Projet de Théorie de l'Information

Stéganographie dans les images

Gautier Darchen, Alexandre Huat, Romain Judic

INSA Rouen
ASI4

12 décembre 2016

Sommaire

1. Stéganographie
   - Stéganographie par substitution de LSB
   - SSIS : Spread Spectrum Image Steganography
   - Stéganographie dans le domaine transformé
2. Stéganalyse
3. Applications

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES ROUEN

Stéganographie par substitution de LSB (1/5)

Définition

- LSB : *Least Significant Bit*
- LSB (pixels) de l'image substitués par bits du message à insérer
- Destinataire connaît le sens de lecture de l'image pour déchiffrer le message

Exemple

Message (M) : $M = 11001000$

00110100	11001010	01101001	11101101
10000010	10100100	00101101	10111011

Table – Image originale en niveaux de gris

Stéganographie : M=**1 1 0 0 1 0 0 0**

0011010**1**	1100101**1**	0110100**0**	1110110**0**
1000001**1**	1010010**0**	0010110**0**	1011101**0**

Table – Image modifiée en niveaux de gris

Stéganographie par substitution de LSB (2/5)

Programme utilisé

- Code *Matlab*
- Deux images en entrée :
  - *cover* : image dans laquelle on dissimule un message
  - l'image à cacher
- Transformation des images en niveaux de gris (pixels codés sur un octet)
- Nombre de bits à substituer choisi par l'utilisateur

Stéganographie par substitution de LSB (3/5)

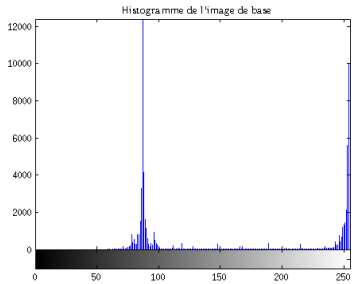
Application

Image de base (*cover*)

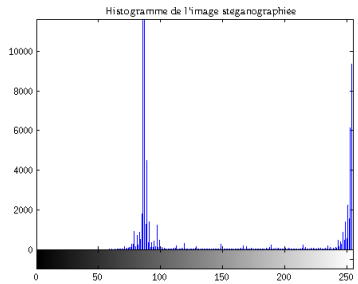
Image à dissimuler

Image stéganographiée

Image extraite de la stéganographie



Histogramme de l'image *cover*



Histogramme de l'image stéganographiée

Stéganographie par substitution de LSB (4/5)

Commentaires (1/2)

- Difficile de voir à l'œil nu qu'un message est dissimulé
- Message récupéré sans trop de distorsion
- $$EQM = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(I_1(i,j) - I_2(i,j) \right)^2 = 1.39 \times 10^4$$

  avec
  - I_1 : l'image originale à dissimuler
  - I_2 : l'image dissimulée récupérée après stéganographie
  - m et j : resp. hauteur et largeur des images.

  L'EQM est relativement élevée car
  - faible distance entre pixels
  - bit de plus faible poids changé ou non pour chaque pixel

  $\Longrightarrow$ nombre de pixels différent entre les deux images (EQM) élevé

Stéganographie par substitution de LSB (5/5)

Commentaires (2/2)

- PSNR : *Peak Signal to Noise Ratio*

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

avec

- d : la dynamique du signal $\iff$ valeur maximale qu'un pixel peut avoir
  - $d = 255$ dans notre cas (pixels codés sur 8 bits)

- Histogrammes grossièrement identiques $\iff$ information de chaque pixel peu modifiée

Critique de la substitution de LSB

Avantage	Facile à implémenter et complexité de calculs faible
Inconvénient	Facilement repérable et attaquable (attaque du χ^2) car distribution statistique du support altérée

SSIS : Spread Spectrum Image Steganography (1/4)

Définition

- Dissimuler le message dans un bruit de faible puissance et de même dimension (spatiale) que l'image *cover*
- Le spectre (fréquentiel) du message est "étalé" $\Longrightarrow$ ses motifs spatiaux ne sont plus visibles à l'oeil nu

Algorithme - Insertion

1. Soit un message m (chiffré ou non) et une *cover* f
2. Générer, avec une clé k, un bruit pseudo-aléatoire n
3. Étaler spatialement m
4. Moduler le bruit n par le message m $\Longrightarrow$ s
5. Additionner la *cover* f et le signal s obtenu : $f + s = g$

SSIS : Spread Spectrum Image Steganography (2/4)

Algorithme - Extraction

1. Soit g l'image stéganographiée
2. On calcule une estimation $\hat{f}$ de l'image initiale
3. On calcule $\hat{s}$ l'estimation de s : $\hat{s} = g - \hat{f}$
4. On génère à nouveau le bruit n avec la clé k
5. On démodule une estimation $\hat{m}$ du message

Exemple : modulation par un bruit

$\rightarrow$ m est une image NB

$\rightarrow$ $m = [1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1]$

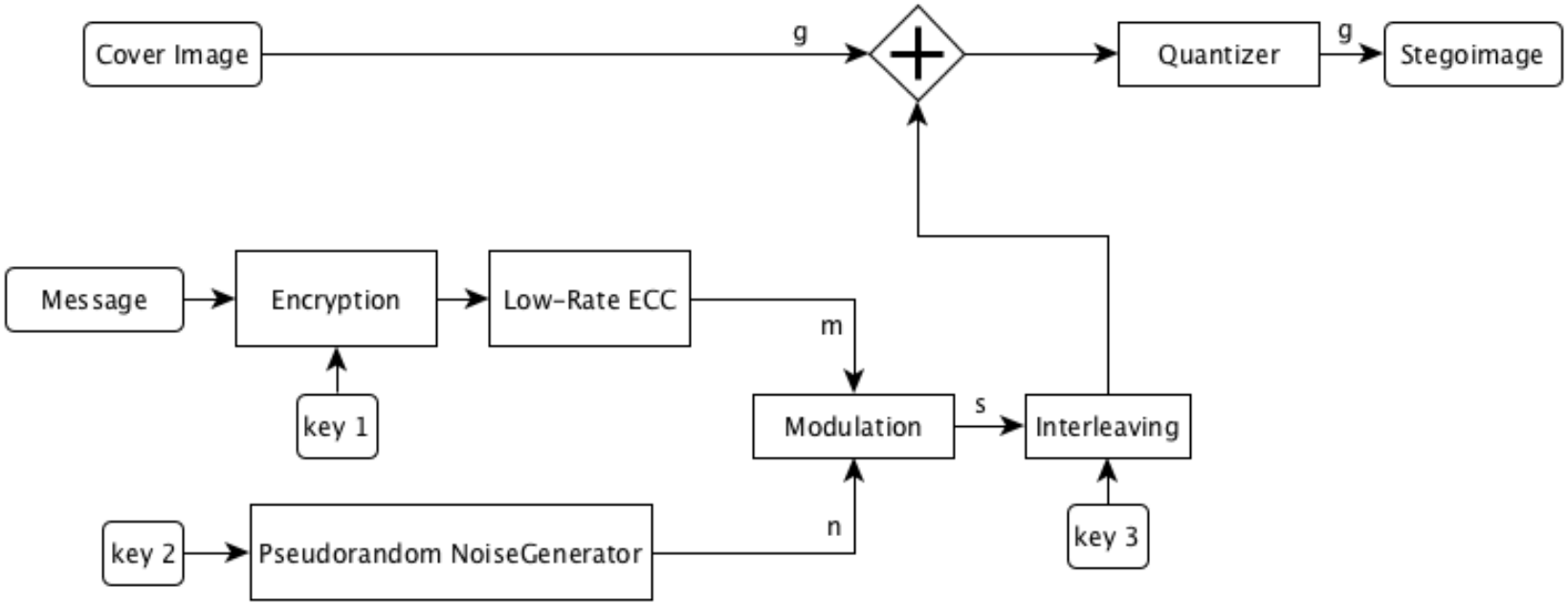
$\rightarrow$ $n = [a \quad b \quad c \quad d \quad e \quad f \quad g]$

$\rightarrow$ On applique le signe de m sur n :

$s = [a \quad -b \quad -c \quad d \quad e \quad f \quad -g]$

SSIS : Spread Spectrum Image Steganography (3/4)

Insertion dans la vraie vie



Algorithme d'insertion de l'Army Research Laboratory

SSIS : Spread Spectrum Image Steganography (4/4)

Critique de la méthode Spread Spectrum

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

Inconvénient Besoin d'un décodeur pour estimer l'image *cover* initiale
$\Longrightarrow$ difficile à mettre en place

Stéganographie dans le domaine transformé (1/5)

Principe

Cacher l'information dans le domaine transformé de l'image (domaine fréquentiel au lieu du domaine spatial)

Différentes méthodes

- Jsteg (Derek Upham, 1998) : LSB sur les coefficients de la transformée en cosinus discrète (DCT)
- F5 (Westfeld, 2001) : générer des nombres pseudo-aléatoires avec une clé k déterminant quel *chemin* suivre pour l'insertion/extraction des bits dans la DCT puis insertion avec un codage de Hamming.
- Utilisation de la **transformée en ondelettes discrète (DWT)** (démonstration).

Stéganographie dans le domaine transformé (2/5)

Exemple avec la DWT

La transformée en ondelettes

Analogue à la transformée de Fourier : la TF décompose le signal en sinus, la DWT en ondelettes. Une ondelette est une fonction arbitraire Φ vérifiant :

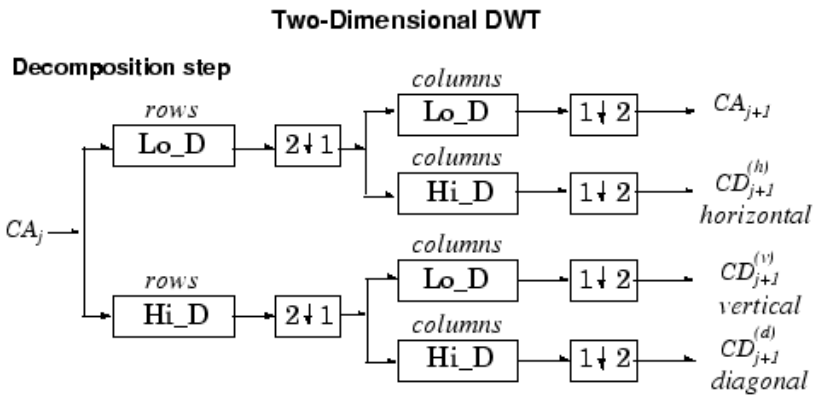
$$\iint_{\mathbb{R}^2} \frac{|\Phi(k)|^2}{\|k\|^2} dk < +\infty$$

On génère une famille d'ondelette par dilatation (coef a), translation (vecteur b) et rotation (angle θ) de l'ondelette mère Φ. D'où la transformée en ondelette :

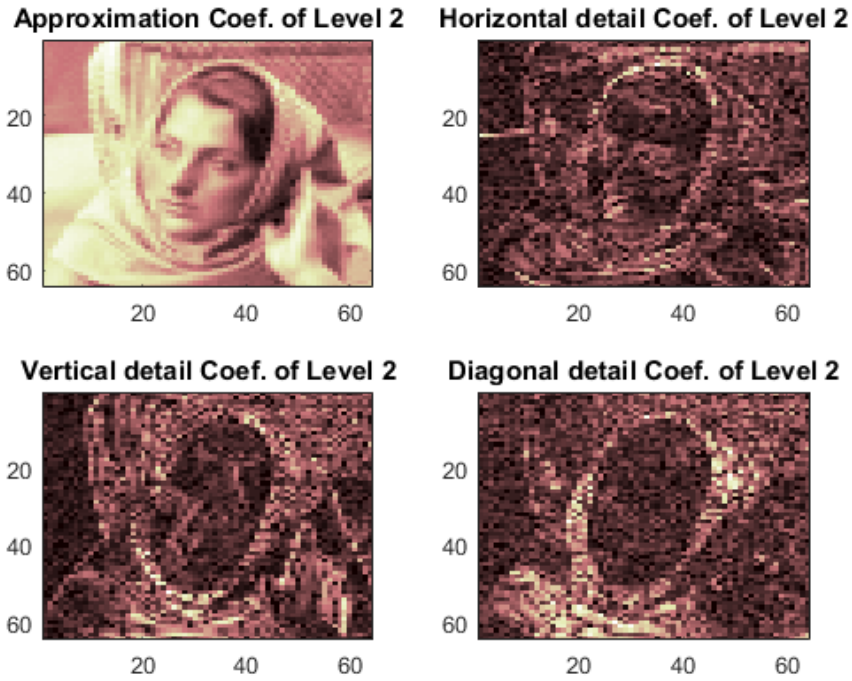
$$Wf(a,b,\theta) = \iint_{\mathbb{R}} f(x)\Phi^*_{(a,b,\theta)} dx$$

Stéganographie dans le domaine transformé (3/5)

Exemple avec la DWT : Et en pratique ?



Etapes de décomposition de la DWT



Exemple de décomposition de la DWT

Stéganographie dans le domaine transformé (4/5)

Exemple avec la DWT

Implémentation

1. Analyser la cover-image (payload, contours), faire des pré-traitements (contraste, luminosité, gamma, etc.).
2. Calculer la DWT.
3. Choisir un chemin d'implantation (connu de l'autre partie) : insérer les bits dans les hautes fréquences (i.e. matrices $\neq CA$).
4. Implanter le message (mix avec une autre technique de stegano possible).
5. Construire la stego-image (DWT inverse).
6. Envoyer le message !

Pour retrouver le message : faire le chemin inverse évidemment.

Stéganographie dans le domaine transformé (5/5)

Exemple avec la DWT

Commentaires

- Robuste à la compression et aux stéganalyses
- Faible payload
- Reconstruction de bonne qualité

Stéganalyse (1/5)

Définition (1/2)

- But : détecter si une image est susceptible de contenir des informations dissimulées par stéganographie
  - Identifier les messages suspects
  - Déterminer s'ils contiennent un message caché
  - Et si possible le décoder
- Discipline duale de la stéganographie
- Difficulté réside dans le fait qu'on ne sait pas si un message est dissimulé ou non
- Différent de la cryptanalyse où on est sûr qu'un message est caché
- Si un message est dissimulé, distribution statistique de l'image certainement altérée
- Problèmes très souvent liés aux distributions statistiques du support des images à analyser

Stéganalyse (2/5)

Définition (2/2)

- Il existe 3 types de stéganalyse :

  Stéganalyse passive Détecter la présence d'un secret.
  Stéganalyse active Détecter puis détruire le secret.
  Stéganalyse malicieuse Détecter le message, comprendre l'algorithme de stéganographie et l'extraire pour ses propres fins.

Stéganalyse d'un message dissimulé par substitution de LSB

- Stéganographie invisible à l'œil nu
- Modification des LSB d'une image $\Longrightarrow$ variations entre les pixels voisins de l'image

Si information dissimulée dans les LSB d'une image
Alors histogramme de l'image non uniforme

Stéganalyse (3/5)

Application à LSB (1/2) (démonstration)

- Message dissimulé sur les bits de poids faibles

  $\Longrightarrow$ la parité des pixels est modifiée

- On parcourt l'image à analyser et on met tous les pixels pairs à 0 (noir en RGB) et tous les pixels impairs à 255 (blanc)
- Cela met en évidence les pixels modifiés par un possible message caché

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES ROUEN

Stéganalyse (4/5)

Application à LSB (2/2)

3. Image steganographiee

Image à analyser

2. Image analysée

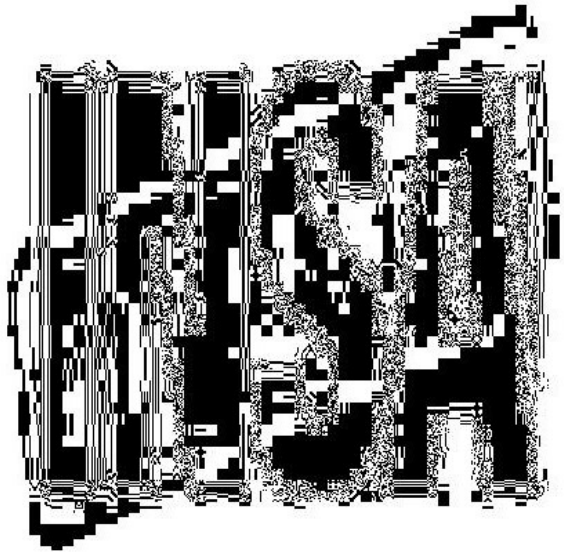


Image révélée

Stéganalyse (5/5)

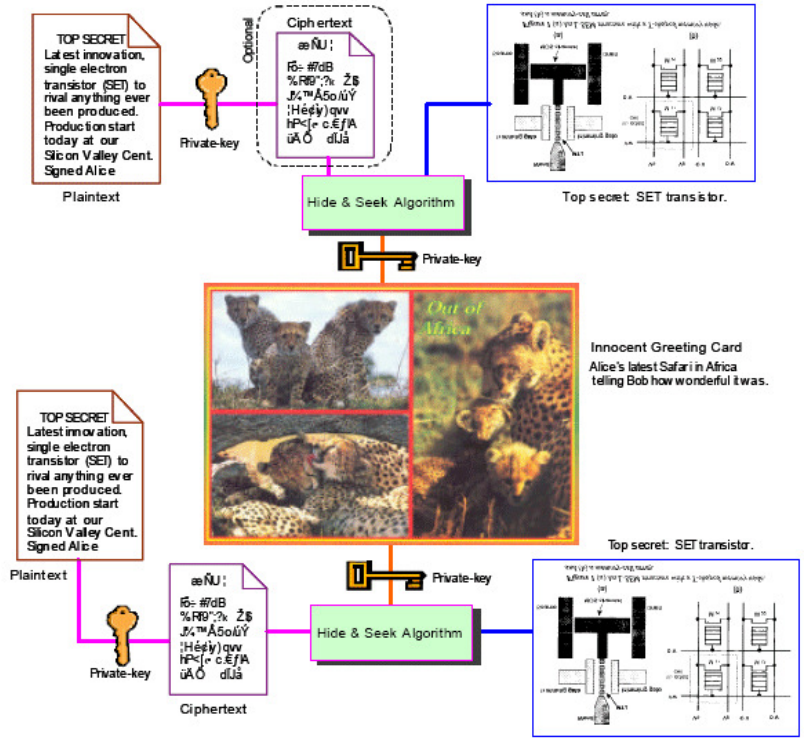
Détection par machine learning

1. Obtenir une grande BD d'images.
2. Séparer les images sur différents ilôts (méthode K-means)
3. Chaque ilôt est associé à un classifieur (le classifieur décide si l'image est cover ou stego). Classifieur au choix (SVG, Average Perceptron, EFLDFS etc.)
4. Apprentissage puis test

Résultats avec un classifieur EFLDFS : $>$ 95% de réussite avec 150 000 images !

Applications

- Tatouage numérique invisible
- Transmission de données confidentielles dans l'industrie nucléaire
- Echange de données militaires ou d'espionnage



Références I

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), 4(6) :9–25, décembre 2013.

G. A. E. G. N. R. M. D. Baby, J. Thomas. A novel dwt based image securing method using steganography. Procedia Computer Science, 46 :612–618, 2015.

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

M. C. J. Pasquet, S. Bringay. Des millions d'images pour la stéganalyse : inutile ! In CORESA2013, COmpression et REprésentation des Signaux Audiovisuels, nomvembre 2013.

J. C. T. R. L. M. Marvel, C. G. Boncelet. Methodology of spread-spectrum image steganography. Technical report, Army Research Laboratory, juillet 1998.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES ROUEN

Références II

D. MATLAB®. dwt2 : Single-level discrete 2-d wavelet transform. https://fr.mathworks.com/help/wavelet/ref/dwt2.html?searchHighlight=dwt2&s_tid=doc_srchtitle, 2016. Consulté le 6 décembre 2016.

V. Perrier. Application de la théorie des ondelettes. http://www-ljk.imag.fr/membres/Valerie.Perrier/PUBLI/Cours2-VP.pdf, mars 2005. Consulté le 10 novembre 2016.

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

U. K. S. Sharma. Review of transform domain techniques for image steganography. International Journal of Science and Research (IJSR), 4 :194–197, mai 2015.

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.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES ROUEN

Références III

M. Weiss. Principles of steganography. http://www.math.ucsd.edu/~crypto/Projects/MaxWeiss/steganography.pdf. Consulté le 6 novembre 2016.