées non compressées, représentée par un $PSNR$ moyen en $dB$.
Nous présentons dans la suite les résultats de décodage après une série d'attaques effectuées sur une séquence tatouée de qualité visuelle correspondante à un $PSNR$ moyen de 42.197

$dB$ (la qualité $Q_3$ dans la figure 4). Nous représentons la force des attaques par le $PSNR$ moyen évalué entre les images de la séquence tatouée et celles de la séquence attaquée. Nous avons réussi à décoder le message après un filtrage median $2 \times 2$ ($PSNR = 25.72\ dB$) et un filtrage median $3 \times 3$ ($PSNR = 26.2\ dB$), et après un filtrage convolutif par un filtre gaussien $3 \times 3$ ($PSNR = 28.5\ dB$), et un filtre de rehaussement $3 \times 3$ ($PSNR = 19.2\ dB$). Nous avons pu décoder le message après l'ajout de bruit blanc, jusqu'à un niveau $PSNR$ élevé de $18\ dB$. Enfin, si les images de la séquence tatouée sont éclaircies ou assombries (changement d'échelle), le décodage est toujours possible.
Ces résultats montrent la robustesse de l'algorithme face aux attaques de type traitement de signal.

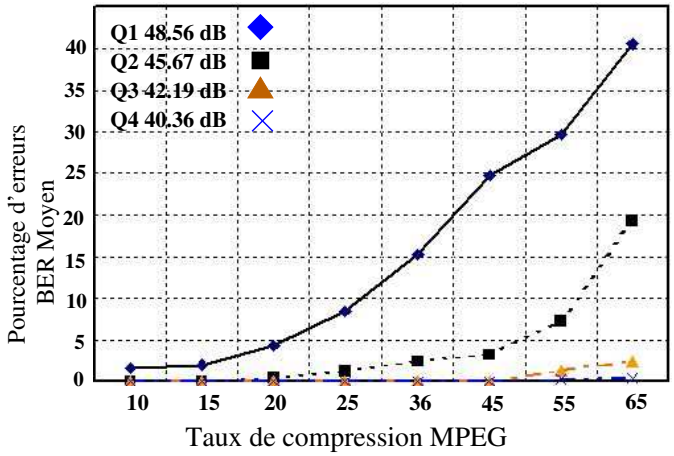


FIG. 4 – *$BER$ moyen suite à une compression $MPEG - 2$, pour quatre qualités de tatouage différentes.*

## 6 Conclusion

Nous avons présenté un système de tatouage informé à base de treillis, testé sur des séquences vidéo : le treillis est utilisé pour représenter différents sous-dictionnaires de codage. Contrairement aux principaux algorithmes de tatouage informés basés sur des quantificateurs, la méthode est plus robuste face à l'attaque qui consiste à modifier l'échelle des niveaux de gris d'une image. La robustesse de la méthode est intéressante face aux attaques de type traitement de signal. La capacité de la méthode peut également être réglée en fonction de l'application (par exemple, transmission au travers de canaux cachés). Cependant, la méthode reste complexe à cause des calculs de corrélation effectués par l'algorithme de Viterbi. Cette compléxité peut cependant être réduite [14]. D'autre part, une adaptation de la force de tatouage en fonction du mouvement et du contenu visuel serait intéressante : un mouvement rapide serait récompensé par un facteur de pondération plus important.
Nous étudions également l'applicatiopn du schéma à des représentations redondantes (*overcomplete expansions*) du signal hôte.

## Références


[1] G. Battail. *Théorie de l'information. Application aux techniques de communication*. Collection Pédagogique des Télécommunications, Masson, 1997.

[2] B. Chen. *Design and Analysis of Digital Watermarking, Information Embedding and Data Hiding Systems*. PhD thesis, Massachusetts Institute of Technology, 2000.

[3] J. Chou, S. S. Pradhan, and K. Ramchandran. On the duality between distributed source coding and data hiding. In *Proceedings of Conference on Signals, Systems and Computers*, Asilomar (CA), USA, 1999.

[4] J. Chou, S. S. Pradhan, and K. Ramchandran. Turbo coded trellis-based constructions for data embedding : Channel coding with side information. In *Proceedings of Conference on Signals, Systems and Computers*, Asilomar (CA), USA, November 2001.

[5] M. Costa. Writing on dirty paper. *IEEE Transactions on Information Theory*, 29(3):439–441, May 1983.

[6] I.J. Cox, M.L. Miller, and A.L. McKellips. Watermarking as communications with side information. *Proceedings of the IEEE*, 87(7):1127–1141, 1999.

[7] J.J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod. Scalar costa scheme for information embedding. *IEEE Transactions on Signal Processing*, to appear in the Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery, 2003.

[8] J.J. Eggers, R.K. Su, and B. Girod. A blind watermarking scheme based on structured codebooks. In *IEE Colloquium on Secure Images and Image Authentification*, London, UK, April 2000.

[9] G. Le Guelvouit and S. Pateux. Wide spread spectrum watermarking with side information and interference cancellation. In *Proceedings of SPIE : Security and Watermarking of Multimedia Contents*, Santa Clara, USA, January 2003.

[10] M. Kesal, M. Kivanc, R. Koetter, and P. Moulin. Iteratively decodable codes for watermarking applications. In *Proceedings of 2nd International Symposium on Turbo Codes and Related Topics*, Brest, France, 2000.

[11] M. L. Miller, G. J. Doër, and I. J. Cox. Dirty-paper trellis codes for watermarking. In *Proceedings of IEEE International Conference on Image Processing*, New York, USA, September 2002.

[12] P. Moulin and J. A. O'Sullivan. Information-theoretic analysis of information hiding. In *Proceedings of IEEE International Symposium on Information Theory*, Italy, June 2000.

[13] S. S. Pradhan and K. Ramchandran. Distributed source coding using syndromes(discus): Design and construction. In *Proceedings of the IEEE International Conference on Data Compression*, Snowbird, USA, March 1999.

[14] A. J. Viterbi and J. K. Omura. *Principles of digital communication and coding*. McGraw Hill, 1979.