STEGANORAPHIE ET CODES SUR Z4

Type de contenu : Images animées

Titre(s) : STEGANORAPHIE ET CODES SUR Z4 ; PARRAUD ; SLT DAVID, Guillaume|SLT PERROTTE, Jean-Paul ; SOUIDI

Autre(s) responsabilité(s) : PARRAUD (Directeur de thèse)
SLT DAVID, Guillaume|SLT PERROTTE, Jean-Paul (Secrétaire)
SOUIDI (Directeur de thèse)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Note de thèses et écrits académiques : Filière Scientifique - Option Informatique Promotion Chef d'Escadron Francoville Date de soutenance : 01/01/2011

Résumé ou extrait : > Étude : Stéganographie orientée Z4 PRESENTATION : La stéganographie, est l'art de dissimuler des données numériques dans un support numérique quelconque. Elle est pour la guerre cybernétique l'équivalent du camouflage sur le champ de bataille; et on dit que les attentats du 11 septembre 2001 auraient été commandités via la couverture de photographies pornographiques circulant sur le web. A l'heure où la numérisation affecte les conflits internationaux il nous paraît évident de la maîtriser pour mieux la contrôler. Notre objectif consiste à améliorer ce qui se fait actuellement en stéganographie via le support quaternaire appelé Z4; c'est à dire l'anneau des entiers compris entre 0 et 3. Cet anneau offrant de plus grandes possibilités que le corps binaire à deux éléments. L'intérêt d'un tel travail est donc d'ouvrir de nouveaux horizons à la recherche en stéganographie. CONTRAINTES : Les difficultés que nous avons rencontrées sont d'ordres mathématiques. Durant notre travail de recherche nous avons abordé puis utilisé des notions qui ne nous étaient pas familières. Et les mathématiques apparaissaient à plusieurs niveaux. Tout d'abord pour innover en stéganographie sous Z4, puis pour obtenir et modéliser les résultats obtenus. Enfin pour trouver un protocole stéganographique qui soit programmable en langage informatique. DEMARCHE : Tout d'abord nous avons présenté simplement la stéganographie et son rapport aux codes correcteur d'erreur. Les codes correcteur d'erreur sont récents et ont pour fonction de corriger les erreurs éventuelles d'un fichier numérique erroné. Ainsi appliquer un protocole stéganographique à un support numérique revient à insérer volontairement des erreurs constituant un message secret dans le support. Tout le travail consiste donc à trouver l'erreur à insérer pour que le code correcteur d'erreur détecte l'erreur voulue. Ensuite, nous avons tout naturellement étudié les codes correcteur d'erreur et nous nous sommes intéressés aux codes parfaits sur Z4. Nous avons alors construit de façon récursive nos propres codes correcteur d'erreur parfait sur Z4. A partir de ces codes nous nous sommes largement inspirés des grandes innovations de la stéganographie numérique binaire au point d'en faire leur analogies sous Z4. Bien sûr, ces innovations ne s'adaptaient pas immédiatement à l'anneau quaternaire, et nous avons dû énoncer et démontrer un certain nombre de lemmes qui nous autorisaient cette transposition. Ces démonstrations ont étés facilitées par la forme récursive de notre code parfait. Tout au long de notre étude, nous avons insisté sur les performances de nos différents protocoles stéganographiques. L'exploitabilité ainsi que l'opérationnalité de nos découvertes furent essentielles. C'est pourquoi nous nous sommes toujours demandés comment améliorer nos résultat, et comment les rendre

optimums. Nous avons donc comparé tous nos résultats entre eux mais aussi et surtout à une des références actuelles de la stéganographie: l'algorithme F5. Algorithme simple, qui possède un bon rapport messages dissimulés-déformation du support. Enfin, nous avons voulu implémenter notre travail de recherche mathématique sous le langage informatique C. Ainsi, nous resituions notre travail dans notre majeure informatique. RESULTATS OBTENUS : Les trois algorithmes que nous avons obtenus offrent des résultats variables. En effet, notre premier protocole stéganographique peut offrir des résultats comparables à l'algorithme F5. Par contre les multiples variantes que nous avons donné pour notre deuxième protocole stéganographique donne des résultats moins performants que le premier protocole. C'est seulement notre troisième protocole stéganographique qui est une nette amélioration du second qui nous permet d'obtenir des résultats très satisfaisants et qui sont par endroits très légèrement supérieurs à F5. LIMITES : Il subsiste néanmoins trois limites : la première est celle inhérente à notre code correcteur d'erreur. Bien que nous

Sujet(s) : algorithme
analyse des données
calcul : mathématiques
codage de données
conflit armé
cybernétique : science
informatique
langage de programmation
protection informatique
stéganographie