

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre de Recherche sur l'Information Scientifique et Technique



Mémoire pour l'obtention du diplôme de
Post-Graduation Spécialisée en Sécurité Informatique

Thème

**Tatouage des images cartographiques raster
pour un contrôle d'authenticité et d'intégrité**

Réalisé et présenté par :
TRYA Mohamed Lazhar.
DJOUAK Toumi.

Thème proposé et encadré par :
Mlle BOUCHAMA Samira.

Devant le jury:

Mr. A.MAREDJ	Président
Mlle N.BOULKRINAT	Examinatrice
Mr. M.SADALLAH	Examineur

Promotion 2010 / 2011

Résumé

L'utilisation de plus en plus fréquente de l'outil informatique n'a pas été sans toucher les professionnels de l'information géographique. Toutefois, la question de sécurité revient toujours lorsqu'il s'agit de transférer ou de stocker les images cartographiques, il s'avère donc nécessaire d'assurer un contrôle d'authenticité, d'intégrité de ce type d'image et préserver la confidentialité des données liées à la carte.

A cet effet, les méthodes de tatouage d'images peuvent être introduites pour satisfaire ce besoin. Ces techniques consistent à introduire dans une image des données (texte ou image) pouvant être exploitée dans plusieurs applications telles que la protection de la propriété intellectuelle, l'authentification, la protection contre les copies illégales, etc.

Appliquées aux images cartographiques, les techniques de tatouage doivent prendre en compte les spécificités de ce type d'image. Dans ce mémoire deux méthodes de tatouage des images cartographiques *raster sont proposées*. La première vise à assurer un contrôle d'authenticité en se basant sur la technique de l'étalement spectral caractérisée par sa robustesse. La deuxième exploite les bits les moins significatifs pour contrôler d'intégrité de l'image cartographique. Des outils de cryptographie sont utilisés pour garder la confidentialité des données de la carte et renforcer leur sécurité.

Mots clés : image cartographique raster, intégrité de l'image, authenticité, région d'intérêt (ROI), étalement spectral, Least Significant Bit, chiffrement, fonction de hachage.

Sommaire

Introduction générale	1
------------------------------------	---

Chapitre 1 : Sécurité informatique et cryptographie

1.1. Introduction	3
1.2. Objectif de la sécurité informatique.....	3
1.2.1. La confidentialité	3
1.2.2. L'intégrité.....	4
1.2.3. Disponibilité.....	4
1.2.4. Authentification	4
1.2.5. Non répudiation	4
1.3. Termes et définitions.....	5
1.3.1. Actifs	5
1.3.2. Vulnérabilités	5
1.3.3. Menaces.....	5
1.3.4. Attaques.....	5
1.3.5. Contre-mesures	5
1.4. Mécanismes de sécurité	5
1.4.1. Mécanismes de contrôle d'accès.....	6
1.4.2. Mécanisme de cryptographie	6
1.4.2.1. Chiffrement	7
1.4.2.2. Fonction de hachage.....	11
1.4.2.3. Signature numérique.....	13
1.5. Conclusion	14

Chapitre 2 : Le tatouage numérique des images

2.1. Introduction	15
2.2. Origines du tatouage numérique	15
2.2.1. Cryptographie.....	15
2.2.2. Stéganographie.....	15
2.3. Historique et définitions du tatouage.....	16
2.3.1. Historique.....	16

2.3.2. Définitions	17
2.4. Le principe du tatouage.....	17
2.4.1. La phase d'insertion.....	17
2.4.2. La phase de détection	18
2.5. Applications de tatouage.....	19
2.5.1. La protection des droits d'auteur	19
2.5.2. Authenticité et contrôle d'intégrité	19
2.5.3. Traçabilité dans un système commercial et la prévention de la redistribution non autorisée.....	20
2.5.4. L'indexation des images.....	20
2.5.5. Le renforcement du contenu.....	20
2.6. Les critères du tatouage	20
2.6.1. Invisibilité.....	20
2.6.2. Tatouage robuste, fragile et semi-fragile.....	21
2.6.3. Capacité de marquage.....	21
2.6.4. Sécurité	21
2.6.5. Spécificité	21
2.6.6. Sélectivité	21
2.7. Classification des méthodes de tatouage	22
2.7.1. Classification selon le type de l'algorithme	22
2.7.2. Classification selon le champ d'application.....	22
2.7.3. Classification selon le domaine d'insertion	22
2.7.3.1. Domaine spatial	22
2.7.3.2. Domaine fréquentiel	24
2.8. Evaluation des algorithmes de tatouage.....	26
2.8.1. Mesure de la qualité de l'image	26
2.8.2. Les attaques	28
2.8.2.1. Les attaques non intentionnelles	28
2.8.2.2. Les attaques intentionnelles	28
2.8.3. Banc d'essai.....	28
2.8.3.1. Stirmark	29
2.8.3.2. Checkmark	29
2.8.3.3. Optimark	29

2.8.3.4. Certimark	29
2.9. Conclusion	29
Chapitre 3 : Tatouage des données géographiques	
3.1. Introduction	31
3.2. Quelques concepts géographiques	31
3.2.1. La cartographie	31
3.2.2. La carte	32
3.2.3. Notion d'échelle	32
3.2.4. Géoréférencement	32
3.2.5. La structuration des données géographiques.....	32
3.2.5.1. L'objet géographique	32
3.2.5.2. Les données raster	33
3.2.5.3. Les données vectorielles	33
3.3. Le Système d'Information Géographique	34
3.3.1. Définitions	34
3.3.2. Principe général	34
3.3.3. Quelques domaines d'application.....	36
3.3.4. Fonctionnalités des SIG.....	36
3.4. Tatouage des données géographiques.....	37
3.4.1. Tatouage des données vectorielles.....	37
3.4.2. Tatouage des données raster.....	40
3.5. Conclusion	43
Chapitre 4: Conception et implémentation	
4.1. Introduction	44
4.2. Schéma de tatouage pour le contrôle d'authenticité	44
4.2.1. Solution proposée	44
4.2.1.1. Tatouage imperceptible	44
4.2.1.2. Tatouage par la technique de l'étalement spectral	46
4.2.1.3. Confidentialité des données	46
4.2.1.4. Tatouage par sélection d'une région d'intérêt	47
1. Schémas d'insertion et de détection de tatouage hors la région d'intérêt	48

2. Schémas d'insertion et de détection de tatouage dans la région d'intérêt.....	51
4.2.2. Résultats et analyses	52
4.2.2.1. Format des données insérées dans l'image	53
4.2.2.2. Tatouage hors la région d'intérêt.....	54
4.2.2.3 Tatouage dans la région d'intérêt	57
4.3. Schéma de tatouage pour le contrôle d'intégrité.....	58
4.3.1 Description du schéma proposé	58
4.3.1.1. Description de la méthode LSB.....	59
4.3.1.2. Etapes d'insertion / détection de la méthode LSB.....	59
4.3.1.3. Fonctions de hachage	60
4.3.1.4. Schéma d'insertion	60
4.3.1.5. Schéma de détection.....	61
4.3.2. Résultats et analyses	62
4.4. Conclusion	66
Chapitre 5 : Application	
5.1. Introduction	67
5.2. Interfaces de l'application	67
5.2.1. Menu principal.....	67
5.2.2. Interface de processus d'insertion par l'émetteur	67
5.2.3. Interface de processus de détection par le récepteur	70
5.2.4. Interface de processus d'évaluation de la qualité visuelle	73
5.3. Conclusion	73
Conclusions et perspectives.....	74
Bibliographie	76