Décodage en liste des codes BCH appliqué à la stéganographie

Type de contenu : Texte

Titre(s) : Décodage en liste des codes BCH appliqué à la stéganographie ; PARRAUD, Patrice ; SLT LE GOUIC, Thomas|SLT GUILHON, Sylvain ; SOUIDI El, Mamoun

Autre(s) responsabilité(s) : PARRAUD, Patrice (Directeur de thèse)
SLT LE GOUIC, Thomas|SLT GUILHON, Sylvain (Secrétaire)
SOUIDI El, Mamoun (Directeur de thèse)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Description matérielle : 1 CD

Note sur le contenu : mémoire

Note de thèses et écrits académiques : Filière Scientifique - Option Informatique Promotion Chef de bataillon Bulle Date de soutenance : 01/01/2013

Résumé ou extrait : PRESENTATION : Le monde dans lequel nous vivons aujourd'hui ne peut se passer de l'informatique, notamment dans le domaine de la communication. Les informations échangées peuvent toutefois être altérées lors de leur passage dans un canal de transmission, il est donc nécessaire de trouver un moyen capable de retrouver l'information envoyée. La Théorie des Codes Correcteurs d'Erreurs permet de détecter et de corriger ces erreurs survenues durant la transmission du message. Notre travail étudie un cas particulier de transmission d'informations, la stéganographie. C'est une discipline liée à la théorie des codes car elle permet d'introduire un message secret dans un support en le modifiant par un moyen d'injection volontaire d'erreurs. Afin de mieux cerner l'intérêt de cette théorie dans la stéganographie, nous avons implémenté trois différents protocoles permettant d'injecter un texte ou une image dans un support image. Ce travail témoigne de l'avantage conféré par l'utilisation de codes BCH, encore peu utilisés jusqu'à présent en stéganographie, mais dévoile également une limite, celle de la capacité de correction du code. Ce sont les algorithmes de décodage en liste qui permettent de dépasser cette limite. L'objectif principal de notre travail est de mieux cerner l'intérêt du décodage en liste de codes BCH dans son application à un stégo-protocole. Nous présentons également les résultats obtenus dans la recherche d'optimisation de nos protocoles, notamment via l'étude de la distribution des poids de leaders de classe et celle des bornes de stégo-protocoles. CONTRAINTES : Durant notre recherche, nous sommes toujours restés en quête de protocoles plus performants en termes de distorsion d'image, de taux d'encodage, de temps d'exécution, de capacité d'injection et de sécurité. Tous ces paramètres dépendant les uns des autres, la première contrainte fut donc de réaliser un protocole optimal en cherchant à obtenir le bon compromis entre ceux-ci. De plus, certains algorithmes de décodage en liste que nous utilisons ne sont en théorie pas utilisable avec des codes BCH. Nous avons donc dû adapter nos programmes afin de faire correspondre entre eux les différents codes compatibles équivalents. Enfin, l'utilisation d'ordinateurs personnels réduit fortement les ressources disponibles pour nos programmes. Une autre contrainte a donc été d'utiliser des codes de petites longueur, moins efficaces lorsqu'utilisés dans un algorithme de décodage

en liste. LIMITES : Les algorithmes de décodage en liste connus actuellement ne sont compatibles que pour des codes de Reed-Solomon, excepté celui de Wu. Or, dans ce projet, nous travaillons avec des codes BCH binaires car peu de travaux ont encore été réalisés à leur sujet. Nous avons réussi à utiliser les propriétés des codes afin de passer d'un code RS à son code BCH équivalent, cependant nous avons atteint plusieurs limites. Tout d'abord les algorithmes de décodage en liste retournent une liste de mots et non l'unique mot correspondant. Or, nos applications reposent sur la réception d'un unique mot. Nous avons donc contourné ce problème en utilisant des codes de petites longueurs, mais nous perdons de fait l'avantage des algorithmes de décodage en liste. Ensuite l'utilisation d'ordinateurs personnels réduit grandement les ressources disponibles pour les algorithmes. Aussi le protocole GS nécessite jusqu'à 10 minutes de décodage pour des messages de plus de 10 ko. Enfin l'utilisation de la bibliothèque de décodage decoding fournie par Guillaume Quintin ne permettait pas d'implémenter l'algorithme de Wu. CONCLUSION : Au fil de notre étude, nous avons testé plusieurs outils mathématiques permettant d'implémenter un protocole stéganographique efficace et sécurisé. Ceux implémentés présentent des résultats convaincants selon le contexte d'emploi. Nous avions pour objectif de déterminer l'intérêt du décodage en liste des codes BCH dans la stéganographie et nous en sommes arrivés à la conclusion su

Sujet(s) : calcul d'erreur
codage de données
protocole
securité des données
stéganographie
traitement de l'information
transmission de données