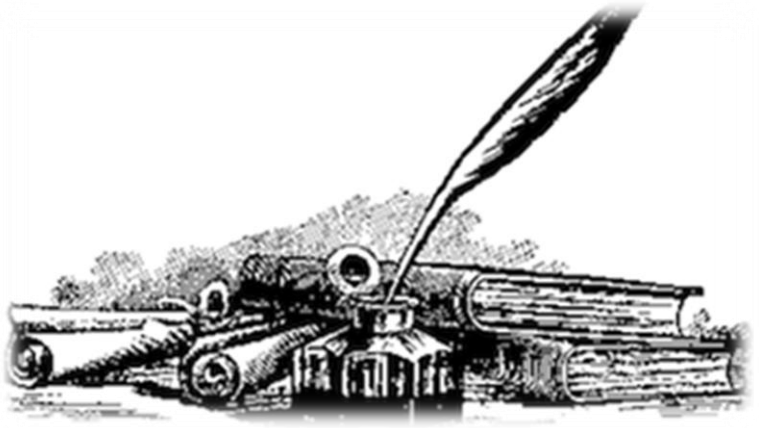
Codes correcteurs et sécurité en stéganographie



Sarra Kouider

Encadrants : **Marc Chaumont**
William Puech

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM

Parcours universitaire

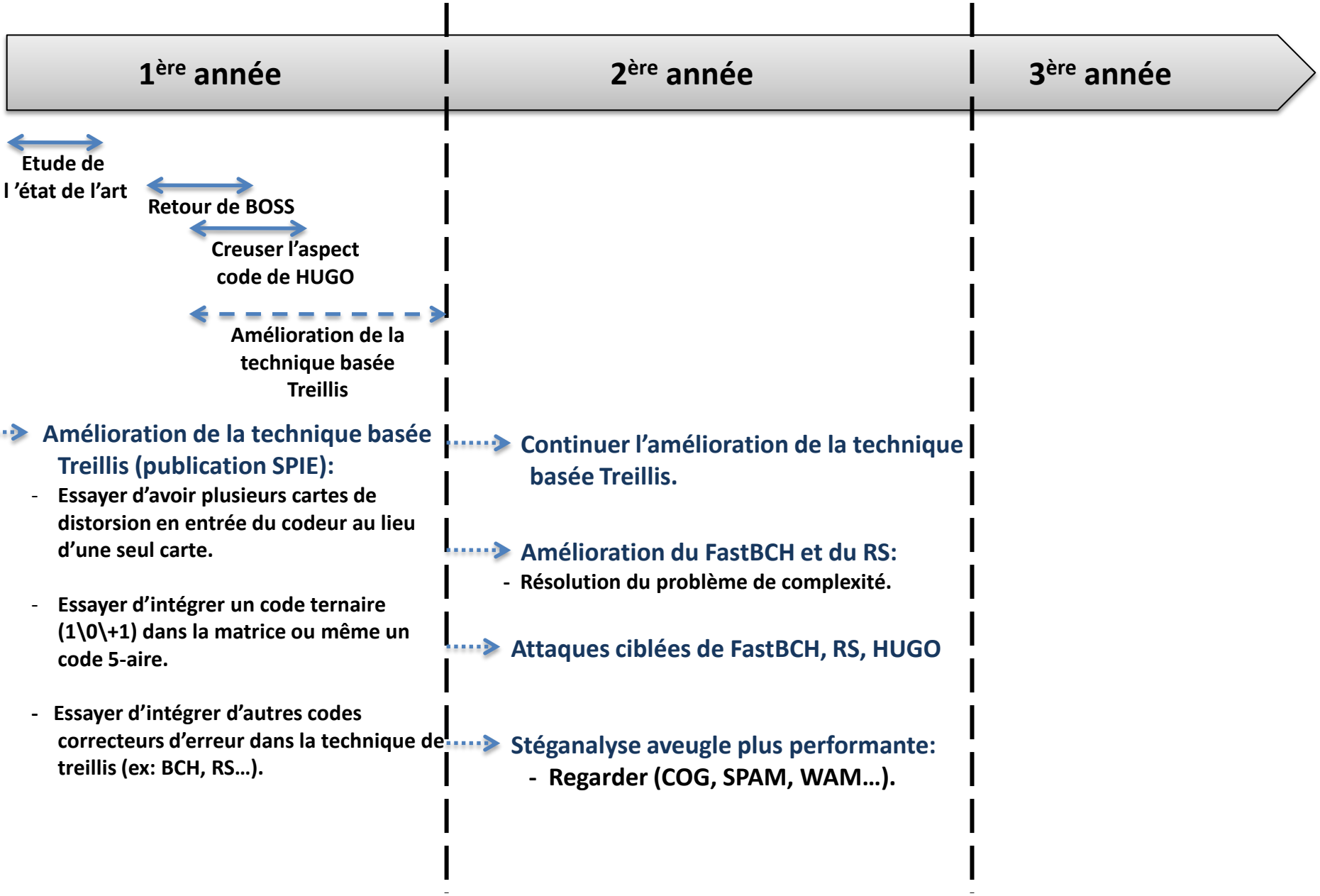
2005-2008 : Diplôme de Licence en Math Informatique
Université Badji Mokhtar, Annaba en Algérie

2008-2009 : 1ère Année Master informatique IFPRU
Université de Montpellier II

2009-2010 : 2ème Année Master informatique IFPRU
Université de Montpellier II
Parcours Ingénierie de l'Intelligence Artificielle (I^2A)

Stage de recherche au Lirmm
avec Marc Chaumont & Gérard Subsol
« Extraction de caractéristiques
pour l'analyse biométrique 3D d'un visage »

Déroulement de la thèse



Déroulement de la thèse

Etude de l 'état de l'art

Retour de BOSS

Creuser l'aspect code de HUGO

Amélioration de la technique basée Treillis

Amélioration de la technique basée Treillis (Publication SPIE):

- Essayer d'avoir plusieurs cartes de distorsion en entrée du codeur au lieu d'une seul carte.
- Essayer d'intégrer un code ternaire (1\0\+1) dans la matrice ou même un code 5-aire.
- Essayer d'intégrer d'autres codes correcteurs d'erreur dans la technique de treillis (ex: BCH, RS…).

Continuer l'amélioration de la technique basée Treillis.

Amélioration du FastBCH et du RS:

- Résolution du problème de complexité.

Attaques ciblées de FastBCH, RS, HUGO

Stéganalyse aveugle plus performante:

- Regarder (COG, SPAM, WAM…).

Présentation

du contexte général

Contexte Général

1. ***La stéganographie***
   - 1.1. Introduction à la stéganographie
   - 1.2. Schéma stéganographique
   - 1.3. Stéganographie, Tatouage et Cryptographie

2. ***La Stéganalyse***
   - 2.1. Modèles de gardien
   - 2.2. Attaques d'un schéma stéganographique

Contexte Général

1. ***La stéganographie***
   - 1.1. Introduction à la stéganographie
   - 1.2. Schéma stéganographique
   - 1.3. Stéganographie, Tatouage et Cryptographie

2. ***La Stéganalyse***
   - 2.1. Modèles de gardien
   - 2.2. Attaques d'un schéma stéganographique

1.1. Introduction à la Stéganographie

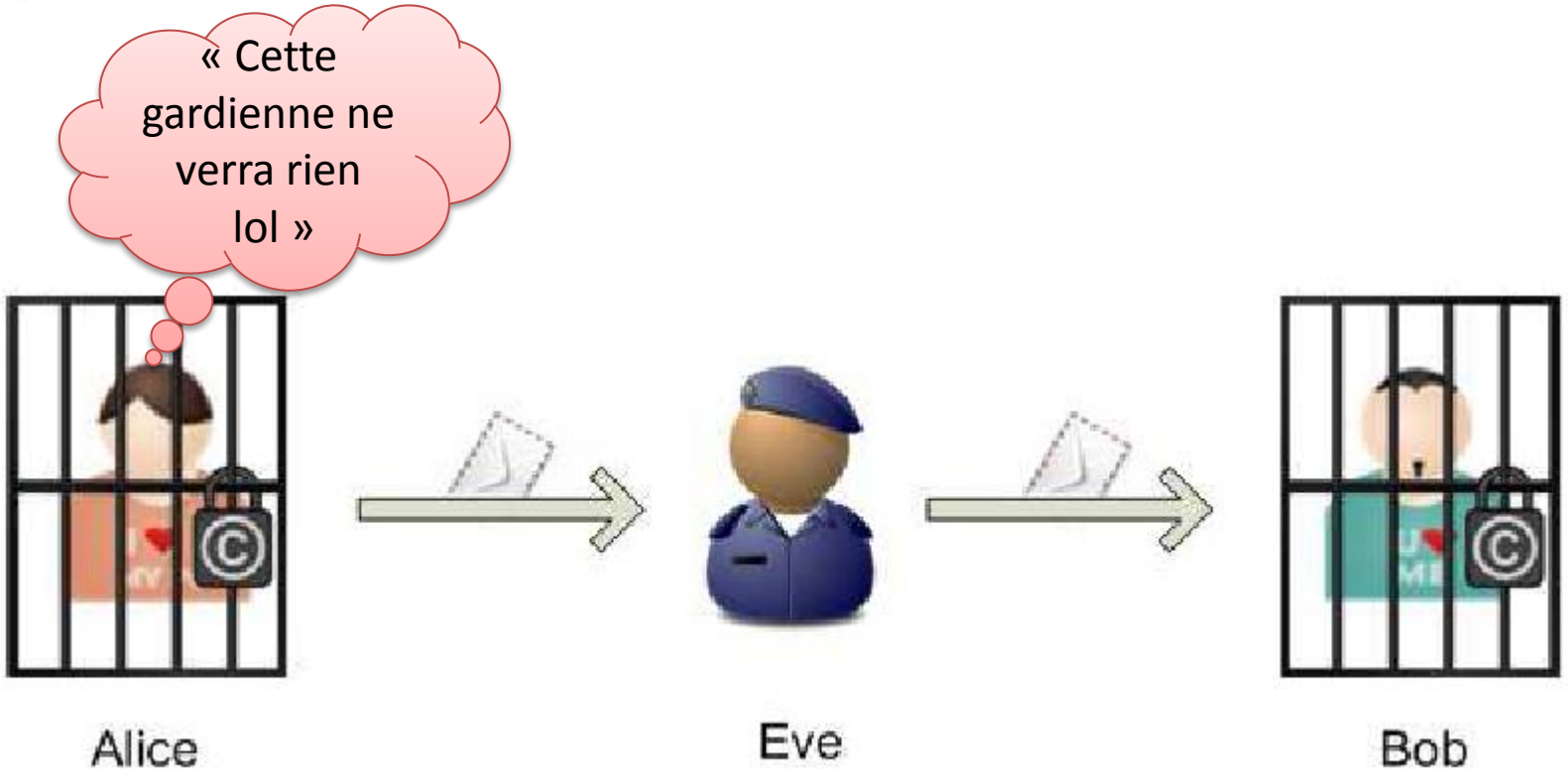
Définition :

La **stéganographie** est l'art de la communication secrète, elle consiste à altérer un média (une image, une vidéo, un son…) de sorte qu'il **contienne un message indétectable.**

≈

Image Hôte **Image Stego**

1.1. Introduction à la Stéganographie



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.

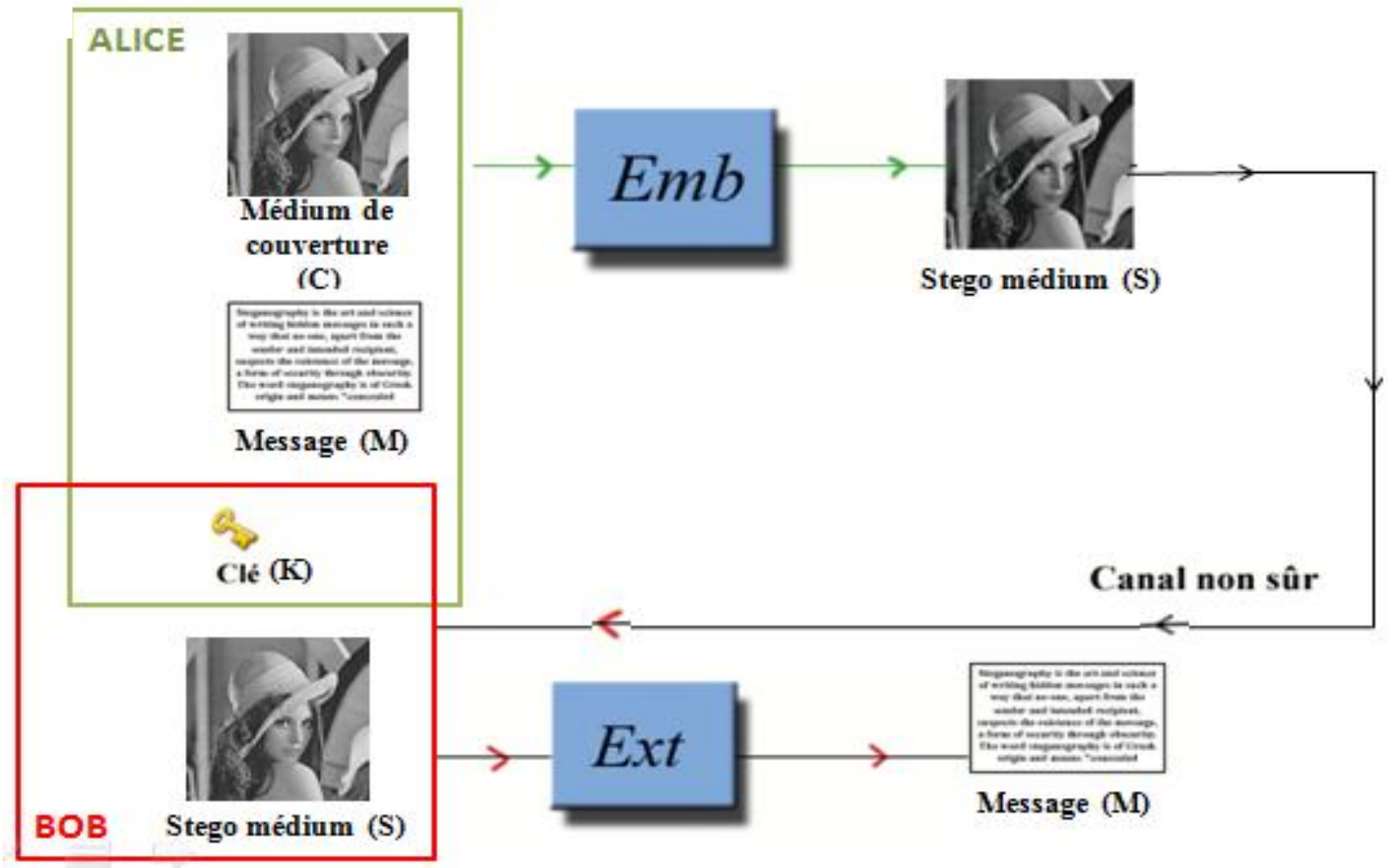
1.2. Schéma stéganographique

Architectures d'un schéma stéganographique [2]:

1. Stéganographie par sélection du médium de couverture.
2. Stéganographie par synthèse du médium de couverture.
3. Stéganographie par modification du médium de couverture

[2] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, 464 pages, Cambridge University Press, 1st edition, Chapters 1-5, December 31, 2009.

1.2. Schéma stéganographique [3]



[3] R. Watrigant. Utilisation des codes correcteurs d'erreurs en stéganographie : De l'algorithme F5 et sa stéganalyse aux codes à papier mouillé, Rapport de projet en L3, Nîmes, France, 2009.

1.3. Stéganographie, Tatouage et Cryptographie

Le tatouage:

est l'art d'altérer un média (une image, une vidéo, un son…) de sort qu'il contienne un message **le plus souvent en rapport avec le média, et ceci d'une manière robuste.**

La cryptographie:

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant **de chiffrer des messages**, c'est-à-dire permettant de **les rendre inintelligibles.**

Contexte général

1. ***La stéganographie***
   - 1.1. Introduction à la stéganographie
   - 1.2. Schéma stéganographique
   - 1.3. Stéganographie, Tatouage et Cryptographie

2. ***La Stéganalyse***
   - 2.1. Modèles de gardien
   - 2.2. Attaques d'un schéma stéganographique

2.1. Modèles de gardien

Le problème des prisonniers

2.1. Modèles de gardien

- ***Gardien passif*:** gardien qui se contentent d'observer le trafic entre Alice et Bob **.**

- ***Gardien actif*:** Ce gardien va essayer d'apporter quelques modifications sur le médium (Compression, filtrage…) dont le but de détruire le processus stéganographique s'il existe **.**

- ***Gardien malicieux*:** Gardien qui va essayer de comprendre la technique stéganographique et extraire le message, dont le but de le contourner pour ses propres fins**.**

2.2. Attaques d'un schéma stéganographique

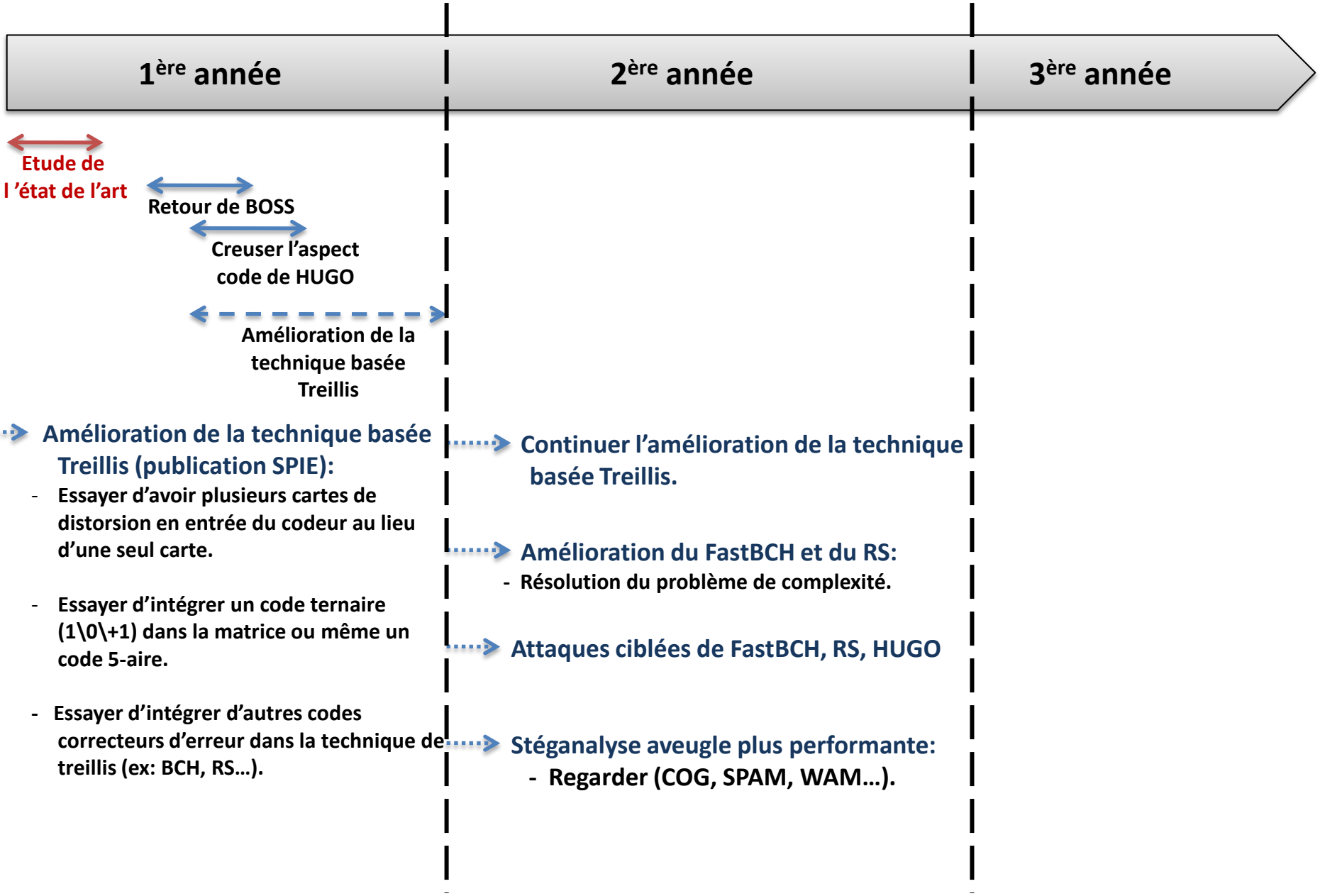
***Attaques ciblées*:** étude d'un algorithme spécifique et utilisation de ces points de faiblesse pour l'attaquer **.**

***Stéganalyses aveugles*:** plus généraliste, elle consiste à utiliser un mécanisme d'apprentissage (SVM, réseau de neurones..)**.**

Pistes éventuelles

pour la poursuite de thèse

Déroulement de la thèse



Merci

pour votre attention

Annexe

Exemple démonstratif

Technique LSB:

***Message (M)*: 0 0 1 10 1 0 0**

Image en niveau de gris

01001011	00101011	10010100	11101000
10011111	01110110	00110111	00110101

Exemple démonstratif

Technique LSB:

***Message (M)*: 0 0 1 1 0 1 0 0**

Image en niveau de gris

01001010	00101010	10010101	11101001
10011110	011101101	00110110	00110100

Highly Undetectable setGO (HUGO) [4]

HUGO:

est un nouvel algorithme de stéganographie d'images dans le domaine spatial dont le principe repose sur la minimisation d'une mesure de distorsion définie comme étant la différence entre les vecteurs caractéristiques SPAM tirés de l'image de couverture et de l'image stégo.

La première étape de cet algorithme consiste à calculé deux cartes de distorsions : une pour l'ajout (+1) dans l'image d'origine, et une autre pour l'ajout (-1). Le calcul de ces deux cartes abouti au final à une seule carte celle du minimum des deux.

[4] T. Pevny, T. Filler, P. Bas. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography presented for Information Hiding, Calgary, Canada, 2010.