Utilisation d'algorithmes adaptatifs pour la stéganographie/stéganalyse

Lambert ROSIQUE

Soutenance de stage

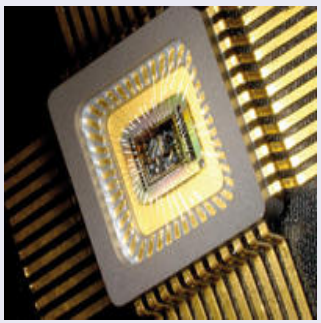
19 septembre 2013

LIRMM

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM
UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES
cnrs
dépasser les frontières

Départements

Informatique



Micro-électronique

Robotique

Quelques Chiffres

$\sim$ 400 personnes (permanents, doctorants...)

$\sim$ 60 stagiaires (M1 et M2)

$\sim$ 300 publications/an

- Partenariats industriels (Alcatel, Thalès, STMicroelectronics, EDF...)

- Création de logiciels, d'équipements (robots, cartes Arduino...)

Le Stage

Le Cadre

1) Intitulé : Codes Correcteurs et Stéganographie Adaptative

2) Encadrants : Anne Elisabeth Baert (équipe MAORE), Marc Chaumont (équipe ICAR) et Eleonora Guerrini (équipe ECO)

3) Durée : du 4 mars au 26 juillet 2013 (5 mois)

4) Domaine : Codes correcteurs, Stéganographie, Image...

Codes correcteurs et stéganographie adaptative

Objectifs du stage : Concevoir des algorithmes adaptatifs performants basés sur les codes correcteurs, les analyser et les évaluer pour des problèmes de stéganographie/stéganalyse.

Travail demandé :

1- Contexte stéganographique

2- Codes correcteurs (approches non-adaptatives)

3- Code de Filler : STC (Syndrome-Trellis Code, 2011) et Pevny HUGO (2010)

4- Algorithmes adaptatifs ? Performances ?

Problématique

STC meilleur code existant (complexité calculatoire $O(2^h n)$)

Unique algorithme adaptatif (performances)

De nombreux choix empiriques et questions ouvertes :

1) Choix de la sous-matrice (des 1 sur la 1ère et la dernière ligne)

2) Pas de colonnes identiques (sous-matrice)

3) Optimiser pour un profil de distortion = optimisé pour tous

4) Peut-on augmenter la taille des cosets ?

5) Comment choisir les matrices ?

Mon approche

1- Découvrir la stéganographie

2- En apprendre davantage sur les Codes Correcteurs (convolutifs)

3- Poser clairement le problème (algèbre linéaire)

4- Ecrire un programme pour simuler des insertions de messages avec diverses matrices...

5- ... pour anticiper les résultats et répondre aux problématiques

Définitions

Stéganographie

Dissimulation d'un message dans un media (image, vidéo, son...)

Code linéaire

Correction d'erreurs après la transmission d'un message grâce à de la redondance. Sous-espace vectoriel de $\mathbb{F}_2^n$

Carte de détectabilité

A chaque pixel on attribue une valeur qui dépend de sa sensibilité à la détection en cas de modification

Introduction

***Le problème des prisonniers* [1]**

[1] G. J. Simmons. The prisoner's problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptography, CRYPTO'83*, pages 51-67, Santa Barbara, CA, August 22-24,1983. New York: Plenum Press.

Introduction

***Le problème des prisonniers* [1]**

[1] G. J. Simmons. The prisoner's problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptography, CRYPTO'83*, pages 51-67, Santa Barbara, CA, August 22-24,1983. New York: Plenum Press.

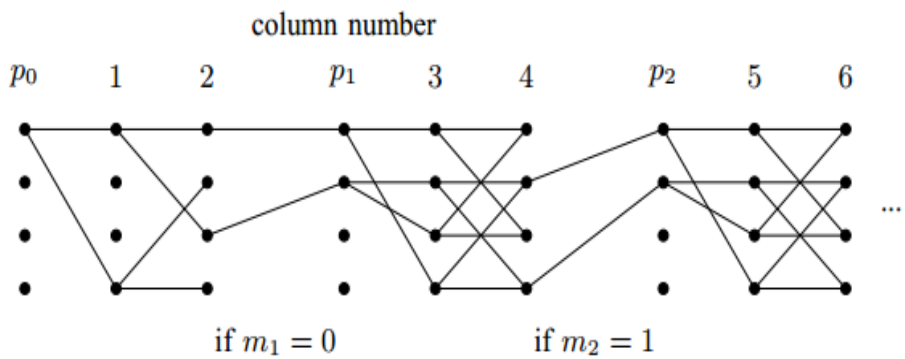
Syndrome-Treillis Code

STC

Algorithme qui résout le problème $\mathbb{H}\mathbf{v} = \mathbf{m}$ avec $\mathbf{v} \cdot \rho$ minimal, grâce à l'algorithme de Viterbi

6

$$\hat{\mathbb{H}} = \begin{pmatrix} 1\,0 \\ 1\,1 \end{pmatrix} \qquad \mathbb{H} = \begin{pmatrix} 1\,0 & & & \\ 1\,1\,1\,0 & & & \\ & 1\,1\,1\,0 & & \\ & & 1\,1 & \\ & & & \ddots\,1\,0 \\ & & & & 1\,1\,1\,0 \end{pmatrix}$$



Nouvelle approche

Objectif : Reformulation

Approche : $\mathbf{Av} = \mathbf{m}$

Echelonnement de $\mathbf{A} \Longrightarrow \mathbf{TA} = \mathbf{H}$

D'où $\boxed{\mathbf{Hv} = \mathbf{Tm}}$ $(\star)$

- $\mathbf{T} \in \mathrm{SL}(\mathbb{F}_p)$
- Exemple matrice échelonnée :

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Intérêt : On a facilement $\ker(\mathbf{H}) := \{\mathbf{u}, \mathbf{Hu} = \mathbf{0}\}$

Problème : lien $\boxed{\mathbf{Hv} = \mathbf{Tm}}$ $(\star)$ et $\ker(\mathbf{H})$?

Si $\mathbf{v}_0$ solution particulière de $(\star)$ alors

$\mathbf{Hv}_0 = \mathbf{Tm} \Longrightarrow \mathbf{H}(\mathbf{v} + \mathbf{v}_0) = \mathbf{0} \Longrightarrow (\mathbf{v} + \mathbf{v}_0) \in \ker(H)$

Donc si $\ker(\mathbf{H}) =< (\mathbf{u}_i) >$ et $\mathbf{Av} = \mathbf{m}$:

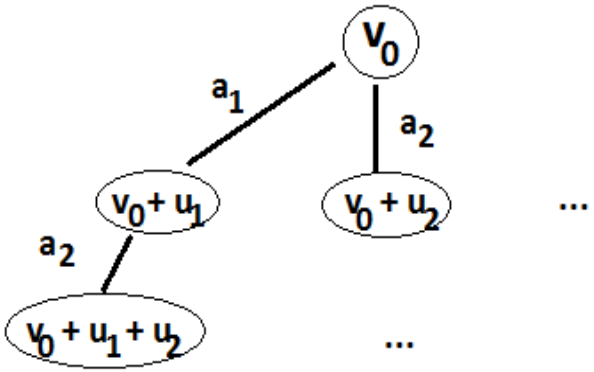
$\boxed{\mathbf{v} = \mathbf{v}_0 + \sum_i a_i \mathbf{u}_i}$

(avec $a_i \in \{0, 1\}$)

Minimisation : $\mathbf{v} \cdot \rho$ avec ρ carte de détectabilité

Combinaison a_i ?

- Bruteforce : $2^{\dim(\ker(\mathbf{H}))}$ évaluations (complexité)
- Arbre :



Problème : répétitions...

- STC : Noyau échelonné réduit puis comparaisons $\Rightarrow 2^h n$ évaluations

$$\begin{pmatrix} & \rho_1 & \rho_3 & \rho_5 & \rho_7 \\ \rho_2 & 1 & 1 & 1 & 1 \\ \rho_4 & 0 & 1 & 1 & 1 \\ \rho_6 & 0 & 0 & 1 & 1 \\ \rho_8 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Coset

Définition

Coset du message $\mathbf{m}$: $\mathcal{C}(\mathbf{m}) = \{\mathbf{v}/\mathbf{Av} = \mathbf{m}\}$

Théorème

La taille des cosets ne dépend que du rang de $\mathbf{A}$

Preuve

Si $r = rg(\mathbf{A})$, $k := dim(ker(\mathbf{A})) = n - r$ *alors*
- on a une base de k vecteurs du noyau, qui permettent de construire 2^k *vecteurs différents (par sommation) i.e.*
$Card(\mathcal{C}(\mathbf{m})) \geq 2^k$
- on a 2^r *cosets (car* 2^r *messages) disjoints (1 vecteur donne 1 message)*
Chaque coset possède au moins 2^k *vecteurs différents*
ce qui fait au total $2^{r+k} = 2^n$ *vecteurs différents de taille n*

Dimension

Lien entre $\mathbb{H}$ et $\hat{\mathbb{H}}$

$$\mathbb{H}\mathbf{v} = \begin{pmatrix} \hat{\mathbb{H}} \\ 0 \\ 0 \\ \dots \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \dots \\ v_h \end{pmatrix} + \begin{pmatrix} 0 \\ \hat{\mathbb{H}} \\ 0 \\ \dots \end{pmatrix} \begin{pmatrix} v_2 \\ v_3 \\ \dots \\ v_{h+1} \end{pmatrix} + \dots + \begin{pmatrix} 0 \\ \dots \\ 0 \\ \hat{\mathbb{H}} \end{pmatrix} \begin{pmatrix} v_{n-h+1} \\ v_{n-h+2} \\ \dots \\ v_n \end{pmatrix}$$

Théorème

$\mathbb{H}$ est de rang max (noté m) ssi $\hat{\mathbb{H}}$ l'est aussi (noté w)

Preuve par récurrence

On considère 2 blocs successifs avec une ligne de 0.
Toute colonne du 2e bloc avec un 0 sur la dernière ligne est combinaison linéaire du 1er bloc
Au moins une colonne possède un 1 à cet endroit (les autres colonnes sont dépendantes de celle-ci)
Les 2 blocs forment donc une matrice de rang w+1

Problématique

De nombreux choix empiriques et questions ouvertes :

1) Choix de la sous-matrice (des 1 sur la 1ère et la dernière ligne)

2) Pas de colonnes identiques (sous-matrice)

3) Optimiser pour un profil de distortion = optimisé pour tous

4) Peut-on augmenter la taille des cosets ?

5) Comment choisir les matrices ?

Résultats principaux

Meilleure compréhension STC :

1) pas d'amélioration grâce au coset

2) répartition quasi-uniforme du noyau = meilleur profil

3) $rg(\mathbb{H})$ lié à $rg(\hat{\mathbb{H}})$ (dimension maximale exigée donc au moins un 1 par ligne/colonne)

Soumission article JC^2S (Journée Dissimulation d'Information Interactions avec les Codes et la Cryptographie)

Algorithme du simplexe revisité

Futurs travaux

Mixe de la stéganographie corrélée avec la stéganographie adaptative

Travailler sur les cartes de détectabilité (ASO,...)

Enlever l'hypothèse d'additivité de la distortion

Modéliser le système par la théorie des jeux

Conclusion

Merci de votre attention ! ☺