Stéganalyse d'algorithmes 1 embedding par classification

(ou comment, entre autre, attaquer l'algorithme HUGO)

Présentée par: Yasmine HACHEMANE

Encadrés par: Marc CHAUMONT
Sarra KOUIDER

Plan

I. *Stéganographie & Stéganalyse*

I.1 Stéganographie

I.2 Stéganalyse

I.3 Exemple d'illustration

II. *HUGO*

II.1 Test des performances d'HUGO

II.2 BOSS: La compétition

III. *L'approche de stéganalyse de Kodovský et Fridrich 2011, classification par un ensemble de classifieurs (boosting)*

III.1 Performances du classifieur

IV. *Déroulement du stage et perspectives*

I. Stéganographie & Stéganalyse

I.1 Stéganographie

Cacher un message de manière indétectable (visuellement et statistiquement)

I.2 Stéganalyse

Détecter la présence de messages cachés

I.3 Exemple d'illustration

Figure(1):Problème des prisonniers

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

II. Highly Undetectable steGO (HUGO)

Algorithme stéganographique d'images publié en Juin 2010, utilisé pour la compétition BOSS.

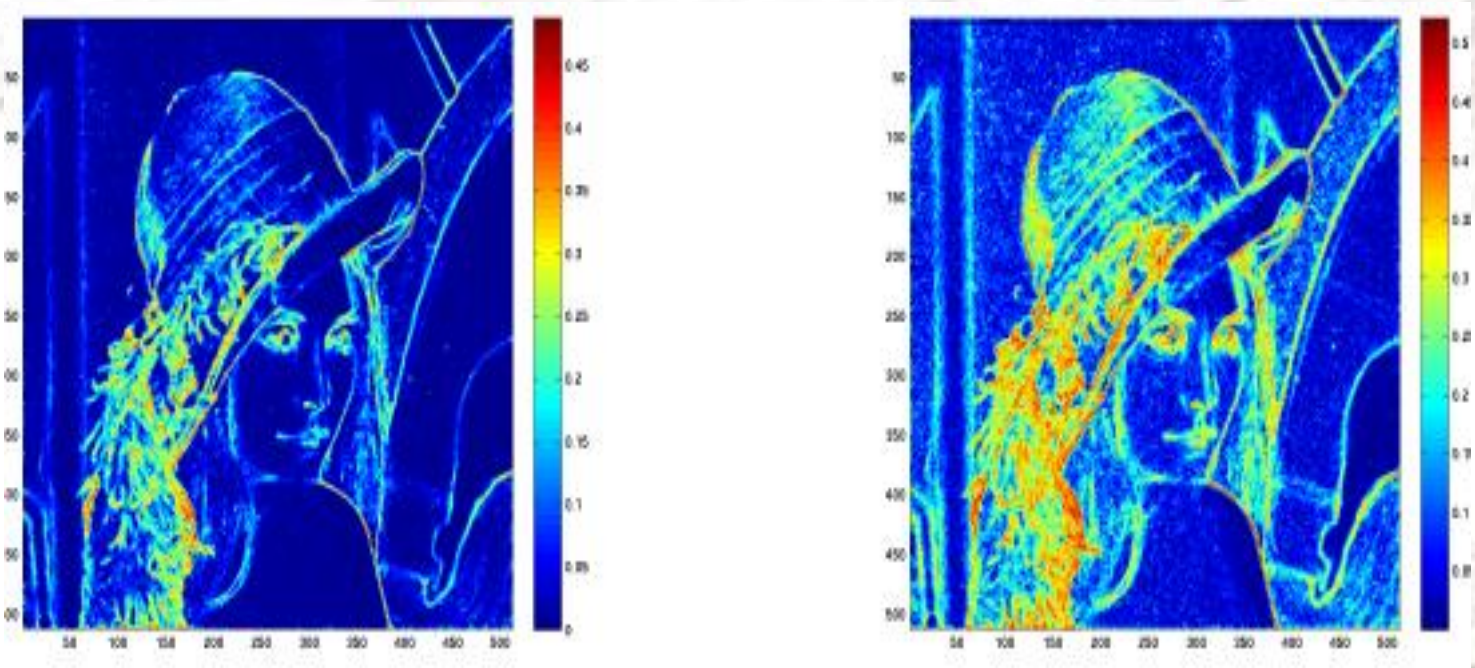
- *Modification de certains pixels par 1*
- *Philosophie de minimisation d'impact d'insertion*

matrix embedding (F5, nsF5): distorsion minimale ⇨ nb minimal de modifications

- *Utilisation d'une carte de distorsion*
- *Utilisation de caractéristiques de haute dimension (10^7)*
- *Intégrer des messages 7x plus long que l'LSB matching*

[HUGO 2010] "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography", T. Pevny, T. Filler and P. Bas, 12th Information Hiding Conference, June 28 - 30, 2010, Calgary, Alberta, Canada.
Code source : Break Our Steganography System, 2010, http://boss.gipsa-lab.grenoble-inp.fr/BOSSRank/.

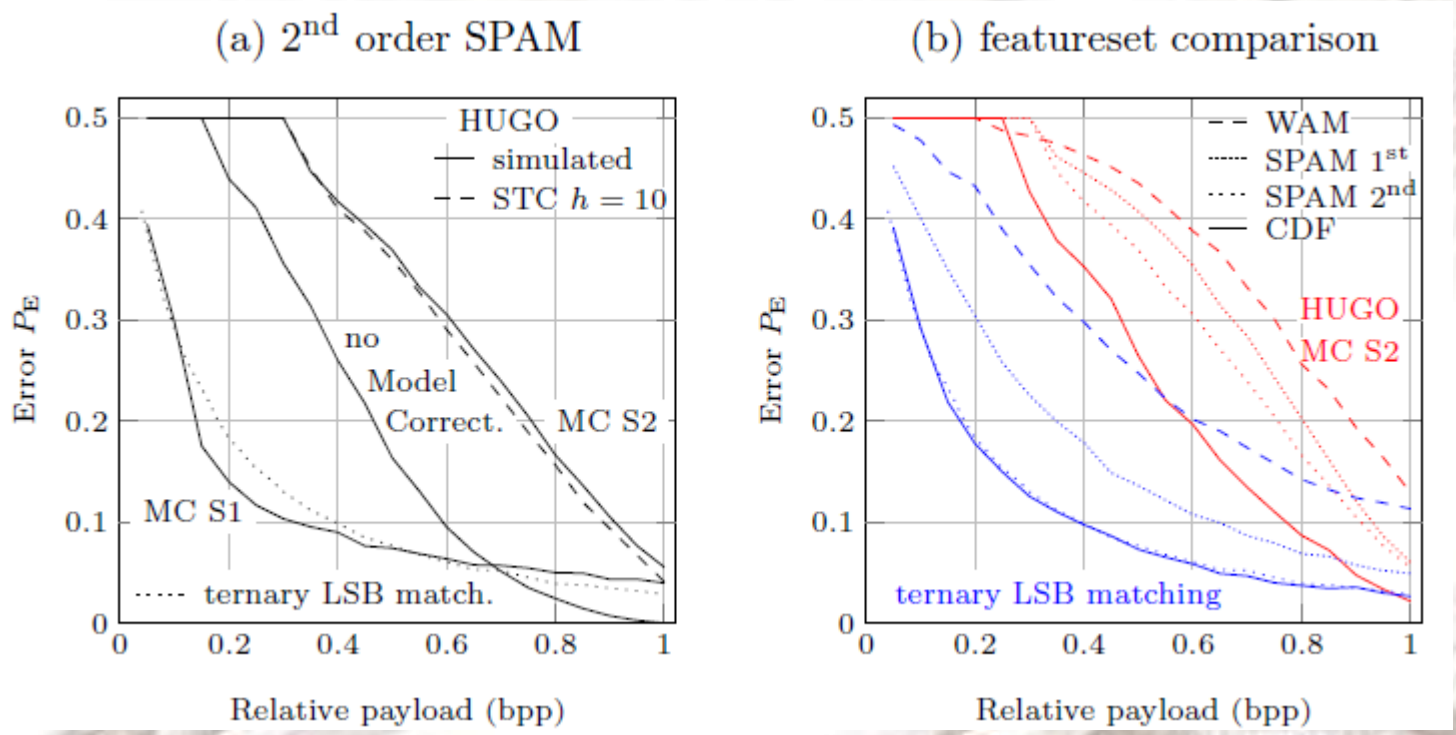
Emplacement du message



Figure(2):Message inséré dans les zones où la détectabilité est faible
(a): 0.25 bpp *(b): 0.5 bpp*

[HUGO 2010] "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography", T. Pevny, T. Filler and P. Bas, 12th Information Hiding Conference, June 28 - 30, 2010, Calgary, Alberta, Canada. Code source : Break Our Steganographic System, 2010, http://boss.gipsa-lab.grenoble-inp.fr/BOSSRank/.

II.1 Test des performances d'HUGO



Figure(3):
(a)Taux de sécurité d'HUGO utilisant les SPAM de 2nd ordre
(b)Stéganalyse d'HUGO par les meilleurs détecteurs actuels

[HUGO 2010] "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography", T. Pevny, T. Filler and P. Bas, 12th Information Hiding Conference, June 28 - 30, 2010, Calgary, Alberta, Canada.
Code source : Break Our Steganography System, 2010, http://boss.gipsa-lab.grenoble-inp.fr/BOSSRank/.

II.2 Break Our Steganographic System(BOSS)

Compétition visant à casser l'algorithme HUGO jugé comme le plus performant du moment.

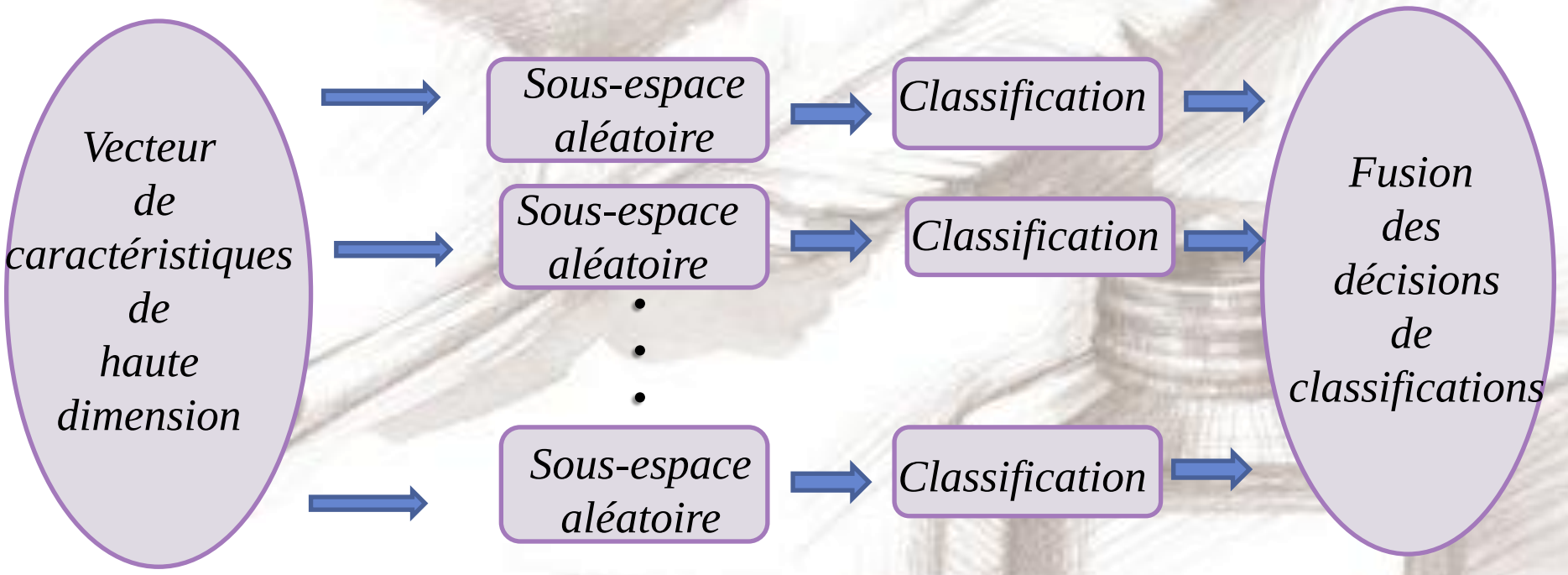
L'équipe de Kodovsky et de Fridrich qui a utilisé la fusion de faibles classifieurs s'est classée première avec une précision de 80,3%

Logo de la compétition BOSS

[BOSS 2010] Break Our Steganographic System, 2010, http://boss.gipsa-lab.grenoble-inp.fr/BOSSRank/.

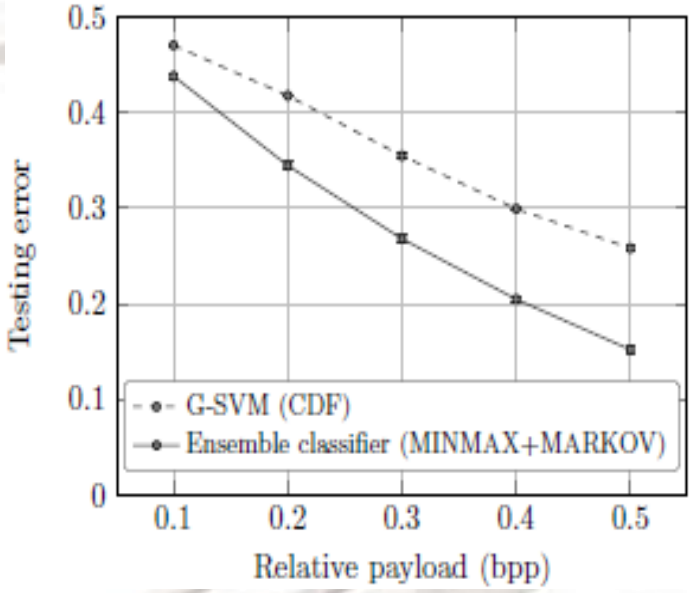
III. Classification par ensemble de classifieurs (boosting)

Approche de Kodovsky et Friddrich pour stéganalyser HUGO



Figure(4): Fusion de classifieurs

III.1 Performances du classifieur



Payload	G-SVM CDF	Ensemble classifier MINMAX+MARKOV
0.1	0.4705	0.4381
0.2	0.4178	0.3447
0.3	0.3549	0.2681
0.4	0.2995	0.2049
0.5	0.2583	0.1522

Figure(5): Erreur du stéganalyseur (Pe) pour un G-SVM et l'ensemble des classifieurs avec cinq taux d'insertion d'HUGO

[Kod2011] « Fusing classifiers built on random subspaces», J.Kodovsky and J.Fridrich Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIII, San Francisco, CA, January 23–26, 2011

Déroulement du stage et perspectives

1er Mois → 2Mois

Etude de l'état de l'art

- *Etude des récentes approche de stéganalyse et d'attaques*
- *Compréhension de vecteurs caractéristiques*
- *Algorithme d'apprentissage*

- *Prendre en mains les vecteurs caractérisant existants*
- *Implémenter l'approche de Kodovsky*

Perspectives :

1) enrichir le vecteur caractérisant
2) utiliser la réduction de dimension (ACP,….) conjointement à l'approche de Kodovsky

Merci
pour votre attention