Coverless image steganography using partial-duplicate image retrieval
Rapport

Notes sur l'algorithme CIS-PDIR

Auteur : MBE MBE MINDJANA Loic Henri
Email : henrimbemindjana@gmail.com

16 février 2024

Table des matières

1 Problème attaqué

Pour transférer avec sécurité une information sensible contenue dans une image dite secrète, on souhaite juste la masquer ‘sans la modifier‘ avant de l'envoyer à un destinataire pour qu'il puisse la retrouver. Pour répondre à cette question les chercheurs Zhili Zhou et Al [1] ont proposés l'algorithme que nous avons nommé **CIS-PDIR** qui est sujet de cette note.

2 Algorithme CIS-PDIR

2.1 Objectif et Idée

On souhaite transférer une image secrète sans la modifier. Pour pouvoir atteindre cette objectif, l'algorithme se base sur l'idée qu'on pourrait retrouver un ensemble d'images naturelles qui la contiendrait chacune partiellement.

N'étant pas forcément pas réalisable, on cherche ainsi pour chacun des blocs (patchs) de l'image secrète, son bloc le plus similaire dans l'ensemble des blocs d'images naturelles par rapport à leurs caractéristiques (histogramme, LBP, transformé de fourier). Ce qui permet d'utiliser les images où ont été trouvées les blocs partiels les plus similaires. Le destinateur enverra donc l'ensemble ces images naturelles (des stégo-images) au destinataire qui contiennent l'image secrète, et le destinataire n'aura qu'à reconstruire cette image secrète de ces images.

2.2 Observations, limites et orientations

On peut déjà noter que les éléments les plus critiques sont ‘les positions des blocs partiels dans les images naturelles‘ qui devront être cachées par un algorithme de cryptographie symétrique ou asymétrique. De ce fait, l'implémentation peut dépendre de l'utilisateur, qui pourrait spécifier l'algorithme à utiliser.

Le principale avantage de cette approche est la capacité d'embarquement (de masquage) des images secrètes. Il serait très utilisé pour des cas où la sécurité des communications est très importante. Néanmoins il pourrait être très coûteux en temps vu la quantité d'images à traiter, malgré une préparation en amont. De plus, la considération de message secret est passée sous silence, ce qui pourrait conduire à une version de l'algorithme pour tenir compte également d'un message secret pour exploiter sa capacité d'embarquement. Celà en fixant un fenêtrage de hachage visant à obtenir une longueur de code correspondant à la longueur d'un caractère dans un système d'encodage donné.

2.3 Grandes parties de l'approche

Nous avons comme parties :

2.3.1 Construction d'une structure d'indexage

Cette étape consiste à préparer une structure pour faciliter et accélérer la recherche des blocs partiels similaires de blocs d'image secrète depuis des images naturelles, en les indexant. Ainsi segmenter l'ensemble des blocs partielles par rapport à leurs caractéristiques est très pertinent. On peut donc penser à utiliser l'algorithme de clustering

KMEANS pour les regrouper en clusters, utiliser les centroïdes pour avoir le groupe d'un bloc d'image secret, pour connaître ses potentiels blocs partiels similaires.

Pour réduire les groupes de blocs par clusters, afin de réduire le temps de recherche plus efficacement, on y ré-applique encore du clustering avec Kmeans un certain nombre de fois. Ce qui permet d'obtenir une hiérarchie de groupes, où en nœuds on a les centroïdes et en feuilles on a des ensembles restreints de blocs.

Pour pouvoir exploiter l'algorithme pas seulement pour transférer une image secrète, on va initialement regrouper les blocs partielles par leurs codes de hachage (chaîne binaire), afin de les regrouper ensuite hiérarchiquement par caractéristiques. Un message pouvant être vu comme une suite binaire, pourrait permettre d'avoir une base de recherche de blocs partiels pour la masquée par des séquences de blocs qu'on pourrait introduire dans l'image secrète. Malheureusement les auteurs ne l'ont pas suffisamment développés.

2.3.2 Masquage de l'image secrète

Cette étape visent à masquer une image secrète par l'ensemble des images naturelles contenant les blocs partielles de ses patchs (parties). Cette opération est réalisée en utilisant la hiérarchie des blocs partielles basée sur l'algorithme Kmeans, d'abord par les codes de hachage, puis par les caractéristiques. En suivant cette hiérarchie, Vue qu'on obtiendra forcément un ensemble de blocs, on va y sélectionner le bloc le plus

2.3.3 Extraction de l'image secrète

Cette étape vise à reconstruire l'image secrète approximativement en utilisant un ensemble d'images naturelles en entrée. Celà en retrouvant les blocs partielles des ses patchs dans l'ensemble des images naturelles, en utilisant leurs positions sauvegardées. puis de les replacer dans l'image finale.

Références

[1] Zhili Zhou, Yan Mu et QM Jonathan Wu. "Coverless image steganography using partial-duplicate image retrieval". In : *Soft Computing* 23.13 (2019), p. 4927-4938.