TATOUAGE D'IMAGES COULEURS AVEC CCE : APPLICATION À LA SÉCURITÉ ROUTIÈRE

G. Lo-varco[1] W. Puech[1] M. Dumas[1]

[1] Laboratoire CEM2, UMR CNRS 5507

Université Montpellier II
Pl. Gabriel Péri, 30021 Nîmes Cedex 1, France

lovarco@cem2.univ-montp2.fr, puech@univ-montp2.fr, dumas@univ-montp2.fr

Résumé

Dans cet article, nous présentons une méthode de tatouage originale s'appuyant sur les informations couleurs des images et intégrant un code correcteur d'erreur (CCE) par polynôme générateur. Cette technique a été développée de manière à être robuste à la compression mais aussi à la détérioration modérée de zones réduites de l'image. Ces modifications sont d'ailleurs typiques de l'application visée : la sécurisation du transfert d'images radars pour la sécurité routière.

Mots clefs

Tatouage couleur, LSB2, Code correcteur d'erreur, Robustesse à la compression, Sécurité routière.

1 Introduction

Le transfert d'images par réseau devient actuellement très important. Les applications vont de l'imagerie médicale à la télésurveillance, en passant par l'imagerie satellitaire et la sécurité routière. Durant le transfert des images, l'aspect sécurité n'est pas encore vraiment résolu [1]. L'objectif du tatouage pour la transmission d'images est d'insérer une information dans l'image de manière invisible et indélébile. L'information insérée peut d'ailleurs être un message de longueur relativement importante. L'insertion peut se faire de manière différente en fonction de la longueur du message à insérer et de la robustesse désirée [2]. Nous présentons dans cet article une optimisation d'une méthode de tatouage spatial par bloc [3] par utilisation de l'information couleur [4] [5] et l'ajout d'un code correcteur d'erreur (CCE) [6].

2 Tatouage couleur et CCE

Le système de tatouage proposé comporte plusieurs étapes qui optimisent la longueur du message afin d'augmenter la redondance [7]. Pour insérer le message, 18 caractères sont nécessaires. La plaque d'immatriculation, l'heure et la date sont codés sur 72 bits en utilisant un codage d'Huffman. Les bits sont ensuite regroupés par blocs de 12. Un CCE par polynôme générateur, Frame Check Control, est alors ajouté [6]. Celui ci permet de détecter la présence d'erreurs. Le message total est alors codé sur 96 bits.
Dans le cas d'images couleurs, le plan bleu est utilisé pour insérer le polynôme générateur, nécessaire au CCE. Le message total de 96 bits est inséré au niveau des plans rouge et vert, autant de fois que possible en fonction de la taille de l'image. Le système complet est illustré figure 1. Pendant le transfert, si une zone est modifiée, du fait de la redondance, le message sans erreur peut quand même être détecté. Cependant, si les modifications sont importantes, tous les messages reçus peuvent être faux. Le CCE détecte alors les bits faux du message reçu.

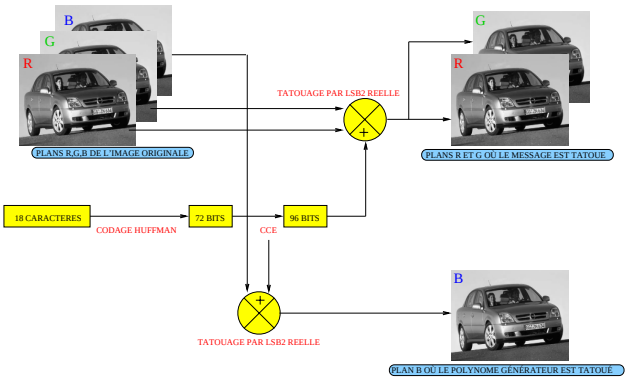


Figure 1 – *Schéma complet de la méthode de tatouage développée.*

2.1 Méthode de tatouage

La méthode de tatouage utilisée s'appuie sur la substitution, par bloc de pixels, du second bit de poids le plus faible (LSB2) d'un critère statistique [4]. Les blocs de N pixels permettent d'insérer le message plusieurs fois dans l'image. Par exemple, dans une image de 300×400 pixels, avec $N = 64$, le message sera inséré 20 fois.
La première étape du tatouage consiste à calculer la moyenne des niveaux de gris d'un bloc de N pixels de

l'image. Celle-ci notée μ vaut $\mu = \sum_{i=1}^{N} p(i)$, $p(i)$ étant le niveau de gris du pixel i de l'image. Ensuite, on calcule la valeur réelle $R_\mu = [\sum_{i=1}^{N} p(i)]\%4$ qui permet d'obtenir le second bit de poids le plus faible ou LSB2 de cette moyenne. Le tatouage consiste alors à modifier la moyenne du bloc pour amener $R_\mu\%4$ à des valeurs stables (1 ou 3) correspondant aux bits 0 ou 1 du message. Enfin, ce bit est tatoué par substitution du LSB2 de la moyenne.

2.2 Originalité du système

La première originalité de notre méthode est la longueur importante du message tatoué (environ 800 bits dans une image de taille 700×600 pixels). Cette longueur est nécessaire pour la redondance du message unitaire.
La seconde particularité de notre principe est le codage source de nos informations. La plaque, l'heure et la date sont codées non pas selon la norme ASCII mais avec un code singulier, calculé selon le principe de Huffman. L'objectif de ce codage spécifique est de diminuer la longueur du message. Pour celà, on utilise un code dont l'entropie est plus élevée que l'entropie du code ASCII. Ainsi, les informations plaque, date et heure ne nécessitent plus que 12 caractères au lieu de 18.
Calculons l'entropie pour un message unitaire :
il faut 12 caractères Huffman soit 72 bits donc entropie (Huffman) = $\frac{12}{72} = 0.167$
il faut 18 caractères ASCII soit 144 bits donc entropie (ASCII) = $\frac{18}{144} = 0.125$.
Enfin, la dernière particularité de notre méthode est son objectif : combiner robustesse à la compression ainsi qu'à la forte détérioration de zones de l'image. La robustesse à la compression est due à la méthode de tatouage par blocs [4]. Cependant, noton que l'image doit être de haute qualité. Certes, pour la détection du message, cela n'est pas nécessaire mais, pour notre application, une accusation doit être possible suite à la détection. Aussi, pour être indiscutable, l'image doit être la plus lisible possible.

2.3 Perturbations liées à la transmission du message

Une des caractéristiques principales de la transmission est son débit. Celui-ci doit être le plus élevé possible. Aussi, les images, porteuses d'une grande quantité d'informations, doivent être comprimées pour une transmission plus rapide. Du fait de son irréversibilité, la compression engendre des perturbations. D'autres erreurs apparaissent également en raison de la physique du réseau utilisé. Outre ces modifications inévitables, il peut survenir des perturbations volontaires du message ou "attaques" visant la falsification du message.

Compression. Avant de transmettre l'information, il est nécessaire de la coder afin de l'adapter au réseau de transmission. On parle alors de codage source. Pour ce qui concerne les images, une norme de compression est fixée, il s'agit du format JPEG. En vue de l'application à la sécurité routière, l'objectif premier est que le tatouage résiste à des facteurs de qualité standards (jusqu'à 75%).

Support de transmission. Tous les systèmes de transmission introduisent des modifications du signal source. Pour quantifier ces erreurs et évaluer la qualité du transfert, un paramètre peut être calculé : le taux d'erreur binaire ou TEB. Il s'agit du rapport entre les bits erronés et les bits transmis.

$$TEB = \frac{Nombre\ de\ bits\ erronés}{Nombre\ de\ bits\ transmis}$$

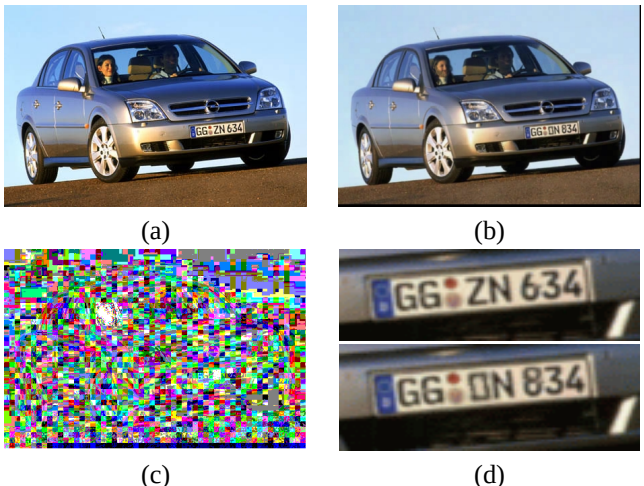
Le nombre de bits erronés reste toutefois très faible puisque le TEB varie de 10^{-4} pour les réseaux courants à 10^{-12} pour les réseaux à fibres optiques. Par conséquent, le CCE utilisé corrige ce faible nombre d'erreurs liées à la transmission.

Attaques. Les attaques que peut subir l'image doivent respecter deux contraintes pour falsifier la photographie sans que cela soit décelable. Tout d'abord, la zone de modification doit être la plus petite possible. En effet, plus la taille augmente, plus le risque de voir la modification grandit. De plus, la modification doit se fondre dans l'image donc elle ne doit pas être trop forte pour rester quasi-invisible.

3 Résultats

3.1 Application sur des images de voitures

Pendant le transfert, l'image originale, figure 2.a, a subi plusieurs modifications illustrées figures 2.b et d. Le tableau 1 nous indique par plan les messages qui ont subi ces modifications. En effet, la différence entre l'image originale et l'image falsifiée, figure 2.c, met en évidence les zones modifiées.



(a) (b) (c) (d)

Figure 2 – *a) Image originale, b) Image tatouée puis falsifiée, c) Différence entre l'image tatouée falsifiée et l'image originale, d) Plaque originale et plaque falsifiée.*

	Plan rouge	Plan rouge falsifié
Messages justes	21/21	17/21
Messages faux	×	32090ZN63482G1010 G0ZN6340213010103 GGWN6340212010712
	Plan vert	Plan vert falsifié
Messages justes	21/21	17/21
Messages faux	×	80130ZN63423130110 GUZN6340213070460 GGYN6340213010712

Tableau 1 – *Messages récupérés avant et après modification, pour le tatouage du message suivant GGZN6340213010103, répété 21 fois.*

3.2 Evaluation de la robustesse du système face aux perturbations

Compression. Les figures 3 et 4 permettent d'évaluer la robustesse de notre système face à la compression. Les résultats obtenus valident l'utilisation du CCE ainsi que l'emploi du vote bit à bit. En effet, la figure 3 montre que dès que le facteur de qualité de 90% est atteint, il y a plus de polynômes avec un bit faux que de polynômes justes. Or, avec le vote bit à bit, on peut observer, figure 4, que jusqu'à un facteur de qualité de 70%, tous les bits du polynôme sont récupérés. La conversion de l'image tatouée au format JPEG en conservant le message inséré est donc possible avec notre méthode.

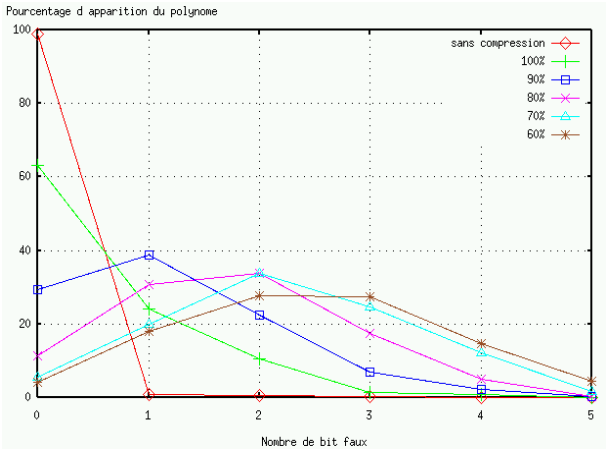


Figure 3 – *Obtention du polynome en fonction du nombre de bits faux pour plusieurs facteurs de qualité de compression.*

Support de transmission. A partir du taux d'erreur binaire (TEB), on peut calculer la probabilité de transmission du message sans erreur, notée P et donnée par la formule suivante : $P = (1 - TEB)^n$ avec n taille du message en bits. La figure 5 illustre les valeurs de P pour plusieurs longueurs de message transmis par différents types de réseau

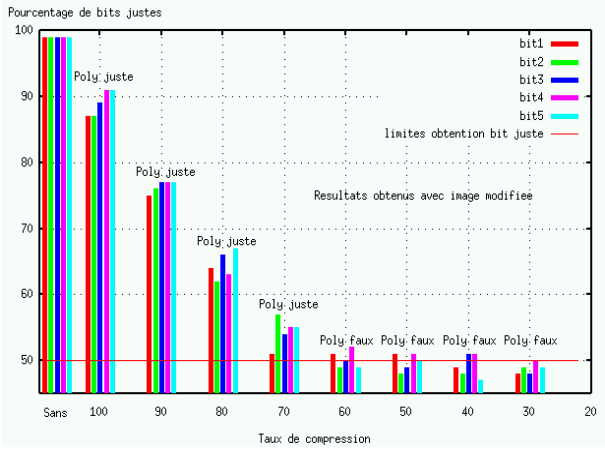


Figure 4 – *Obtention du polynome générateur en fonction du facteur de qualité.*

aux TEB différents. Pour une image de taille 715×582 transmise par un réseau classique (TEB de 10^{-4}), P vaut 90%. A partir d'un TEB de 10^{-6} la probabilité d'avoir un bit faux pendant la transmission d'un message de 800 bits est quasi nulle. Par conséquent, les erreurs engendrées par le support de transmission n'ont qu'un faible impact sur notre tatouage, bien moindre que celui provoqué par la compression.

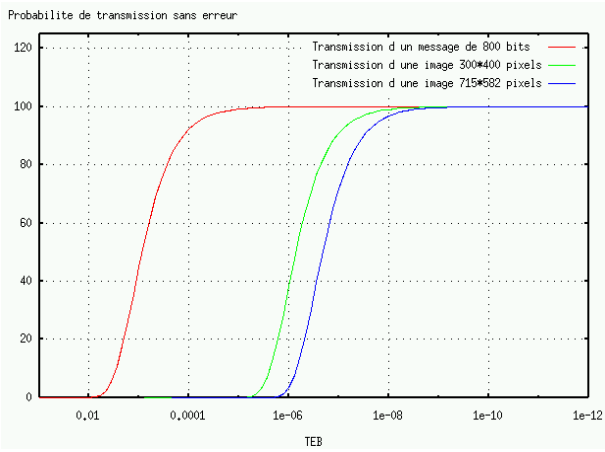
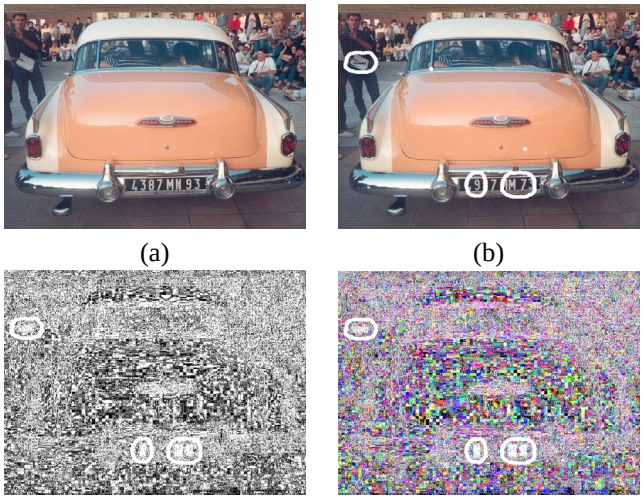


Figure 5 – *Probabilité de transmission d un message sans erreur en fct du TEB.*

Attaques. La figure 6.b montre les attaques subies par l'image orignale figure 6.a. Que ce soient pour le tatouage ou pour les attaques, les modifications doivent rester indécelables pour le SVH. La figure 7 illustre le PSNR entre le plan rouge de l'image originale et le plan rouge de l'image tatouée, falsifiée et comprimée avec différents facteurs de qualité. L'image différence pour un facteur de qualité de 80% est illustrée figure 6.c pour le plan rouge et figure 6.d pour l'image couleur.
Du fait de leur nature, ces attaques ne modifient donc que localement le message tatoué. Or, le message tatoué est re-

dondant, les mêmes informations sont tatouées un grand nombre de fois. Par conséquent, seuls quelques messages unitaires sont modifiés par les attaques et les informations peuvent donc être récupérées.



(a) (b)

(c) (d)

Figure 6 – *a) Image originale, b) Image originale tatouée et comprimée avec un facteur de qualité de 80 %, c) Image différence entre le plan rouge original et celui comprimée à 80 % d) Image différence entre l'image originale et l'image comprimée à 80 %*

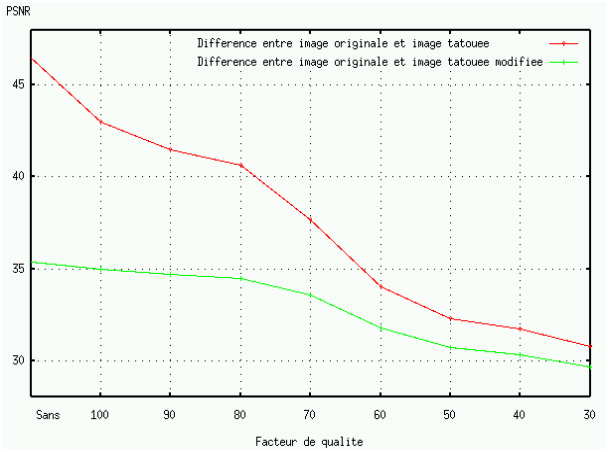


Figure 7 – *PSNR calculé pour le plan rouge.*

A partir de l'image figure 6.a, sur le plan bleu, le polynôme générateur de 5 bits est inséré 804 fois. Comme l'image est falsifiée, certains bits sont erronés. Cependant le pourcentage de bits faux reste faible (1 à 2 %). Par une méthode de vote bit à bit, nous sommes capables de restituer la bonne valeur du polynôme générateur. A partir de ce polynôme, grâce au CCE, nous détectons, sur les plans rouge et vert, un message dégradé suite à la falsification de l'image. En effet, sur le plan rouge, figure 6.c, le message original $4387MN931708281002$ est inséré 66 fois. Grâce au CCE, nous détectons des erreurs sur 7 messages, illustrées tableau 2. Ces messages sont donc localisés sur les deux zones ayant subi des attaques.

Indice	Message falsifié
16	4387MN931708271002
17	4387MN931703481002
52	4387MK431708281002
53	4387L18B0321I34040
54	438959V93170828100
55	4313293N9317082810
56	45K93N931708281002

Tableau 2 – *Messages faux détectés sur le plan rouge.*

4 Conclusion

Nous avons présenté une méthode de tatouage spatial d'images couleurs résistant aux perturbations que peut subir une image au cours du transfert. Cette robustesse est due à l'ajout d'un CCE dans le message ainsi qu'à l'utilisation des 3 plans couleur. De plus, nous montrons comment cette méthode peut aussi résister à la compression, nécessaire pour le transfert. Comme nouveaux axes de recherches, nous envisageons d'une part de nous appuyer sur le contenu de l'image pour insérer le message mais aussi de décomposer l'image dans d'autres espaces couleurs.

Références

[1] F. Deguillaume, S. Voloshynovskiy, et T. Pun. Hybrid robust watermarking resistant against copy attack. Dans *EUSIPCO'02, Toulouse, France*, 2002.

[2] Macq et Dugelay. Technologies du tatouage pour l'authentification et la protection des images. *Annales des télécommunications*, 2000.

[3] W. Puech et M. Dumas. Transfert sécurisé d'images par combinaison de techniques de cryptographie et de tatouage. Dans *CORESA'01, Dijon, France*, 2001.

[4] W. Puech, P. Montesinos, et M. Dumas. Color Image Watermarking Robust to JPEG Compression. Dans *Proc. 1^{st} European Conference on Color in Graphics, Imaging and Vision (CGIV-02), Poitiers, France*, pages 81–85, Apr. 2002.

[5] G. Chareyron et A. Tremeau. Watermarking of color images based on a multi-layer process. Dans *CGIV'02, Poitiers, France*, pages 77–80, 2002.

[6] M. Maiman. *Télécoms et réseaux*. Masson, Paris, 1997.

[7] A. Guyader, E. Fabre, et C. Guillemot. Robust decoding of vlc encoded markov sources. Dans *GRETSI'01, Toulouse, France*, 2001.