Syndrome coding in adaptative steganography (STC's code)

L. Rosique[1], M. Chaumont[12], A.-E. Baert[2] and E. Guerrini[2]

[1] UNIVERSITE DE NIMES, F-30021 Nîmes Cedex 1, France
[2] UNIVERSITE MONTPELLIER 2, UMR5506-LIRMM, F-34095 Montpellier Cedex 5, France
[3] {lambert.rosique, marc.chaumont, anne-elisabeth.baert, eleonora.guerrini}@lirmm.fr

Abstract

Cet article fait suite aux travaux de Tomas Filler, Jan Judas et Jessica Fridrich sur l'utilisation des "Syndrome-Trellis Codes"[4] en stéganographie adaptative. Nous analysons ici les choix que proposent les auteurs pour les matrices, les possibilités d'améliorations et développons une approche par l'algèbre linéaire afin de résoudre le système. En effet, dans la littérature, ces résultats se basent sur des méthodes empiriques qu'il peut être intéressant de revoir.

1 Introduction

La stéganographie est l'art de dissimuler un message de manière secrète dans un support anodin. Dans ce papier nous nous intéressons plus particulièrement à la stéganographie par modification d'images. Un message binaire est dissimulé au sein d'une image en modifiant les valeurs de certains pixels.

Depuis la fin 2010 (avec l'algorithme HUGO [3] et la compétition BOSS [1]), on admet que la modification de certains pixels implique un effet plus ou moins important sur la détectabilité de l'image. Certains pixels sont donc plus "sensibles" que d'autres. On modélise cette "sensibilité" par une valeur de détectabilité, $\rho_i \in \mathbb{R}_+$, attribuée à chaque pixel [2] (HUGO[3], MOD, S-UNIWARD, ASO).

Une fois la *carte de détectabilité* construite, on l'utilise pour insérer le message, en utilisant le *Syndrome-Trellis Code* (STC) [4]. Cet algorithme détermine parmis les *mots de code* représentant le message celui qui minimise la somme des valeurs de détectabilité des pixels que l'on a modifié. On parle alors d'algorithme adaptatif pour de la stéganographie adaptative.

Il est à noter que le seul code existant permettant de prendre en compte une carte de détectabilité est le code STC [4]. Ce code est très proche de la borne théorique et linéaire en complexité calculatoire. Cependant, de nombreux points de l'algorithme ne sont pas explicités et nous proposons faire une analyse plus formelle du problème. Par exemple, les auteurs utilisent des matrices de contrôle de parité d'une forme particulière. Ce choix, ainsi que celui des coefficients utilisés pour remplir la matrice, est empirique. Nous allons donc les justifier.

Dans cet article, nous proposons en section 2 de rappeler le problème ainsi que le principe de STC. En section 3 nous reformulons le problème par de l'algèbre linéaire en utilisant les matrices échelonnées. Nous donnons ensuite les critères nécessaires à la résolution du problème d'insertion d'un message.

2 Mise en place du problème

En stéganographie, un message secret est caché dans une image source $\mathbf{x} = (x_1, ..., x_n) \in \{0, ..., 255\}^n$ en modifiant individuellement ses élements, pour produire une image stégo $\mathbf{y} = (y_1, ..., y_n)$.

Un protocole stéganographique d'insertion a pour objectif d'insrer avec une contrainte de minimisation de la fonction de distortion D entre $\mathbf{x}$ et $\mathbf{y}$. Cette fonction est le degr de ?? la dtectabilit de l'image.

2.1 Syndrome-Trellis Code

Dans le décodage par syndrome, qui est la méthode employée par l'algorithme STC, on dfinit les fonctions d'insertion et d'extraction à l'aide de la théorie des codes correcteurs. Soit $\mathcal{C}$ un code binaire linéaire de longueur n et de dimension n-m, avec m la taille du message. Soit $\mathbb{H} \in \{0, 1\}^{m \times n}$ sa matrice de parité et $C(\mathbf{m}) = \{\mathbf{z} \in \{0, 1\}^n \mid \mathbb{H}\mathbf{z} = \mathbf{m}\}$ le coset correspondant au syndrome $\mathbf{m}$. Les fonctions d'insertion et d'extraction du message sont définies par

$$\begin{cases} \text{Emb}(\mathbf{x}, \mathbf{m}) = \arg\min_{\mathbf{y} \in \mathcal{C}(\mathbf{m})} D(\mathbf{x}, \mathbf{y}) & (1) \\ \text{Ext}(\mathbf{y}) = \mathbb{H}\mathbf{y} & (2) \end{cases}.$$

On a pour habitude de prendre la fonction de distortion additive suivante : $D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \rho_i \cdot [x_i \neq y_i]$, avec $\rho_i \in \mathbb{R}^+$ le degr de dtectabilit du pixel, et $[S]$ le crochet d'Iverson, qui vaut 1 si l'assertion S est vraie et 0 sinon.

La matrice $\mathbb{H}$ est publique. La rsolution de (1) permet d'obtenir un vecteur stgo $\mathbf{y}$. Pour cela, la matrice $\mathbb{H}$ est reprsente sous la forme d'un treillis et l'algorithme de Viterbi calcule ce $\mathbf{y} \in \mathcal{C}(\mathbf{m})$ le plus "proche" de $\mathbf{x}$.

2.1.1 Matrice de parité

La matrice $\mathbb{H}$ est une matrice par blocs qui s'obtient en répétant une petite sous-matrice $\hat{\mathbb{H}} \in \{0, 1\}^{h \times w}$ où h et w seront explicités par la suite. Ces petites matrices sont placées cte à cte, et décalées d'une ligne par rapport à celle qui la précède, la première commenant à la première ligne, première colonne. Le paramètre h, communément appelé *constraint height*, affecte la complexit calculatoire de l'algorithme de Viterbi puisqu'il y a 2^h tats dans le treillis. Il est pris généralement entre 6 et 15, et w affecte le *relative payload* (proportion de bits insérés dans l'image) noté $\alpha = \frac{m}{n} \leq \frac{1}{2}$, par la relation $w = E(\frac{1}{\alpha})$ (où E désigne la partie entière).

$$\begin{pmatrix} \hat{\mathbb{H}} & \hat{\mathbb{H}} & & \\ & & \ddots & \\ & & & \hat{\mathbb{H}} \end{pmatrix}$$

L'intérêt de la représentation par blocs est d'une part de limiter le nombre de bits de $\mathbf{y}$ qui influent sur un bit du message par la relation $\sum_{j=E(i/h)}^{bw+E(i/h)} h_{i,j} y_j = m_i$, b tant le nombre de copies de $\hat{\mathbb{H}}$ dans $\mathbb{H}$, et d'autre part d'avoir une structure simple pour le treillis, trs rptitive.

2.1.2 Algorithme

Le but de l'algorithme est de trouver $\mathbf{y}$ tel que $\mathbb{H}\mathbf{y} = \mathbf{m}$ avec $D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \rho_i [x_i \neq y_i]$ minimale.

Sans détailler la construction du treillis, on rappelle qu'il s'agit d'un graphe constitué de b blocs (des sous-treillis), chacun contenant $2^h(w + 1)$ nuds, organisés en un treillis de $w + 1$

colonnes et 2^h lignes, de sorte que toutes les arêtes ne connectent que des nuds de colonnes adjacentes. Chaque $\mathbf{y}$ solution de $\mathbb{H}\mathbf{y} = \mathbf{m}$ est représenté comme un chemin dans le treillis, partant du premier état de 0 (en haut à gauche) et se déroulant vers la droite. Le chemin est alors le calcul étape par étape du syndrome partiel, à mesure que l'on utilise des bits de $\mathbf{y}$. Même si, a priori, le nombre de chemins dans le treillis est exponentiel en n, le problème de trouver le plus court peut se résoudre efficacement grâce à l'Algorithme de Viterbi.

En effet, il se décompose en deux parties : *forward* et *backward*. La première, en $n + b$ étapes, consiste à calculer progressivement le chemin le plus court entre le point de départ et les nuds de la i-ème colonne du treillis. Ensuite, dans la seconde partie, on reprend le chemin à l'envers et l'on retrouve l'objet stégo $\mathbf{y}$ à partir des étiquettes des nuds.

La complexité de cet algorithme est en $O(2^h n)$ et il s'avère très efficace : la distortion associée à l'insertion d'un message est proche de la valeur théorique de la distortion minimale par pixel attendue pour l'insérer. Pour plus de détail on peut se référer à [4].

2.2 Considérations sur la matrice

Revenons sur le design de la matrice $\mathbb{H}$. Quelles sous-matrices $\hat{\mathbb{H}}$ sélectionner pour que l'algorithme STC soit proche de la borne théorique en terme d'efficacité ? Dans l'article original de T.Filler et J Fridrich [4], les matrices sont dtermines de manire empirique. Nous allons expliquer pourquoi ces choix sont naturels.

Une première remarque est de dire que $\hat{\mathbb{H}}$ ne dépend pas du profil de la fonction de distortion, auquel cas il aurait fallu le communiquer en plus de la matrice. Selon les auteurs il faut optimiser la matrice pour un profil quelconque afin d'obtenir de bons résultats pour tous les profils. Ensuite, $\hat{\mathbb{H}}$ ne doit pas avoir de colonnes identiques sinon le treillis contiendrait au moins deux chemins distincts de poids égal, ce qui diminuerait les performances générales de l'algorithme. Enfin, leur dernière observation est de dire que la première ligne et la dernière ligne doivent contenir des "1".

Tout ceci a été observé expérimentalement dans 97% des 1000 codes tests avec $h = 7$ et $w = 4$. L'expérience laisse penser que le design du code est stable par rapport au profil et qu'une matrice peut être utilisée pour plusieurs profils de distortion.

3 Nouvelle approche

Nous allons proposer une approche par l'algèbre linéaire du problème prcdent $\mathbf{Av} = \mathbf{m}$ tel que $(\mathbf{v} + \mathbf{x}) \cdot \rho$ soit minimal dans $\mathbb{R}^+$ (on se place ici dans $\mathbb{F}_2$ en prenant le LSB de l'image $\mathbf{x}$). Ensuite, nous motiverons certains choix à faire sur $\mathbb{H}$.

3.1 Algèbre linéaire

Travaillons pour l'instant avec une matrice quelconque $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{F}_2)$ plutt qu'avec la matrice particulière $\mathbb{H}$. Comme on cherche à résoudre un système de m équations à n inconnues, on peut penser "diagonaliser" le système afin d'avoir une expression simple de l'ensemble des solutions au problème. Dans le cas de matrices rectangulaires, cette notion s'étend à celle des matrices échelonnées.

3.1.1 Matrices Echelonnées et Noyau

On rappelle qu'une matrice échelonnée en lignes est une matrice rectangulaire telle que la première valeur non-nulle de chaque ligne (appele pivot) est décalée d'au-moins une colonne par rapport à celle de la ligne précédente. Toute matrice $\mathbf{A}$ admet une forme chelonne en lignes $\mathbf{T}^{-1}E$, où T^{-1} est la matrice de passage. On a donc : $\mathbf{Av} = \mathbf{m} \Longleftrightarrow \mathbf{TAv} = \mathbf{Tm} \Longleftrightarrow \mathbf{Ev} = \mathbf{m'}$ où $\mathbf{m'} = \mathbf{Tm}$.

Grâce à cette nouvelle écriture, on peut calculer le noyau de la matrice $\mathbf{E}$ (grâce à un algorithme d'algèbre linaire sur les matrices chelonnes), que l'on va faire intervenir dans le problème, ainsi que son rang. Tout d'abord, il nous faut trouver une solution particulière $\mathbf{v'}$ au système "$\mathbf{Ev} = \mathbf{m}$". On procède ainsi : si r désigne le rang de $\mathbf{E}$, on a m équations à n inconnues. Rappelons que n est le nombre de pixels de l'image, et m est la taille du message. Il faut fixer n-r inconnues à 0 (ce qui nous revient en calculer r) pour obtenir une solution unique. On fixera donc à chaque ligne toutes les variables (non dj fixes) à 0 sauf une qui sera ensuite calcule pour satisfaire l'quation, et ce tant qu'on n'en aura pas calcul r.

Maintenant nous supposons $\mathbf{v'}$ calcul tel que $\mathbf{Ev'} = \mathbf{m'}$. Soit $(\mathbf{u}_i)_{i\in\{1,\ldots,\dim(\ker(\mathbf{E}))\}}$ une de base du noyau (un algorithme trs simple nous la donne). On a :

$$\mathbf{Ev} = \mathbf{m'} \Longleftrightarrow \mathbf{Ev} = \mathbf{Ev'} \Longleftrightarrow \mathbf{E}(\mathbf{v} + \mathbf{v'}) = \mathbf{0} \Longleftrightarrow (\mathbf{v} + \mathbf{v'}) \in \ker(\mathbf{E})$$

$$\Longleftrightarrow \exists(\lambda_1, \ldots\lambda_{n-r}) \in \{0,1\}^{n\text{-}r},\ \mathbf{v} = \mathbf{v'} + \sum_{i\in\{1,\ldots,n\text{-}r\}} \lambda_i \mathbf{u}_i \qquad (3).$$

Ainsi, le problème est, désormais, de trouver la meilleure combinaison de λ_i telle que $(\mathbf{v} + \mathbf{x}) \cdot \rho = (\mathbf{v'} + \mathbf{x}) \cdot \rho + \sum_{i\in\{1,\ldots,n\text{-}r\}} \lambda_i \mathbf{u}_i \rho$ soit minimale. Ce problme trs gnral se rsout par brute-force en $O(2^n)$, tandis que STC propose, dans un cas plus particulier mais tout aussi gnralisable, une rsolution en $O(2^h n)$ d'o sa force.

3.2 Propriétés

3.2.1 Coset

Soit $\mathbf{A} \in \mathcal{M}_{m,n}(\mathbb{F}_2)$. On dénote le coset du message $\mathbf{m} \in \{0,1\}^m$ comme $\mathcal{C}(\mathbf{m}) := \{\mathbf{v} \in \{0,1\}^n, \mathbf{Av} = \mathbf{m}\} = \{\mathbf{v} \in \{0,1\}^n, \mathbf{Ev} = \mathbf{Tm}\}$.

Il peut être intéressant de se demander si un "meilleur" choix de $\mathbf{A}$ donnerait plus de possibilités en termes de coset. En fait, ce n'est pas le cas si le rang de $\mathbf{A}$ est maximal, et nous allons le démontrer, et donc prendre une matrice STC ne nous pnalise pas.

On a, pour tout $\mathbf{v}, \mathbf{v'} \in \mathcal{C}(\mathbf{m})$, $(\mathbf{v} + \mathbf{v'}) \in \ker(\mathbf{E})$. Si le rang de $\mathbf{A}$ est m, son noyau est de dimension $k := n - m$, et on peut facilement trouver $\ker(\mathbf{E}) =< (\mathbf{u}_i) >_{i\in\{1,\ldots,k\}}$ avec les $\mathbf{u}_i$ dans le noyau tous indépendants entre eux. Ainsi, on peut former 2^k vecteurs différents, puisqu'ils forment une base, en les sommant de toutes les manières possibles. Rajouter $\mathbf{v'}$ à ces combinaisons opère juste une translation sans changer le nombre total de vecteurs. Ainsi, $\mathrm{Card}(\mathcal{C}(\mathbf{m})) \geq 2^k$

On peut alors voir qu'on a une égalité en observant l'ensemble des cosets : au total, on a 2^m messages, donc cosets associés. Ils sont tous disjoints puisqu'un même vecteur ne peut donner qu'un seul message. Chacun de ces cosets contient au moins 2^k vecteurs différents, ce qui fait un total d'au moins $2^{m+k} = 2^n$ vecteurs différents. Comme ces vecteurs sont de taille n, on a obtenu tout l'espace.

En conclusion, la taille des cosets dpend uniquement du rang de la matrice et ne peut donc pas etre optimise. Toutefois, la rpartition de ses vecteurs dans l'espace dpend de son noyau, et il peut être intressant de travailler là-dessus.

3.2.2 Profil

On se pose naturellement la question suivante "Est-ce qu'une rpartition plus uniforme des vecteurs du noyau dans l'espace permet d'avoir de bons profils de distortion?"

On peut essayer de répondre par l'affirmative en remarquant que les vecteurs associés à une faible distortion sont presque tous dans un voisinage de $\mathbf{x}$ (pour la distance de Hamming). En effet, on construit l'ensemble ordonn $\mathcal{E} = \{\mathbf{u} \in \{0,1\}^n / \forall \mathbf{v} \in \{0,1\}^n, \mathbf{u}$ est avant $\mathbf{v}$ si $\mathbf{u}\cdot\rho < \mathbf{v}\cdot\rho\}$ (en cas d'galit, on met arbitrairement l'un devant l'autre).

En fonction de l'écart type relatif $\tilde{\sigma} = \frac{\sigma}{\bar{\rho}}$ avec $\sigma = \sqrt{\frac{1}{n}(\sum_{i=1}^n \rho_i^2) - \bar{\rho}^2}$ l'écart type et $\bar{\rho} = \frac{1}{n}\sum_{i=1}^n \rho_i$ la moyenne, les vecteurs de $\mathcal{E}$ seront plus ou moins nombreux à être rangés par rapport à leur poids de Hamming, puisqu'un faible écart type relatif augmentera les probabilités, par exemple, que $\rho_k < \rho_i + \rho_j$ pour la plupart des triplets $(i,j,k) \in \{1,...,n\}$.

Calculons cette probabilit dans le pire cas grce la formule de Bienaym-Tchebichev, qui donne la probabilit de s'loigner de la moyenne en fonction de l'cart-type :

$\forall i \in \{1,...,n\}, P[|\rho_i - \bar{\rho}| \geq t\sigma] \leq \frac{1}{t^2}$ avec $t \in \mathbb{R}_*^+$.

Ce pire cas correspond $\rho_i, \rho_j \leq \bar{\rho}$ et la probabilit la plus leve d'avoir notre ingalit est de prendre un $\rho_k = \bar{\rho} + t_k\sigma$ tel que $\bar{\rho} \leq \rho_k$. Notons aussi $\rho_i = \bar{\rho} - t_i\sigma$ et $\rho_j = \bar{\rho} - t_j\sigma$, avec $t_i, t_j, t_k \in \mathbb{R}_*^+$.

On a alors $\rho_i + \rho_j < \rho_k \Longleftrightarrow \frac{1}{\tilde{\sigma}} - (t_i + t_j) < t_k$ et donc

$P[\rho_i + \rho_j < \rho_k] = P[|\rho_k - \bar{\rho}| \geq (\frac{1}{\tilde{\sigma}} - (t_i + t_j))\sigma] \leq \frac{1}{(\frac{1}{\tilde{\sigma}} - (t_i+t_j))^2}$

Comme $\mathbf{x}$ est aléatoirement placé dans l'espace des vecteurs, les probabilités pour que $\{\mathbf{v}|\mathbf{A}\mathbf{v} = \mathbf{m}\}$ rencontre $\mathcal{E}$ "rapidement", et donc que la distortion soit faible, dépendent de la répartition des vecteurs $\mathbf{u}_i$ dans l'espace puisque le voisinage de $\mathbf{x}$ ne rencontrera aucun $\mathbf{u}_i$ avant d'être suffisamment large. En d'autres termes, on a intrt ce que les vecteurs du noyau soient rpartis uniformment dans l'espace, ce qui est gnralement le cas pour les matrices STC qui sont donc un bon choix.

3.2.3 Sous-matrice

Maintenant que l'on a étudié les cas du coset et du profil, on peut s'intéresser aux propriétés précises que doit avoir $\mathbb{H}$ et surtout $\hat{\mathbb{H}}$, dont les dimensions sont bien moindre. Pour passer de $\mathbb{H}$ à $\hat{\mathbb{H}}$, on peut développer le produit matriciel de $\mathbb{H}$ par un certain vecteur $\mathbf{v}$:

$\mathbb{H}\mathbf{v} =$

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

On retrouve ainsi dans cette formule le déroulement du treillis donné auparavant avec le calcul des syndromes partiels.

Concernant le rang, il faut que $\mathbb{H}$ soit de rang m car tout message doit pouvoir être insr. D'autre part, si $\hat{\mathbb{H}}$ n'est pas de rang w (le plus grand rang possible pour cette matrice), alors $\mathbb{H}$ ne sera pas de rang m. En effet, le premier bloc de $\mathbb{H}$ est de rang w. Chaque colonne du bloc suivant qui possède un "0" sur sa dernière ligne est combinaison des vecteurs du bloc prcdent. Au moins une colonne possède un "1" à cet endroit, et donc est indpendante du bloc prcdent. Ainsi, ces deux blocs ensemble forment une matrice de rang *w +1*. Par rcurence, on montre que $\text{rang}(\mathbb{H}) = \text{rang}(\hat{\mathbb{H}}) + b - 1$ (ou -2 suivant si le dernier bloc est complet ou non), ce qui fait viddarmment m (à chaque nouveau bloc $\mathbb{H}$ gagne une ligne et son rang augmente de 1).

De fait, $\hat{\mathbb{H}}$ ne doit avoir ni de ligne ni de colonne nulle. En outre, un grand nombre de "1" dans la matrice augmente le nombre de pixels susceptibles de contenir un morceau du message sans changer l'efficacité de l'algorithme.

4 Conclusion

Grâce à cette nouvelle approche, on a pu mieux comprendre les mécanismes sous-jacents aux matrices STC. Une première idée d'amélioration de STC consistait à changer la taille des cosets pour avoir plus de vecteurs et donc une distortion potentiellement meilleure. Toutefois, cela n'est pas possible. Ensuite, on a vu comment $\hat{\mathbb{H}}$ agit sur les propriétés de $\mathbb{H}$ et ce qu'il faut exiger de cette matrice pour avoir de bons résultats avec l'algorithme STC. Notons ici que le système proposé à résoudre, dans son approche par l'algèbre linéaire, est très proche de ce que résout l'Algorithme du Simplex, à ceci près qu'on travaille dans $\mathbb{F}_p$ et non $\mathbb{R}$. Cette particularité nous empêche, d'ailleurs, d'y avoir recours.

References

[1] P. Bas, T. Filler, and T. Pevný. "Break Our Steganographic System": The Ins and Outs of Organizing BOSS. In *Information Hiding, 13th International Conference, IH'2011*, volume 6958 of *Lecture Notes in Computer Science*, pages 59–70, Prague, Czech Republic, May 2011. Springer.

[2] J.J. Fridrich and T. Filler. Practical Methods for Minimizing Embedding Impact in Steganography. In *Security, Steganography, and Watermarking of Multimedia Contents IX, part of IS&T SPIE Electronic Imaging Symposium*, volume 6505, pages 02–03, San Jose, CA, January 29-February 1 2007.

[3] T. Pevný, T. Filler, and P. Bas. Using High-Dimensional Image Models to Perform. Highly Undetectable Steganography. In *Information Hiding - 12th International Conference*, volume 6387 of *Lecture Notes in Computer Science, IH'10*, pages 161–177, Berlin, Heidelberg, October 01 2010. Springer-Verlag.

[4] Jan Judas Tomas Filler and Jessica Fridrich. Minimizing additive distortion in steganography using syndrome-trellis codes. In *IEEE Transactions on Information Forensics and Security*, volume 6, pages 920–935, 2011.