17044 HAMDOUN Anas

Applications des codes de Reed-Solomon en Stéganographie

Lors de la dissimulation d'un message, un problème se pose: plus on injecte de l'information dans un support, plus celui-ci est détérioré et l'information est détectable. Pour remédier à ce problème, j'ai pensé à utiliser les fameux codes correcteurs d'erreurs dites de Reed Solomon dans un contexte stéganographique.
La Stéganographie est l'une des solutions qui s'avère efficace, s'alliant à la cryptographie, voire la remplaçant parfois, pour la sécurisation des données et informations personnelles. Cette sécurité d'informations est l'un des enjeux sociétaux modernes.

Positionnement thématique (ETAPE 1)

MATHEMATIQUES (Algèbre), MATHEMATIQUES (Mathématiques Appliquées), INFORMATIQUE (Informatique Théorique).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Stéganographie	*Steganography*
Codes correcteurs d'erreurs	*Error-correcting codes*
Codage Reed-Solomon	*Reed-Solomon coding*
Codage Matriciel	*Matrix encoding*
Efficacité d'insertion	*Embedding efficiency*

Bibliographie commentée

La stéganographie est une science et un art utilisé depuis des siècles pour faire passer inaperçu un message secret dans un fichier anodin. Ce mot vient du grec "Stéganô", qui signifie couvrir et "Graphô" qui veut dire écriture. Ainsi, on dissimule les informations que l'on souhaite transmettre confidentiellement dans un ensemble de données d'apparence anodine afin que leur présence reste imperceptible.
Dans son Enquête, l'historien grec Hérodote (484-445 av. J.-C.) rapporte ainsi une anecdote qui eut lieu au moment de la seconde guerre médique. En 484 avant notre 1ère, Xerxès, fils de Darius, roi des Perses, décide de préparer une armée gigantesque pour envahir la Grèce. Quatre ans plus tard, lorsqu'il lance l'offensive, les Grecs sont depuis longtemps au courant de ses intentions. C'est que Démarate, ancien roi de Sparte réfugié auprès de Xerxès, a appris l'existence de ce projet et décidé de transmettre l'information à Sparte: " il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis".
L'introduction de cette problématique dans les thèmes de recherches académiques doit beaucoup à G. Simmons et son problème des prisonniers (cf.[5]). Simmons envisage le cas de deux prisonniers autorisés à échanger des messages authentifiés, mais non chiffrés. L'algorithme d'authentification est connu et le but des prisonniers est d'échanger des messages planifiant une évasion. Lors de la parution de [5], la question des fuites d'information se posait déjà très fortement et le même auteur

détaille dans [4] la manière dont les États-Unis et l'Union soviétique, à la fin des années 1970, au cours de négociations sur un traité de non prolifération des armes nucléaires, se sont trouvés confrontés au problème de connaître très précisément quelles données pouvaient être émises par un détecteur. Les protagonistes étudiaient un dispositif devant permettre de détecter la présence de missiles dans les silos, sans révéler les emplacements de ces derniers. Parmi les contraintes imposées, il devait être impossible de modifier l'information émise et également impossible de transmettre plus que le strict nécessaire. Simon Litsyn explique, dans [6], de quelle façon il a été amené à étudier ce dispositif et à constater qu'il était possible de transmettre une dizaine de bits sans que cela soit détectable.

Les codes correcteurs d'erreurs sont utilisés dans la communication numérique pour protéger les données numériques contre les bruits lors de la transmission à travers un canal de communication et permettent aussi la protection de données lors de leur stockage. Mais ils peuvent encore être employés en cryptographie. Ils sont dans ce contexte un outil permettant, de chiffrer des données et d'authentifier des personnes. Le domaine de la cryptographie basé sur les codes correcteurs d'erreurs a vu le jour après l'invention du premier cryptosystème à clef publique par Diffie et Hellman[7], cette nouvelle branche de la cryptographie moderne, a donné l'idée au mathématicien français R.J.McEliece[8] pour imaginer le premier et le plus célèbre des cryptosystèmes à clef publique utilisant des codes correcteurs d'erreurs. Notons quand même que les codes ont aussi beaucoup d'applications dans d'autres domaines parmi eux la stéganographie, en général l'implémentation de la stéganographie avec les codes correcteurs d'erreurs est connu sous le nom de codage matriciel, a été introduite en stéganographie par Cranddall[2] en 1998. L'implémentation a ensuite été proposée par Westfeld avec l'algorithme de stéganographie F5 [1]. L'objectif est toujours le même (une image, audio, vidéo...) en modifiant celle-ci, mais avec la contrainte de minimiser le nombre de modifications introduites dans le fichier. L'insertion est basée sur le calcul de syndrome, mais le but est d'obtenir une efficacité d'insertion meilleure que celle trouvée par les algorithmes précédents. Une autre évolution de stéganographie avec les codes a été également proposée à travers les "codes à papier mouillé"[3], et consiste à sélectionner les sites d'insertion du côté codeur, mais avec un décodeur ignorant les sites sélectionnés.

Problématique retenue

Comment peut-on minimiser les modifications du support lors de l'insertion de l'information ? Et pourquoi les codes de Reed-Solomon peuvent être de bons outils pour réaliser des schémas stéganographiques ?

Objectifs du TIPE

-Une étude plus ou moins complète des codes correcteurs d'erreurs dans leur contexte courant (utiliser la redondance pour détecter la présence d'erreurs, puis les corriger lors de la transmission de messages au travers d'un canal de communication bruité) avec une approche purement mathématique puis informatique pratique, tout en montrant la particularité et l'efficacité des codes de Reed-Solomon par rapport aux autres codes.

-Une description explicite des relations entre les codes correcteurs
d'erreurs et les systèmes stéganographiques.

-Réalisation d'un schéma stéganographique à l'aide des codes de Reed-Solomon.

Références bibliographiques (ETAPE 1)

[1] Andreas Westfeld : F5—a steganographic algorithm: High capacity despite better steganalysis : *Springer-Verlag, 4th International Workshop on Information Hiding*

[2] R. Crandall : Some notes on steganography : *http ://os.inf.tu-dresden.de/ westfeld/crandall.pdf, 1998*

[3] Jessica Fridrich, Miroslav Goljan, David Soukal : Wet paper codes with improved embedding efficiency : *IEEE Transactions on Information Security and Forensics*

[4] G.J. Simmons : The history of subliminal channels : *IEEE Journal on Selected Areas in Communication*

[5] G.J. Simmons : The prisoners problem and the subliminal channel, in Advances in Cryptology : *Plenum Press*

[6] F. Levy-dit Vehel, S. Litsyn : Parameters of Goppa codes revisited : *IEEE Transactions on Information Theory*

[7] W. Diffie and M. Hellman : New directions in cryptography : *IEEE Transactions on Information Theory*

[8] R. J. McEliece : A public-key cryptosystem based on algebraic coding theory : *DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol., Pasadena, CA*

[9] C. Munuera : Steganography and error-correcting codes, Signal Processing

[10] M.B. Medeni, EL. Souidi : A Novel Steganographic Protocol from Error-correcting Codes : *Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 4*

DOT

[1] *Choix du sujet de mon TIPE suite à la lecture de certains articles et thèses sur la théorie des codes.*

[2] *Approfondissement de mes connaissances en les codes correcteurs d'erreurs et la dissimulation de l'information(Stéganographie).*

[3] *Choix du codage de Reed-Solomon et étude de sa particularité et son efficacité par rapport aux autres codages de correction d'erreurs.*

[4] *Construire un programme Python pour le codage Reed-Solomon.*

[5] *J'ai essayé enfin d'utiliser toutes ces connaissances pour réaliser un schéma stéganographique, c'est à dire un protocole permettant de dissimuler et récupérer un message secret.*