République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Tatouage numérique basée sur la cryptographie visuelle

Ce projet est réalisé par :

- BAHLOUL Rami
- BAKHTI Rayane abderraouf
- BOUZIRA MOHAMED

Encadré par :

— Dr. BOUCHOUCHA

Remerciements

Je souhaite adresser mes plus sincères et profonds remerciements à Madame Dr Bouchoucha, enseignante de cryptographie, pour son accompagnement précieux, la richesse de son enseignement et sa grande disponibilité.

Grâce à sa pédagogie claire, son exigence intellectuelle et sa bienveillance, elle a su éveiller en moi un réel intérêt pour la cryptographie et m'a permis de mieux appréhender les concepts complexes abordés au cours de ce module.

C'est en grande partie grâce à la qualité de son encadrement que j'ai pu mener à bien ce travail avec rigueur et motivation.

Qu'elle trouve ici l'expression de ma reconnaissance et de mon profond respect.

Résumé

À travers cet exposé, nous explorons les principes théoriques et les applications concrètes du tatouage numérique lorsqu'il est combiné à la cryptographie visuelle. En croisant ces deux approches, on obtient des solutions à la fois robustes et innovantes pour protéger, authentifier et sécuriser les contenus multimédias à l'ère numérique. Cette intégration renforce significativement la sécurité des données tout en veillant à préserver leur qualité visuelle, un enjeu crucial dans de nombreux domaines d'application.

Table des matières

Table des figures

Liste des tableaux

1 Introduction

La sécurité et l'authentification des contenus multimédias sont devenues des préoccupations majeures à l'ère de la numérisation, notamment face à la propagation de la contrefaçon et à la facilité avec laquelle leur diffusion non autorisée peut être réalisée. Le tatouage numérique (ou filigrane) apparaît comme la méthode idéale pour intégrer des informations d'identification ou de traçabilité au sein même des fichiers numériques, sans en dégrader significativement la qualité. Cependant, pour sécuriser ces données intégrées, il est nécessaire d'y intégrer des mécanismes cryptographiques. C'est dans ce contexte que la cryptographie visuelle offre une solution innovante : en permettant de dissimuler des informations secrètes sous forme d'images qui ne révéleront leur contenu que sous une superposition visuelle, elle introduit une couche supplémentaire de confidentialité et d'authentification. En combinant ces deux disciplines, le tatouage numérique basé sur la cryptographie visuelle permet non seulement l'intégration subtile de l'information dans un support numérique, mais aussi la garantie que leur extraction ou véri cation est sécurisée, dans la plupart des cas sans besoin d'un traitement informatique intensif. Cette méthode à aujourd'hui des usages divers dans la protection des droits d'auteur, l'authenti cation de documents, la traçabilité ou encore la combat contre la contrefaçon.

1.1 Définition du tatouage numérique

Il s'agit d'incorporer une marque invisible, appelée tatouage ou filigrane, à un support numérique tel qu'une image, une vidéo, un fichier audio ou un fichier. Cette marque est une information relative à la propriété du créateur, à la source ou à l'authenticité du support. Contrairement au chiffrement, qui rend les données inintelligibles et nécessite une clé de déchiffrement pour les lire, le tatouage numérique préserve l'utilisation du support tout en y intégrant des informations.

1.2 Définition de la cryptographie visuelle

La cryptographie visuelle est une approche cryptographique proposée par Naor et Shamir en 1994, permettant le chiffrement visuel d'informations secrètes. Son principe constitutif consiste à diviser l'image secrète en parts qui, individuellement, ne contiennent aucune information sur l'image originale. L'information secrète n'est récupérée que lorsque les parts sont superposées dans l'espace réel, sans calculs complexes.

1.3 Importance dans la protection des données numériques

À l'ère numérique contemporaine, où la circulation et le partage de contenus sont omniprésents, le contrôle des auteurs sur le matériel, l'utilisation de documents pour produire des informations trompeuses, les monopoles de documents virtuels, la publicité aveugle sur les documents en ligne, les problèmes de contrôle :

- Sauf quelques dérogations spécifiées dans le texte, les dispositions de la présente.
- Vérification de l'authenticité et de l'intégrité des documents
- Traçabilité des contenus numériques

- Identification des manipulations frauduleuses
- Authentification des transactions électroniques

2 Fondements de la Cryptographie Visuelle

2.1 Principe du partage de secret visuel (Visual Secret Sharing - VSS)

Le partage de secret visuel (VSS) est le principe fondamental de la cryptographie visuelle. Il s'agit d'un système permettant de diviser une image secrète en n parts de telle sorte que :

- Chaque part individuellement ne révèle aucune information sur l'image secrète
- La superposition d'un nombre suffisant k de parts permet de reconstituer visuellement l'image secrète

Cette technique repose sur la perception visuelle humaine plutôt que sur des calculs mathématiques complexes pour reconstituer le secret.

2.2 Schémas de seuil (k,n)

Un schéma de seuil (k, n) en cryptographie visuelle signifie que :

- L'image secrète est divisée en n parts
- Au moins k parts sont nécessaires pour reconstituer l'image secrète ($k \leq n$)
- Moins de k parts ne révèlent aucune information sur l'image secrète

Mathématiquement, chaque pixel de l'image secrète est codé en plusieurs sous-pixels dans chaque part, selon une distribution probabiliste qui garantit les propriétés ci-dessus.

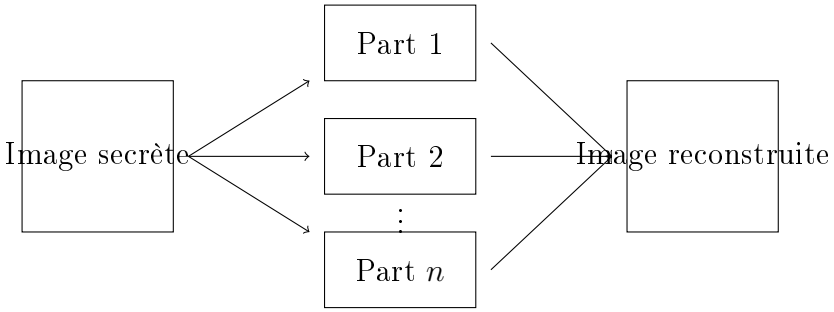

FIGURE 1 – Principe du schéma de partage de secret visuel (k, n)

2.3 Différence avec les méthodes cryptographiques traditionnelles

La cryptographie visuelle se distingue des méthodes cryptographiques traditionnelles par plusieurs aspects :

Cryptographie traditionnelle	**Cryptographie visuelle**
Utilise des algorithmes mathématiques complexes	Exploite la perception visuelle humaine
Nécessite des calculs pour chiffrer/déchiffrer	Déchiffrement par simple superposition physique
Sécurité basée sur la complexité calculatoire	Sécurité basée sur l'information théorique (inconditionnelle)
Clés numériques requises	Pas de calcul ni de clé numérique pour le déchiffrement
Vulnérable aux avancées en puissance de calcul	Résistante aux attaques par force brute

TABLE 1 – Comparaison entre cryptographie traditionnelle et cryptographie visuelle

3 Mécanismes du Tatouage Numérique

3.1 Types de tatouages

Les tatouages numériques peuvent être classifiés selon différents critères :

3.1.1 Visibilité

- **Tatouages visibles** : Perceptibles à l'œil nu, comme les logos ou filigranes apparents sur les images
- **Tatouages invisibles** : Imperceptibles pour l'utilisateur mais détectables par des algorithmes spécifiques

3.1.2 Robustesse

- **Tatouages fragiles** : Conçus pour être altérés ou détruits par la moindre modification du contenu, servant ainsi à vérifier l'intégrité
- **Tatouages semi-fragiles** : Résistent à certaines modifications bénignes mais sont altérés par des modifications significatives
- **Tatouages robustes** : Conçus pour résister à diverses transformations et attaques (compression, recadrage, filtrage, etc.)

3.1.3 Capacité d'extraction

- **Tatouages aveugles** : L'extraction ne nécessite pas l'image originale
- **Tatouages non-aveugles** : L'extraction requiert l'image originale
- **Tatouages semi-aveugles** : L'extraction nécessite certaines informations sur l'image originale, mais pas l'image complète

3.2 Domaines d'insertion

Le tatouage peut être inséré dans différents domaines de représentation de l'image :

3.2.1 Domaine spatial

L'insertion se fait directement sur les valeurs des pixels de l'image. Les méthodes courantes incluent :

- Least Significant Bit (LSB) : Modification des bits de poids faible
- Quantification d'Index de Modulation (QIM)
- Méthodes additives : ajout d'un motif de bruit à l'image

3.2.2 Domaine fréquentiel

L'insertion s'effectue après transformation de l'image dans un domaine fréquentiel :

- Transformée de Fourier Discrète (DFT)
- Transformée en Cosinus Discrète (DCT), utilisée notamment dans le format JPEG
- Transformée de Hadamard

3.2.3 Domaine des ondelettes

Utilisation de la Transformée en Ondelettes Discrète (DWT) qui offre une bonne localisation spatiale et fréquentielle :

- Insertion dans différentes sous-bandes (LL, LH, HL, HH)
- Exploitation de la multi-résolution pour un tatouage hiérarchique
- Meilleure résistance à certaines attaques comme la compression JPEG2000

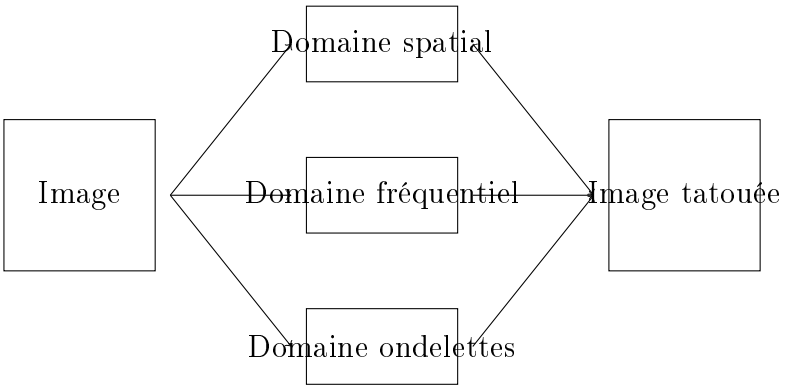

FIGURE 2 – Domaines d'insertion du tatouage numérique

3.3 Critères d'évaluation

L'efficacité d'un système de tatouage numérique est évaluée selon plusieurs critères :

3.3.1 Imperceptibilité

Mesure la capacité du tatouage à rester invisible pour l'utilisateur. Évaluée par :

- PSNR (Peak Signal-to-Noise Ratio)
- SSIM (Structural Similarity Index)
- Tests perceptuels humains

3.3.2 Robustesse

Capacité du tatouage à résister aux attaques et transformations :

- Compression avec perte (JPEG, MPEG)
- Filtrage (médian, gaussien)
- Recadrage, rotation, mise à l'échelle
- Attaques géométriques
- Attaques statistiques

3.3.3 Capacité

Volume d'information pouvant être intégré dans le contenu :

- Exprimée en bits par pixel (bpp)
- Compromis avec l'imperceptibilité et la robustesse

3.3.4 Sécurité

Résistance aux tentatives malveillantes de détection, d'extraction ou de falsification du tatouage.

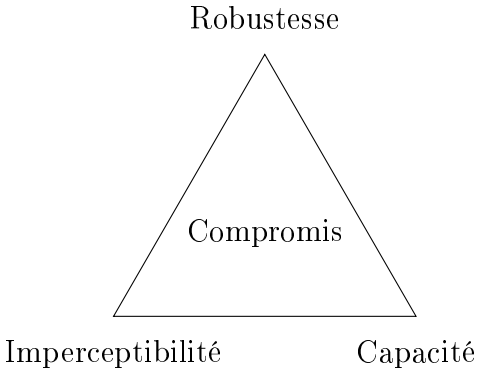

FIGURE 3 – Triangle des compromis en tatouage numérique

4 Tatouage Numérique Basé sur la Cryptographie Visuelle

4.1 Principes fondamentaux de l'approche hybride

L'approche hybride combinant tatouage numérique et cryptographie visuelle repose sur les principes suivants :

- **Division du tatouage** : Le tatouage (marque) est divisé en plusieurs parts selon les principes de la cryptographie visuelle
- **Distribution des parts** : Ces parts sont intégrées soit dans différentes régions d'une même image, soit dans différentes copies de l'image
- **Extraction et vérification** : La reconstitution et la vérification du tatouage nécessitent la superposition des parts extraites

4.2 Techniques d'intégration des deux domaines

4.2.1 Schéma à deux phases

- **Phase 1** : Application de la cryptographie visuelle pour diviser le tatouage en parts
- **Phase 2** : Intégration des parts dans le contenu hôte via des techniques de tatouage traditionnel

Algorithm 1 Schéma à deux phases pour le tatouage numérique basé sur la cryptographie visuelle

Entrée : Image hôte I, Image du tatouage W, Paramètres (k, n)
Sortie : Image tatouée I_w
// Phase 1 : Cryptographie visuelle
Générer n parts $\{S_1, S_2, ..., S_n\}$ à partir de W en utilisant un schéma (k, n)

// Phase 2 : Tatouage
for $i = 1$ to n **do**
  Sélectionner une région R_i dans I
  Insérer la part S_i dans R_i en utilisant une technique de tatouage
end for
return Image tatouée I_w

4.2.2 Schéma basé sur la confusion/diffusion

- Utilisation de la cryptographie visuelle pour la confusion (mélange des informations)
- Application de techniques de tatouage pour la diffusion (étalement du tatouage)
- Introduction de clés secrètes pour renforcer la sécurité

4.2.3 Tatouage multi-niveau

- Premier niveau : tatouage robuste classique pour la protection des droits d'auteur
- Second niveau : parts de cryptographie visuelle pour l'authentification et la vérification d'intégrité
- Possibilité d'ajouter des niveaux supplémentaires pour différents usages

4.3 Avantages par rapport aux méthodes classiques

Aspect	**Avantage**
Sécurité	Double protection par cryptographie et tatouage
Vérification visuelle	Possibilité de vérification sans équipement complexe
Résistance aux attaques ciblées	Distribution du tatouage en parts indépendantes
Preuve de propriété	Niveau de preuve renforcé par la combinaison des techniques
Flexibilité	Adaptation à différents niveaux de sécurité via les schémas (k, n)
Authentification	Détection plus fiable des manipulations frauduleuses

TABLE 2 – Avantages de l'approche hybride

5 Applications Pratiques

5.1 Protection des droits d'auteur

Le tatouage numérique basé sur la cryptographie visuelle offre une solution robuste pour la protection des droits d'auteur :

- **Identification du propriétaire** : Intégration d'informations d'identification dans les images numériques
- **Traçabilité des copies** : Création de tatouages uniques pour chaque copie distribuée (fingerprinting)
- **Preuve de propriété** : Les parts cryptographiques servent de preuve en cas de litige
- **Détection de piratage** : Identification des copies non autorisées circulant sur Internet

5.2 Authentification de documents

L'approche hybride est particulièrement adaptée à l'authentification de documents :

- **Vérification d'intégrité** : Détection de toute modification du document original
- **Authentification de source** : Confirmation de l'origine du document
- **Tatouages semi-fragiles** : Tolérance aux modifications légitimes tout en détectant les falsifications
- **Horodatage sécurisé** : Incorporation d'informations temporelles non modifiables

5.3 Détection de falsification

La combinaison du tatouage et de la cryptographie visuelle permet une détection précise des falsifications :

- **Localisation des modifications** : Identification des zones altérées dans l'image
- **Différenciation des types d'altération** : Distinction entre modifications bénignes et malveillantes
- **Résilience contre les attaques anti-tatouage** : La structure en parts multiples complique la suppression complète du tatouage
- **Vérification visuelle** : Possibilité d'une vérification rapide par superposition

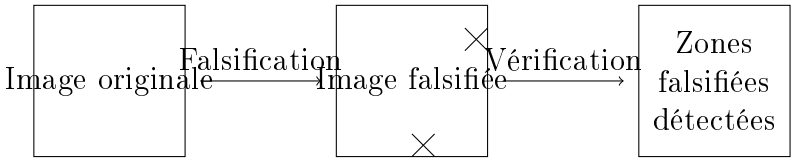

FIGURE 4 – Détection de falsification par tatouage basé sur la cryptographie visuelle

5.4 Sécurisation des documents d'identité

Les documents d'identité et les documents officiels bénéficient particulièrement de ces techniques :

- **Passeports électroniques** : Intégration de tatouages vérifiables visuellement
- **Cartes d'identité** : Association d'éléments visibles et invisibles pour une vérification à plusieurs niveaux
- **Diplômes et certificats** : Protection contre la contrefaçon
- **Billets de banque** : Combinaison d'éléments de sécurité physiques et numériques
- **Documents officiels** : Vérification d'authenticité par superposition avec une clé visuelle

6 Défis et Limitations

6.1 Résistance aux attaques

Malgré ses avantages, cette approche hybride fait face à plusieurs défis :

- **Attaques de collusion** : Combinaison de plusieurs copies tatouées pour supprimer ou altérer le tatouage
- **Attaques géométriques** : Rotation, mise à l'échelle, recadrage peuvent désynchroniser l'extraction des parts
- **Attaques par compression** : La compression avec perte (JPEG) peut dégrader significativement les parts du tatouage
- **Attaques ciblées** : Analyses statistiques visant à identifier et à supprimer les parts du tatouage

6.2 Compromis entre invisibilité et robustesse

Un défi majeur est le compromis entre :

- **Invisibilité** : L'incorporation des parts de cryptographie visuelle peut affecter la qualité perceptuelle
- **Robustesse** : Le renforcement de la robustesse nécessite généralement une modification plus importante du contenu hôte
- **Capacité** : Les schémas de cryptographie visuelle augmentent la taille des données à intégrer

6.3 Complexité algorithmique

La mise en œuvre de ces techniques présente des défis techniques :

- **Coût calculatoire** : Génération et intégration des parts nécessitant des ressources importantes

- **Synchronisation** : Alignement précis requis pour la superposition des parts
- **Expansion des pixels** : Les schémas de cryptographie visuelle traditionnels entraînent une expansion des pixels
- **Gestion des couleurs** : Extension des techniques aux images en couleur augmentant la complexité

7 Perspectives d'Évolution

7.1 Nouvelles approches hybrides

Plusieurs pistes d'évolution sont explorées :

- **Cryptographie visuelle sans expansion de pixels** : Réduction du problème d'agrandissement des images
- **Tatouage adaptatif** : Adaptation du schéma de tatouage aux caractéristiques locales de l'image
- **Schémas à seuil progressif** : Révélation graduelle de l'information en fonction du nombre de parts disponibles
- **Cryptographie visuelle probabiliste** : Amélioration du contraste et de la qualité visuelle

7.2 Intégration avec l'intelligence artificielle

L'IA offre de nouvelles perspectives pour cette technologie :

- **Optimisation par apprentissage profond** : Réseaux de neurones pour l'insertion optimale du tatouage
- **Détection robuste** : Algorithmes d'IA pour l'extraction et la reconstruction des tatouages
- **Adaptation intelligente** : Ajustement dynamique des paramètres selon le contenu
- **Contre-mesures adaptatives** : Défense contre les attaques évolutives

7.3 Adaptation aux nouvelles technologies

L'évolution technologique ouvre de nouveaux champs d'application :

- **Réalité augmentée** : Tatouages vérifiables dans les environnements AR
- **Blockchain** : Association avec les technologies de registre distribué pour l'authentification
- **Internet des objets (IoT)** : Protection légère adaptée aux contraintes des appareils IoT
- **Vidéos et flux en temps réel** : Extension des techniques aux contenus dynamiques
- **Cloud computing** : Vérification d'intégrité des données stockées dans le cloud

8 Conclusion

Le tatouage numérique basé sur la cryptographie visuelle représente une évolution significative dans le domaine de la sécurité des contenus numériques. Cette approche hybride combine les avantages de deux technologies complémentaires pour offrir des solutions robustes face aux défis contemporains de protection de l'information.

Les principales forces de cette approche résident dans :

- La double protection offerte par la combinaison des techniques
- La possibilité de vérification visuelle intuitive dans certains cas
- La flexibilité des schémas adaptables à différents niveaux de sécurité
- L'applicabilité à une large gamme de domaines, des documents d'identité aux œuvres artistiques

Si des défis subsistent en termes de compromis entre imperceptibilité, robustesse et capacité, les recherches actuelles ouvrent des perspectives prometteuses pour résoudre ces limitations. L'intégration avec l'intelligence artificielle et l'adaptation aux nouvelles technologies devraient permettre d'étendre encore le champ d'application de ces techniques dans les années à venir.

Le tatouage numérique basé sur la cryptographie visuelle s'inscrit ainsi dans une approche globale de sécurisation de l'information, essentielle à l'ère du tout numérique, où l'authenticité et l'intégrité des contenus sont devenues des préoccupations majeures pour les individus, les organisations et les États.

Références

[1] Naor, M., & Shamir, A. (1994). Visual cryptography. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 1-12). Springer, Berlin, Heidelberg.

[2] Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2007). Digital watermarking and steganography. Morgan Kaufmann.

[3] Katz, J. (2017). Digital signatures. Springer Science & Business Media.

[4] Zheng, D., Liu, Y., Zhao, J., & El Saddik, A. (2006). A survey of RST invariant image watermarking algorithms. ACM Computing Surveys, 39(2), 5-es.

[5] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment : from error visibility to structural similarity. IEEE transactions on image processing, 13(4), 600-612.

[6] Hamidi, M., Hazrati, A., & Asadi, S. (2018). A novel hybrid approach for copyright protection of images using visual cryptography and digital watermarking. Journal of Information Security and Applications, 42, 8-21.

[7] Liu, Y., Guan, Q., Zhao, X., & Cao, Y. (2019). Image forgery localization based on multi-scale convolutional neural networks. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security (pp. 85-90).

[8] Wu, H. T., Huang, J., & Shi, Y. Q. (2018). Recent advances in digital image security via visual cryptography. Journal of Visual Communication and Image Representation, 56, 256-271.

[9] Kabbaj, A. (2022). *Sécurisation des images médicales par tatouage numérique basé sur la cryptographie visuelle.* Thèse de doctorat, Université Hassan II Casablanca. Disponible sur : `https://theses.hal.science/tel-03659821`