Tatouage informé pour le codage distribué

Cagatay Dikici, Khalid Idrissi, Atilla Baskurt

INSA de Lyon, Laboratoire d'InfoRmatique en Images et Systèmes d'information,
LIRIS, UMR 5205 CNRS, France

Concours jeune chercheur : Oui

Résumé

Nous partons de la dualité entre le tatouage et le codage distribué pour proposer un schéma qui exploite ces deux techniques dans un même système. Dans celui-ci, nous proposons de faire simultanément de l'insertion de message et de la compression en faisant appel au codage distribué. Pour la compression, nous utilisons des méthodes de code de correction d'erreurs comme LDPC, alors que pour l'insertion il sera fait appel à une méthode de quantification simple afin de ne pas augmenter la complexité du codeur. Des résultats expérimentaux pour des données de synthèse sont fournis, puis le système proposé est comparé à d'autres systèmes existants.

Mots clefs

Codage distribué, tatouage, LDPC

1 Introduction

La dualité entre le codage canal et le codage source est connue depuis quelques décennies [1] et les techniques cherchant à s'approcher de la capacité limite sont développées dans les deux cas. Pour le codage source, ou tout simplement la compression, les approches qui exploitent la redondance de la source, telle que le codage arithmétique [2] peuvent atteindre des taux proches des limites données par la théorie de l'information. De même pour le codage canal, les codeurs convolutionnels et les décodeurs itératifs ont permis [3] s'approcher des limites
Le codage source avec une information parallèle, désignée par Side Information (SI), disponible au décodeur a été étudié par Slepian Wolf [4] and Wyner Ziv[5], respectivement pour les cas sans et avec pertes. Les applications qui utilisent ce schéma datent de quelques années, et ont cherché à déporter la complexité vers le décodeur, afin de compresser à moindre coût en terme de puissance de calcul. De nombreuses approches pour le codage de sources distribuées (DSC) sont proposées telles que le codage par block [6], les turbo codes [7] ou les codes LDPC [8]
De la même manière, le codage canal avec une SI disponible au codeur a été étudié par [9] et [10]. La similarité entre ce schéma et le tatouage aveugle, dans lequel un message est transmis à travers un canal et où le signal support est disponible uniquement au codeur a été initialement abordée par [15]**.** Par la suite, des travaux ont concerné la dualité entre le codage source avec SI (SCSI) et le codage canal avec SI (CCSI) [11][12][13] puis de nombreux systèmes de tatouage informé exploitant cette dualité ont été proposés [14][15][16].

Dans ce papier, on se propose d'utiliser cette dualité pour réaliser un système de tatouage informé couplé avec du codage source distribué. Un message caché M sera alors inséré dans un signal hôte X puis compressé, sachant qu'un signal Y, corrélé avec X est disponible au niveau du décodeur.

Ce papier est organisé de la façon suivante: dans la Section 2 nous formalisons le problème du tatouage informé, puis la théorie du codage de sources distribuées est présentée en Section 3. Après une brève introduction sur la technique de quantification structurée basée sur les codes LDPC en Section 4, les détails de la méthode proposée sont présentés en Section.5. Enfin, la dernière section est consacrée à la discussion des premiers résultats obtenus, ainsi qu'à la comparaison avec des méthodes existantes.

2 Tatouage Informé

Le problème du tatouage aveugle peut être abordé comme du codage canal avec une SI au codeur tel que présenté en Figure 1. Le codeur a accès au signal de tatouage M, ainsi qu'au signal support X dans lequel l'information de tatouage va être insérée. Une contrainte de distorsion entre X et le signal tatoué W est fixée telle que $E[(X-W)^2] \le D_1$, avec $W = X + e$, et l'erreur e est dépendante de X et de M.Ensuite, le signal tatoué W peut être sujet à une distorsion à l'issue d'une attaque Z.
La capacité que l'on peut atteindre [9] pour un système de tatouage avec une probabilité d'erreur $P_e^n = \Pr\left\{\hat{M}(Y^n, X^n) \neq M\right\}$ est :

$$C_{10} = \max_{p(u,w|x)} [I(U;Y) - I(U;X)] \quad (1)$$

où U est une variable auxiliaire, où la maximisation porte sur toutes les fonctions de densité de probabilités conditionnelles $p(u,w|x)$ et où $I(U;Y)$ représente l'information mutuelle entre U et Y. Un taux R peut être atteint s'il existe une séquence parmi les $(2^{nR},n)$ codes avec $P_e \to 0$ [13].

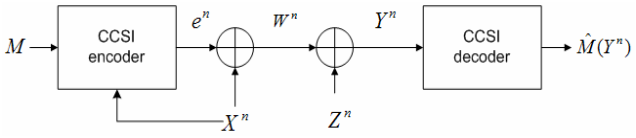


Figure 1. Codage Canal avec une information parallèle au codeur

3 Codage Distribué

Le codage de sources distribuées (DSC) peut être considéré comme un problème de Débit/Distorsion avec une SI disponible au décodeur tel que représenté Figure 2. La notation dans [13] est telle que l'indice 01 dans $RDSI_{01}$ indique la disponibilité de la SI au décodeur et non au codeur. Considérons $\{(X_k,Y_k)\}$ une séquence i.i.d. $\approx p(x,y)$ des variables aléatoires X et Y. X_k est codé sur un block de longueur n dans un flux binaire avec un débit utilisant une séquence parmi les $(2^{nR},n)$ codes avec $i: X^n \to \{1,2,..,2^{nR}\}$ et $\hat{X}^n : \{1,2,..,2^{nR}\} \to \hat{X}^n$. Le signal d'entrée X doit être codé et transmis au récepteur où l'on dispose de Y, une observation bruitée du signal d'entrée X et de $\hat{X}$ une estimation de X avec un critère de fidélité D_2 tel que $E[(\hat{X}-X)^2] \le D_2$. Le débit minimum de codage [5] pour un critère de fidélité donné D_2 est:

$$R_{01}(D_2) = \min_{\hat{X}=f(U;Y),p(u|x)} [I(U;X) - I(U;Y)] \quad (2)$$

Où la minimisation porte sur toutes les fonctions de densité de probabilités conditionnelles $p(u|x)$ et la fonction $f(U;Y)$ telle que $E(X-\hat{X})^2 \le D_2$. U étant une variable auxiliaire pour l'ensemble des mots-codes représentant X et $I(U;X)$ l'information mutuelle entre U et X.

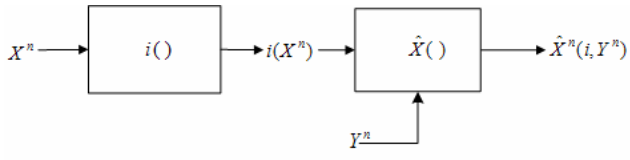


Figure 2.Codage Source avec une information parallèle en décodeur

4 Codage LDPC

Les limites théoriques présentées dans les Sect. 2 et 3 peuvent être atteintes dans le cas de codes à longueur infinie, en utilisant une technique de quantification aléatoire. Cependant, il ne semble pas réaliste d'utiliser cette approche, étant donné sa complexité et la longueur des blocs excessive nécessaire. En revanche, un codage canal adéquat, peut permettre de se rapprocher de ces limites.

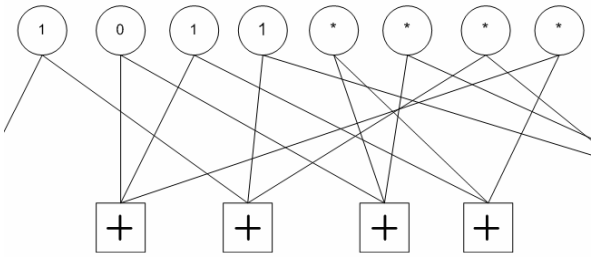


Figure 3.Le codage LDPC

Les codes LDPC initialement proposes par [17] et revus par [18] font partie des codes blocs ou les bits de contrôle sont intégrés au signal d'information de manière à détecter et corriger les erreurs introduites lors de la transmission. Il est fait appel à une matrice de parité H composée d'un faible nombre de 1. Les codes LDPC sont dits réguliers ou irréguliers selon que le nombre de bits de contrôle rajoutés est fixe ou non. Dans notre cas nous utiliserons le code régulier. La Figure 3 illustre un exemple de codage LDPC : Les cercles représentent les bits du message, tandis que les carrés représentent des nœuds de contrôle. Pour le codage, l'addition modulo 2 des bits reliés à chaque nœud doit être nulle. Une partie du bloc à coder est donnée en Figure 3, le but étant de trouver les bits de contrôle notés $*$. Ainsi pour le premier nœud, le bit de contrôle doit être à 1 alors que pour le deuxième, il doit être à 0. Ceci permet de trouve un mot-code unique.

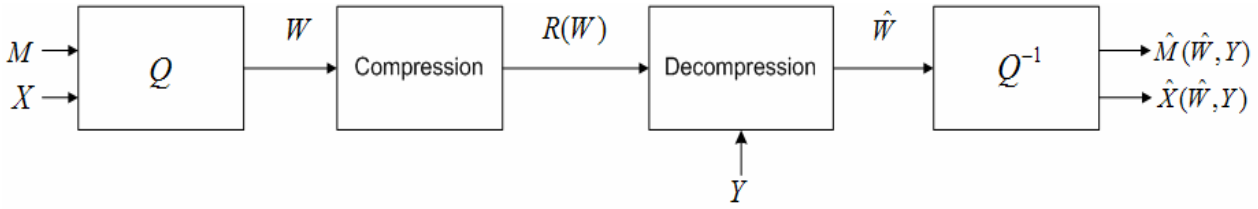


Figure 4. Le système proposé

Le décodeur basé sur un algorithme MAP est optimal pour décoder les codes LDPC. Mais, étant donné la longueur des blocs, il ne semble pas réaliste d'implémenter ce genre d'algorithme en raison de la complexité induite. Cependant, une bonne estimation $\hat{X}$ peut être obtenue en un algorithme de vraisemblance [3] comme dans le décodage LDPC classique [18].

5 Système proposé

Nous proposons un schéma hybride utilisant le codage canal au codeur et le principe de débit/distorsion avec SI au décodeur (Figure 4). Précisément, notre système permet de d'insérer un message M dans un signal hôte X avec une certaine distorsion D_1. Ensuite le signal tatoué W est compressé et transmis avec un critère de fidélité D_2, le récepteur disposant de Y, une observation bruitée de X.

Y est obtenue en simulant un canal binaire symétrique entre le signal d'entrée X et l'information parallèle Y. Le récepteur decode alors le signal reçu, en exploitant l'information Y avec un critère de fidélité D_2 tel que $E[(\hat{W}-W)^2] \le D_2$ et fournit une estimation du message inséré $\hat{M}$ avec une probabilité d'erreur $P_e(\hat{M})$.

Mathématiquement, le but est de résoudre le problème :

$$\min_{E[(X-W)^2 \le D_1, E[(\hat{W}-W)^2 \le D_2]} P_e(\hat{M}) \qquad (3)$$

où $P_e(\hat{M})$ représente la probabilité de l'erreur de décodage $\Pr\{\hat{M}(\hat{W},Y) \neq M\}$, et W, X, Y sont des variables aléatoires i.i.d. $\approx p(w,x,y)$.
De plus, la contrainte de distorsion $E[(\hat{W}-W)^2] \le D_2$ amène à une fonction de débit minimal:

$$R(D_2) = \min_{p(u|w,x)\,p(\hat{w}|u,y)} [I(U;X,W) - I(U;Y)] \qquad (4)$$

Ce problème hybride peut être présenté comme une forme de tatouage semi-aveugle, le récepteur n'ayant pas accès au signal d'entrée X pour extraire le message $\hat{M}$ depuis le message tatoué W, mais seulement à Y, observation bruitée de X.

6 Expérimentation

A ce stade, nous nous sommes intéressés à l'aspect théorique de la dualité codage canal avec SI et codage source avec SI. Dans cette section, nous présentons le système réel proposé, et qui implémente simultanément, l'insertion de message et la compression.

6.1 Les signaux d'entrée

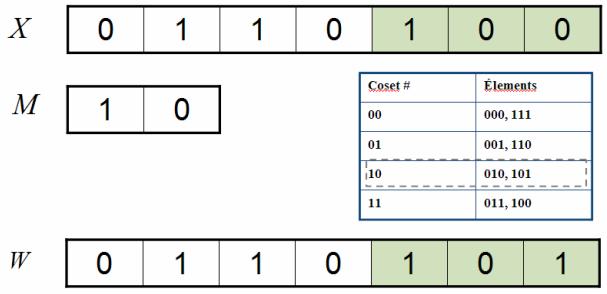
Pour la simulation, des données de synthèse sont générées sous forme de vecteurs binaires i.i.d X et Y, respectivement disponibles au codeur et au décodeur, ainsi que pour le message M à insérer. L'information X est créée à partir d'une source de Bernoulli pseudo aléatoire ½ de longueur de block adaptée pour avoir $H(X) = 1$ bit/symbole.

L'information parallèle est donnée par $Y = X \oplus N$ où le niveau de corrélation N entre X et Y est un vecteur pseudo aléatoire de Bernoulli(p) de même longueur que Y et $\oplus$ est l'opérateur d'addition modulo 2. La variable $p : 0 \le p \le 1$ contrôle le niveau de corrélation tel que $H(X|Y) = H(p) = p \times \log_2(p) + (1-p) \times \log_2(1-p)$

6.2 Le Tatouage

Dans le cas d'un tatouage informé, où l'on insère M dans X, une quantification basée sur la construction de cosets est utilisée. L'algorithme se comporte de la manière suivante : 3 bits d'information sont partitionnés en 4 cosets tels qu'une distance de hamming de 3 existe entre chaque couple de cosets. L'élément du coset à utiliser sera choisi en fonction de la valeur des bits de M qui sont à insérer (ici par groupe de 2 bits, donc $Coset00 = \{000,111\}, Coset01 = \{001,110\}$, $Coset10 = \{010,101\}, Coset11 = \{011,100\}$). Une fois le dictionnaire créé, 2 bits de M et R bits de X sont considérés, formant un bloc de 2+ R bits. On prend les 3 bits de poids faible de ce dernier pour réaliser

l'insertion. Ces 3 bits sont quantifiés par $W : W(X, M) = \arg \min_{Z \in CosetM} \|Z - X\|$ où W a au plus 1 bit de différence avec X. La distance de hamming est choisie. Ce processus d'insertion de 2 bit dans un bloc de R bits est poursuivi jusqu'à épuisement des données de M. Un exemple est présenté en Figure 5 : si le message 10 doit être inséré dans les 3 bits de X de valeur 100, le minimum de distance de hamming entre 100 et les éléments du $Coset10$ est obtenu pour $W = 101$, ce qui sera retenu comme sortie. Au niveau du décodeur, l'extraction du tatouage est simple, car la connaissance du dictionnaire permet de retrouver le message inséré



Coset #	Elements
00	000, 111
01	001, 110
10	010, 101
11	011, 100

Figure 5. Un exemple d'insertion de tatouage

6.3 DSC

Cette partie décrit la compression du signal tatoué W utilisant la technique du codage de sources distribuées, sachant que l'information parallèle Y est connue uniquement au décodeur. Classiquement, les codes LDPC rajoutent de la redondance au signal d'entrée. Après le processus de codage, l'ensemble peut être décomposé en 2 parties, la partie systématique S_w contenant le signal d'origine et la partie de contrôle P_w contenant les cosets. En fait, après le codage du signal d'entrée, seule l'information de contrôle est transmise. Le Récepteur a accès à Y et aux bits de contrôle du signal tatoué P_w. Le but de décodeur est d'extraire les erreurs entre Y et W. Pour cela un algorithme de propagation de vraisemblance modifié, proche du codage LDPC standard [18].

Tout d'abord, les taux de vraisemblance des bits systématiques sont initialisés en adéquation avec le niveau de corrélation N entre X et Y. Ensuite, les taux de vraisemblance des bits de contrôle sont choisis sachant que la probabilité d'erreur en réception de ces bits est faible ε. De plus, la mise à jour des noeuds de contrôle est modifiée de manière à corriger les erreurs dans les bits systématiques, sachant que les bits de contrôle sont corrects avec une probabilité élevée. Enfin, la connaissance du dictionnaire des cosets et l'estimation de $\hat{W}$ à l'aide du décodage LDPC rend l'extraction du message $\hat{M}$ triviale. Les niveaux de distorsion obtenus sur $\hat{W}$ et $\hat{M}$ sont donnés dans les résultats.

7 Simulations

Dans l'expérimentation réalisée, 100 blocs de 4000 bits chacun, représentant le signal d'entrée X sont générés. L'information parallèle Y est créée comme cela a été décrit dans la Sec.6.1 avec une entropie conditionnelle $H(X|Y)$ entre 0 et $0{,}5$. Un premier test a consisté à évaluer les performances de la compression sans tatouage. Le signal d'entrée X est compressé à l'aide de LDPC avec un taux de 1/2 tel que décrit dans la Sec.6.3, puis les 2000 bits de contrôle de chaque bloc sont transmis. Au niveau du récepteur, le décodage est réalisé par LDPC à l'aide de l'information parallèle Y, en se limitant à 50 itérations.

Le système proposé a été comparé à d'autres systèmes existants basés sur le turbo code ou le LDPC régulier et irrégulier avec différentes longueurs de blocs [8][19] [20]. Par la suite, et toujours avec le même schéma, un message M est inséré avec un taux de $1/200$ pour différentes valeurs de $H(X|Y)$. Dans ce test, 2 bits de tatouage sont insérés dans chaque bloc de 400 bits X (cf Sec.6.2).

La Figure 6 représente la probabilité d'erreur entre le signal X et son estimation au décodeur $\hat{X}$ en fonction de l'entropie conditionnelle $H(X|Y)$, autrement dit, en fonction de la distorsion entre X et l'information parallèle Y. Le réseau de courbe est relatif à différentes méthodes de codage et à différentes longueurs de blocs. La limite théorique de Slepian Wolf pour un codage ½ est $H(X|Y) = 0{,}5$. La courbe relative à notre système (LDPC régulier avec une longueur de bloc de 4000 bits) atteint une erreur de 10^{-6} pour $H(X|Y) = 0{,}36$. La comparaison avec les autres méthodes montre que le turbo code [19] permet d'avoir le même résultat pour $H(X|Y) = 0{,}35$ et que le codage régulier LDPC avec une longueur de block de 10^4 [20] donne de meilleures performances que le système proposé. En revanche il nécessite une longueur de blocs 3 fois supérieure. Comme on peut le voir sur la courbe, le codage LDPC irrégulier avec des blocs de longueur 10^4 et 10^5 [8]

atteint le même niveau d'erreur pour des valeurs de $H(X|Y)$ respectivement de 0,42 et 0,45.

A noter que l'augmentation de la longueur des blocs entraîne un accroissement de la complexité et du temps de décodage.

La courbe en haut à gauche est relative au système complet, incluant tatouage et compression. Il faut bien voir que nous avons définit un critère de similarité entre le signal d'entrée X et le signal tatoué W, or, étant donné que c'est W qui est utilisé pour le décodage, l'erreur entre X et son estimation au décodeur $\hat{X}$ ne peut pas être inférieure à l'erreur de $W - X$. Ainsi, le système complet permet d'avoir une probabilité d'erreur de 5×10^{-3} pour $H(X|Y) = 0{,}34$. Le message M quant à lui, peut être retrouvé avec une probabilité d'erreur de 10^{-6} pour $H(X|Y) = 0{,}36$. D'autres tests seront effectués afin de comparer les méthodes entre elles, en utilisant les mêmes longueurs de blocs.

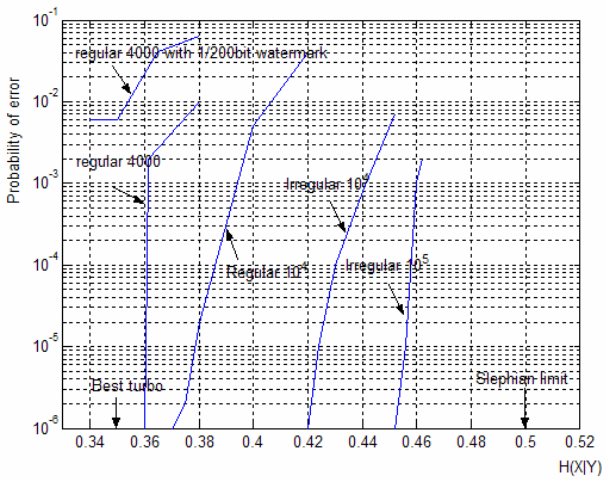


Figure 6 – la comparaison du system codage distribué

8 Conclusions

Un système hybride pour le tatouage et la compression, se basant sur la technique du codage distribué a été proposé. Les récents travaux sur la dualité entre le codage canal et la notion de débit/distorsion exploitant l'existence d'une information parallèle a été employé.

Le schéma de la Figure 4 permet de nombreuses possibilités d'usage. Les entrées et la nature du message M à insérer pouvant être choisis en fonction du problème à traiter. Le système proposé a été comparé à des systèmes existants utilisant diverses méthodes de codage. D'autres approches peuvent être envisages (tatouage à base de treillis, ou de quantification LDPC) pour améliorer les performances. Ce système peut également être facilement adapté à la vidéo, en utilisant la corrélation entre les images successives.

Références

[1] C. E. Shannon, Coding theorems for a discrete source with a fidelity criterion , IRE Nat. Conv. Rec., vol. Part 4, pp. 142-163, 1959.

[2] Elias, P. (1975) Universal codeword sets and representations of the integers. IEEE Trans. Info. Theory 21 (2): 194-203.

[3] Berrou, C., and Glavieux, A., Near optimum error correctingcoding and decoding: Turbo-codes. IEEE Trans. On Communications 44: 1261-1271,1996.

[4] J. D. Slepian and J. K. Wolf, Noiseless coding of correlated information sources , IEEE Transactions on Information Theory, vol. IT-19, pp. 471-480, July 1973.

[5] A. D. Wyner and J. Ziv, The Rate-Distortion Function for Source Coding with Side Information at the Decoder , IEEE Transactions on Information Theory, vol. IT-22, no. 1, pp. 110, Jan. 1976.

[6] S.S. Pradhan, K. Ramchandran, Distributed Source Coding Using Syndromes (DISCUS). *IEEE Transactions on Information Theory*, vol. 49, no. 3, March 2003. IEEE, USA.

[7] B. Girod, A. Aaron, S. Rane and D. Rebollo-Monedero , Distributed video coding, *Proceedings of the IEEE, Special Issue on Video Coding and Delivery*, vol. 93, no. 1, pp. 71-83, Jan. 2005.

[8] Z. Xiong, A. Liveris, and S. Cheng, Distributed source coding for sensor networks, IEEE Signal Processing Magazine, vol. 21, pp. 80-94, September 2004

[9] S. Gel'fand and M. Pinsker, Coding for channel with random parameters , Problems of Control and Information Theory, vol. 9, pp. 19-31, 1980.

[10] M. Costa, Writing on dirty paper, IEEE Trans. on Information Theory, vol. 29, pp. 439-441, May 1983.

[11] S. S. Pradhan, J. Chou and K. Ramchandran, Duality between source coding and channel coding and its extension to the side information case. IEEE Transactions on Information Theory, vol. 49, vo. 5, May 2003. IEEE, USA.

[12] J. K. Su, J. J. Eggers and B. Girod, Illustration of the Duality Between Channel Coding and Rate Distortion with Side Information, Actes de la *34th Asilomar Conf. on Signals, Systems, and Computers*. Oct. 29-Nov. 1, 2000, Asilomar, CA, USA.

[13] T. M. Cover and M. Chiang, Duality between channel capacity and rate distortion with two-sided state information, IEEE Trans. of Inform. Theory, vol. 48, no. 6, pp. 1629 - 1638, June 2002.

[14] Chappelier V., C. Guillemot and S. Marinkovic, Turbo Trellis Coded Quantization, Actes de la *Intl. symp. on turbo codes*, September, 2003.
[15] Miller M. L., G. J. Dorr and I. J. Cox., Applying informed coding and informed embedding to design a robust, high capacity watermark," IEEE Trans. on Image Processing, 3(6): 792807, 2004.
[16] Eggers J., R. Buml, R. Tzschoppe and B. Girod, Scalar costa scheme for information embedding, IEEE Trans. Signal Processing,2002.
[17] R. G. Gallager, Low density parity check codes, Ph.D. dissertation, MIT, Cambridge, MA, 1963.
[18] MacKay, D. J. C. and R.M. Neal, Near Shannon limit performance of low density parity check codes, Electronics Letters, vol. 33, pp. 457-458, 1996.
[19] A. Aaron and B. Girod, Compression with side information using turbo codes, Proc. DCC'02, Snowbird, UT, April 2002.
[20] A. Liveris, Z. Xiong and C. Georghiades, Compression of binary sources with side information at the decoder using LDPC codes, IEEE Communications Letters, vol. 6, pp. 440-442, October 2002.