Théorie de l'information
Suivi de projet
Stéganographie dans les images

Gautier Darchen
Alexandre Huat
Romain Judic

7 novembre 2016

---

1 Avancement du projet

1.1 Définition de la stéganographie

La stéganographie permet de dissimuler un message (dit secondaire) dans un autre (dit primaire) tout en laissant le message primaire lisible de tous. Le message secondaire, lui, ne devra être lisible que par une personne possédant une information spéciale comme une clé ou une méthode d'extraction du message secondaire.

Il existe la stéganographie textuelle et la stéganographie dans les images. La stéganographie textuelle est très facile à déceler car elle n'offre pas vraiment d'autre choix que générer un texte incompréhensible, dont on comprend facilement qu'il cache quelque chose. La stéganographie dans les images est beaucoup plus efficace et il existe de très nombreuses méthodes pour cacher, extraire ou déceler un message dans une image[1].

1.2 Exemples de méthodes de stéganographie

Il existe plusieurs méthodes de stéganographie dans les images, nous en avons abordé trois :
— la stéganographie par substitution ;
— la stéganographie par étalement de spectre ;
— la stéganographie dans le domaine transformé.

1.2.1 Stéganographie par substitution de LSB *(LSB Replacement)*[2–4]

Définition

La stéganographie par substitution de *LSB* (*Least Significant Bit*) – dans l'exemple de la stéganographie au travers d'une image – consiste à substituer les bits de poids faibles (les *LSB*) des pixels de l'image originale par les bits du message que l'on souhaite insérer. À la réception de l'image, le destinataire du message caché doit savoir au préalable dans quel sens parcourir les pixels pour retrouver le message (usuellement, parcours pseudo-aléatoire choisi, avec une clé secrète k).

Exemple

Message (M) : $M = 11001000$

Traitement de l'image en niveau de gris :
On découpe le message M=**1 1 0 0 1 0 0 0**

00110100	11001010	01101001	11101101
10000010	10100100	00101101	10111011

TABLE 1 – Image originale en niveaux de gris

00110101	11001011	01101000	11101100
10000011	10100100	00101100	10111010

TABLE 2 – Image modifiée en niveaux de gris

Application

On utilise un programme Matlab permettant de réaliser de la stéganographie par substitution de *LSB*. On fournit à ce programme deux images carrées de dimension similaires : l'une des images est la *cover* (l'image dans laquelle on veut dissimuler un message), la seconde est l'image à cacher. Le programme transforme ensuite ces images en niveaux de gris. On choisit également le nombre de bits à substituer.

Voici un exemple d'application. La stéganographie est ici réalisée par substitution d'un seul bit : le bit de plus faible poids.

FIGURE 1 – Image de base (*cover*)

FIGURE 2 – Image à dissimuler

FIGURE 3 – Image stéganographiée

FIGURE 4 – Image extraite de la stéganographie

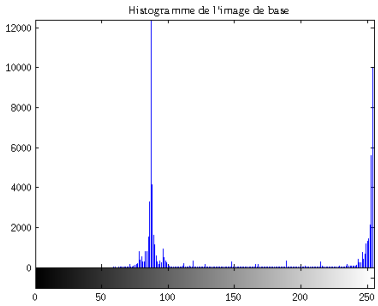

FIGURE 5 – Histogramme de l'image *cover*

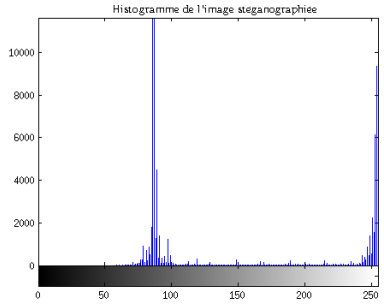

FIGURE 6 – Histogramme de l'image stéganographiée

Commentaires

Sur la figure 3, on ne voit pas à l'œil nu qu'un message est dissimulé. Pourtant, on voit bien sur la figure 4 qu'un message caché a pu être extrait de l'image stéganographiée. Ce message caché est même récupéré sans trop de distorsion. Le programme nous renvoie les résultats suivants pour le PSNR [1] et l'EQM [2] :

$$EQM = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \big(I_1(i,j) - I_2(i,j)\big)^2 = 1.39 \times 10^4$$

où I_1 représente l'image originale à dissimuler, I_2 est l'image dissimulée récupérée après la stéganographie, m est la hauteur des images et j est la largeur des images. L'EQM est relativement élevée puisqu'elle compare chaque pixel entre les deux images, et qu'ici les pixels sont modifiés, bien que très peu puisqu'on ne change que le bit de poids faible de certains des pixels, mais modifiés tout de même.

$$PSNR = 10 \cdot \log_{10}\left(\frac{d^2}{EQM}\right) = 10.6027$$

où d est la dynamique du signal, donc ici la valeur maximale qu'un pixel peut avoir, soit $d = 255$ dans notre cas (pixels codés sur 8 bits).

Enfin on voit sur les figures 5 et 6 que les histogrammes sont grossièrement identiques, ce qui est logique. En effet, seul le bit de plus faible poids est modifié ici. Ce bit est donc celui qui apporte le moins d'information sur chacun des pixels. Sa modification n'a donc pas un impact grave sur le pixel original.

Critique de cette méthode

Avantage Facile à implémenter et calculs de complexité relativement faible.

Inconvénient Assez facilement repérable et attaquable (attaque du χ^2) car, bien que peu visible à l'œil nu, la distribution statistique du support est relativement altérée.

1.2.2 Stéganographie par étalement de spectre *(SSIS : Spread Spectrum Image Steganography)*[5, 6]

Définition

La technique d'étalement de spectre consiste à dissimuler le message dans un bruit de même taille que l'image *cover* et à l'additionner à cette dernière. La modulation du message par le bruit permet d'étaler son spectre, c'est-à-dire de le rendre moins facile à détecter car ne présentant plus de motifs

1. *Peak Signal to Noise Ratio.*
2. Erreur Quadratique Moyenne.

distincts. On va utiliser un bruit de très faible puissance par rapport à celle de l'image. De cette manière, en additionnant ces deux derniers, l'image ne sera pas altérée visuellement.

Insertion

- On dispose du message m et de la *cover* x de taille n
- On génère, grâce à une clé secrète, un bruit de taille n et de faible puissance par rapport à celle de x (la clé sera transmise au destinataire de l'image tatouée)
- On module le message m par le bruit puis on l'étend spatialement (en le répliquant par exemple) $\rightarrow$ on obtient un signal m_b de taille n
- On additionne pour obtenir w le signal à envoyer : $w = x + m_b$

Extraction

Pour récupérer le message m, le destinataire doit posséder la clé de génération du bruit. On doit disposer de techniques de restauration d'images pour continuer.

- À partir de w, le décodeur produit une estimation $\hat{x}$ de l'image initiale
- $(w - \hat{x})$ correspond à la différence (estimée) entre l'image initiale et le signal reçu, c'est-à-dire à une estimation $\hat{m_b}$ du message bruité
- Grâce à la connaissance de la clé, on peut générer le bruit b et donc démoduler une estimation du message $\hat{m}$

Exemple simple

Pour illustrer la partie sur la modulation du message, soit m un message bilatéral ($m_i \in \{-1, +1\}$) et b un bruit gaussien b généré grâce à une clé k (par exemple $k = \sigma$).
Phase d'insertion : on assigne simplement au bruit le signe du message à dissimuler.

$$w = m \times b$$

Phase d'extraction : Après avoir identifié la partie correspondant au bruit sur l'image reçue, un simple examen des signes de m_b permet de retrouver le message.

$$\hat{m} = signe(m_b)$$

Critique de cette méthode

Avantages Le tatouage est complètement invisible et difficilement décelable par analyse informatique.

Inconvénients L'extraction du message dissimulé nécessite la connaissance de techniques d'étalement spatial (pour donner au message la même taille que l'image) et de restauration d'image relativement complexes à mettre en œuvre.

1.2.3 Stéganographie dans le domaine transformé[7, 8]

Introduction

Cette technique de stéganographie consiste à intégrer l'information secrète dans un domaine transformé du signal. Dans une image, on distingue le domaine spatial, basé sur les pixels, et son domaine transformé qui est celui des fréquences. Les techniques de stéganographie sur le domaine transformé utilisent la transformée orhtognale de l'image (exemple : transformée de Fourier discrète) plutôt que l'image elle-même. La transformée orthogonale ayant donc deux composantes, la magnitude et la phase.

Nous ne présentons ici qu'une des méthodes utilisées dans le domaine transformé : l'utilisation de la transformée d'ondelettes discrète (DWT, pour *Discrete Wavelet Transform*).

Transformée d'ondelettes discrète (DWT)

La DWT permet une décomposition hiérarchique d'une image. Elle se base sur l'utilisation d'ondelettes qui sont de fréquences et durées variables. Ces ondelettes permettent à la fois une description spatiale et fréquentielle de l'image : la DWT indique quelle fréquence apparaît, où, et sur quelle surface. La transformée en ondelettes détecte les zones riches en informations (à fort contraste) et les sépare. Une ondelette est une fonction de valeur moyenne nulle et limitée dans le temps. Les ondelettes sont générées par des translations, compressions et dilatations d'une ondelette mère.

L'application de la DWT, consiste à filtrer l'image dans les deux dimensions (filtrage vertical, horizontal et diagonal). Ces filtres décomposent l'image en 4 parties (sous-bandes) de résolution inférieure. Ces sous-bande sont sans chevauchement et ont différentes résolutions, on les nomme LL, LH, HL et HH. La sous-bande LL correspond aux coefficients de corrélation déterminés par une fonction d'ondelette dilatée jouant le même rôle qu'un filtre passe bas. Les autres sous bandes montrent les valeurs déterminées par la fonction d'ondelette mère compressée, faisant office de filtres passe haut. On peut appliquer plusieurs DWT à la suite, on le fait alors sur la sous-bande LL. Après N DWT on se retrouve ainsi avec $3N + 1$ sous-bandes.

Par sa capacité à bien représenter les fréquences dans l'espace, la DWT est très efficace pour la stéganographie. En effet, la plus grande quantité d'énergie dans l'image est stockée dans les basses fréquences (sous-bande LL_N). Ainsi, cacher un message en basse fréquence altérerait beaucoup la qualité de l'image et serait facilement décelable, même si cela serait plus robuste. Par conséquent, cacher un message dans les hautes fréquences (sous-bandes LH_X et HL_X) serait bien plus discret car l'œil humain remarque difficilement les changements dans les contours.

FIGURE 7 – Exemple de deux DWT successives (sur l'image du milieu : LL en haut à gauche, LH en bas à gauche, HL en haut à droite, HH en bas à droite)

Algorithme générique d'implantation et d'extraction d'un message

Implantation d'un message secret

1. Étudier l'image et le message secret (texte/image) pour trouver la meilleure manière de le cacher.
2. Transformer le message en fichier binaire s'il ne l'est pas encore. Réaliser une DWT sur l'image de couverture.
3. Déterminer les coefficients de filtrage dans les directions verticale et horizontale (LH et HL). Cacher les bits du message dans ces coefficients (remplacement).
4. Créer la stego-image (par transformée inverse IDWT).

Extraction d'un message secret

1. Étudier la stego-image pour savoir comment a pu être dissimulé le message.
2. Calculer la DWT et extraire les coefficients de filtrage verticaux et horizontaux.
3. Reconstruire le message bits par bits à partir des coefficients.
4. Recomposer le message compréhensible par l'humain.

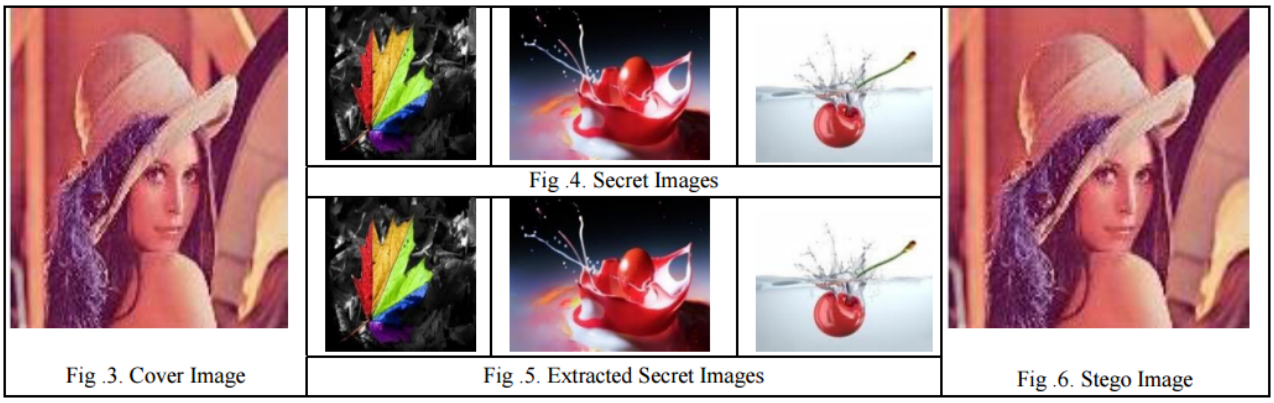

FIGURE 8 – Exemple de stéganographie avec une DWT : implantation de trois images secrètes dans une seule en utilisant les trois canaux RGB[9]

Commentaire

La DWT est une des transformations les plus robustes et les plus efficaces pour la stéganographie dans le domaine transformé. Elle ne permet pas de cacher un gros volume de données mais assure une forte invisibilité du message, une forte robustesse contre les traitements d'image ultérieurs et permet une faible détérioration du message à l'extraction. Elle est souvent présentée comme la méthode la plus sûre pour la stéganographie dans le domaine transformé.

2 Répartition des tâches

Gautier : stéganographie par substitution de LSB (voir code Matlab).

Romain : stéganographie par étalement de spectre (SSIS).

Alexandre : stéganographie dans le domaine transformé.

3 Suite envisagée du projet

— S'intéresser aux techniques de détection de message stéganographiés et de comparaison de méthodes de stéganographie.
— Coder des exemples de stéganographie.

Références

[1] G. U. C. P. Sumathi, T. Santanam, "A study of various steganographic techniques used for information hiding," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 4, pp. 9–25, décembre 2013.

[2] U. M. . S. e. T. Sarra Kouider, "Stéganographie et stéganalyse." `https://www.lirmm.fr/~wpuech/enseignement/master_informatique/Compression_Insertion/Dissimulation_de_donnees_Cours3.pdf`. Consulté le 6 novembre 2016.

[3] zathuros, "La stéganographie par substitution." `https://histoiresecretes.wordpress.com/2013/05/05/la-steganographie-par-substitution/`, mai 2013. Consulté le 6 novembre 2016.

[4] M. Weiss, "Principles of steganography." `http://www.math.ucsd.edu/~crypto/Projects/MaxWeiss/steganography.pdf`. Consulté le 6 novembre 2016.

[5] M. Fortini, "Patchwork." `http://www.lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti98/Fortini/patchwork.html`. Consulté le 6 novembre 2016.

[6] J. C. T. R. Lisa M. Marvel, Charles G. Boncelet, "Methodology of spread-spectrum image steganography," tech. rep., Army Research Laboratory, juillet 1998.

[7] U. K. Sudhanshi Sharma, "Review of transform domain techniques for image steganography," *International Journal of Science and Research (IJSR)*, vol. 4, mai 2015.

[8] F. L. Sang, "La compression par ondelettes (dwt)." `http://etud.insa-toulouse.fr/~flone_sa/BEmultimedia/index.php?Dwt`, février 2010. Consulté le 6 novembre 2016.

[9] G. A. E. G. N. R. M. Della Baby, Jitha Thomas, "A novel dwt based image securing method using steganography," *Procedia Computer Science*, vol. 46, pp. 612–618, 2015.