République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de Batna 2

Faculté de mathématiques et d'informatique

Thèse

En vue de l'obtention du diplôme de
Doctorat en Informatique

Développement et mise en œuvre de méthodes de cryptographie et de tatouage pour la protection de données numériques

Présentée Par
MERABET Nour El Houda Asma

Soutenue le : 08 /07/2018

Membres du jury :

Président :	Kamal-Eddine MELKEMI	Professeur	Université de Batna 2
Rapporteur :	Redha BENZID	Professeur	Université de Batna 2
Co-rapporteur :	Lamine MELKEMI	Professeur	Université de Batna 1
Examinateurs :	Lemnouar NOUI	Professeur	Université de Batna2
	Mohamed Chaouki BABAHENINI	Professeur	Université de Biskra
	Rachid SEGHIR	*M C* A	Université de Batna2

Remerciements

Je tiens d'abord à remercier **Dieu** le tout puissant pour me munir de la volonté, la santé et de la patience pour accomplir ce travail.

J'exprime mes sincères remerciements et toute ma gratitude à mon directeur de thèse Professeur **Redha BENZID** pour son excellente qualité d'encadrement : sa disponibilité, ses conseils précieux, et pour toutes les notions de base qu'il m'a appris tout au long de ces années que ce soit dans le domaine informatique, mathématique ou électronique que je les considère comme un baguage utile pour la poursuite dans la recherche scientifique. Un vif merci a mon co-directeur de thèse Professeur **Lamine MELKEMI** pour son aide, ses qualités pédagogiques, scientifiques et humaines, qui ont contribué à l'aboutissement de cette thèse.

Je remercie vivement les honorables membres du jury qui ont accepté d'évaluer ce travail. Je remercie Professeur Kamel-Eddine MELKEMI qui a bien voulu présider le jury. Je remercie également les examinateurs : Professeur Lemnouar NOUI, Docteur SEGHIR Rachid, et Professeur Mohamed Chaouki BABAHENINI.

A ma chère promotrice de Licence et de Master Docteur Souheila BOUAM, qui est restée fidèle à moi par ses conseils continuels, son encouragement. Sa bonne humeur m'a donné la force pour donner plus aux moments difficiles.

Dédicaces

À la perle la plus rare que Dieu a créée sur terre, à ma maman qui m'a donné sans cesser, ni compter, qui sans elle ce travail n'aurait jamais été accompli.

À la personne la plus gentille que j'ai connue dans ce monde qui n'a jamais cessé de me soutenir par tout ce qu'il a, qui m'a appris toutes les valeurs nobles de la vie. À Mon père je dédié ce travail.

À mes deux chers frères, Mohamed Hicham et Djamel Eddine.

À mon âme sœur, et mon cher époux, je dédie ce travail.

À mon petit ange, mon fils Anes Menouar.

À la plus généreuse, douce, sage femme que j'ai jamais connue, ma grand-mère.

À mes oncles paternels (MERABET) et maternels (ZOUATINE).

À mes chers beaux-parents, et toute ma belle-famille BENABBAS.

Aux âmes des personnes qui nous ont quittées : mes grand-pères, ma tente Safia, Doudja et mon oncle qui a tant voulu assister à ma soutenance.

À tous mes collègues de la promotion 2012, option : Cryptographie et sécurité.

À tous ceux qui m'ont inspiré, à ceux qui m'ont par un mot, donné la force de continuer.

"The brighter you are, the more you have to learn." Don Herold

ملخص

عرف التشفير منذ العصور القديمة كأداة لحماية المعلومات السرية ضد كل عمليات القرصنة من قبل أناس مخادعين اليوم مع زيادة تطوير تكنولوجيا المعلومات والاتصالات والتوسع في استخدام البيانات الرقمية في مختلف التطبيقات، أصبح من المهم تطوير خوارزميات التشفير لضمان مستوى عال من سرية البيانات، بصفة عامة تستند عملية التشفير على استخدام المشاكل الرياضية الصعبة مثل تحليل عدد طبيعي إلى عدة عوامل أولية أو مشكل اللوغاريتم المنفصل ، مما يجعل عملية فك التشفير صعبة ومكلفة. التشفير البصري هي تقنية تقوم على مفهوم تقيسم معلومة سرية إلى عدة مفاتيح بحيث تكون عملية الكشف عن السر بتجميع مفاتيح جميع المشاركين ذلك أنه حتى في حالة فقدان مفتاح أو في حالة وجود عطب في الكمبيوتر فإن ذلك لا يعوق عملية الكشف السرية التي تتم بفضل مبدأ مخطط العتبة. في هذا السياق ، تم اقتراح العديد من مخططات التشفير المرئي. ومع ذلك ، تم تمييز عدة ثغرات نذكر الحجم الموسع للسر الذي أعيد بناؤه ، و النوعية المتدهورة للسر الذي تم الكشف عنه. مخططات أخرى للتشفير المرئي تسمح بالمشاركة السرية بين عدد محدود جداً من المشاركين مما يحد من تطبيقات التشفير المرئي. في هذه الأطروحة ، نقترح طريقة تسمح بتقيسم السر تدريجيا بالإعتماد على عمليات منطقية التي تضمن إعادة البناء التدريجي والكامل للسر في نفس الوقت. الكشف الكلي للسر يتم عندما يقوم جميع المشاركين بتكديس مفاتيحهم ، وبشكل تدريجي خلاف ذلك. يمكن إجراء المشاركة السرية مع عدد غير محدود من المشاركين ومع جميع أنواع الصور. كتطبيق نستخدم مخطط مشاركة الصور السري لـ وانج و آخرون لتقسيم صوت سري. من ناحية أخرى ، لا تزال حماية الملكية الفكرية وسلامة الرسائل لا تزال تشكل تحديات لا يمكن إنكارها. ونتيجة ذلك سوف يرتكز الجزء الثاني على تقنية الوشم الرقمي من خلال تطبيقها لنظام تقيسم السر لعلاج (مشكلة الغش) عن طريق الكشف عن أي أخطاء وتصحيحها باستخدام رمز تصحيح بسش(١٦،١١).

مفاتيح البحث:
تقسيم السر، مخطط العتبة، التشفير البصري، البيانات الرقمية، الوشم الرقمي.

Résumé

La cryptographie est connue depuis l'antiquité comme étant un outil qui sert à protéger des informations secrètes contre toutes tentations d'usurpation menées par des gens malhonnêtes. Aujourd'hui avec le développement accru des TICs et l'expansion de l'utilisation de données numériques dans diverses applications, il est devenu important de développer des algorithmes cryptographiques permettant de garantir un haut niveau de confidentialité des données. Généralement le processus de cryptage repose sur l'utilisation des problèmes mathématiques difficiles comme la factorisation des grands entiers ou le logarithme discret, ce qui rend le processus de décryptage difficile et couteux. La solution pourrait venir de la cryptographie visuelle qui est une technique reposant sur le concept de partage de secret en plusieurs clés en fournant un accès partagé à la source de telle sorte que même si l'une des clés est perdue ou l'ordinateur qui la sauvegarde est endommagé, cela ne gêne pas le processus de révélation du secret grâce au principe de schéma à seuil utilisé pour partager un secret. Dans ce contexte, de nombreux schémas de cryptographie visuelle ont été proposés. Toutefois des lacunes sont distinguées mentionnant la taille expansée du secret reconstruit, la qualité dégradée du secret révélé. Ainsi, d'autres schémas de cryptographie visuelle permettent le partage de secret entre un nombre de participants très limité ce qui restreint ses applications. Dans cette thèse, nous proposons une méthode de partage de secret progressive basée sur des opérations Booléennes qui assure une reconstruction du secret progressive et parfaite en même temps. La reconstruction parfaite est achevée quand tous les participants empilent leurs clés, et progressive autrement. Le partage de secret peut être fait avec un nombre quelconque de participants et avec tout type d'images. Comme application nous utilisons le schéma de partage des images se-

crètes de Wang et al. pour partager un secret audio. D'autre part, la protection de la propriété intellectuelle et l'intégrité de messages persistent toujours comme des défis incontestables à soulever. Conséquemment, la deuxième partie est concentrée sur un tatouage fragile en l'appliquant sur un schéma de partage de secret afin de traiter le (cheating problem) en détectant toutes altérations et les corriger en utilisant le code correcteur BCH réduit (16,11).

Mots clés : partage de secret, schéma à seuil, cryptographie visuelle, données multimédias, tatouage.

Abstract

Cryptography has been known since antiquity as a tool to protect secret informations against any attempt of usurpation by dishonest people. Today, with the increased development of ICT and the expansion of the use of digital data in various applications, it has become important to develop cryptographic algorithms to ensure a high level of confidentiality of data, while the encryption process is generally based on the use of mathematically difficult problems such as integer's factorization or discrete logarithm's problem, which make the decryption process difficult and expensive. Visual cryptography which is a technique that is based on the concept of sharing a secret into several keys and provides shared access to the source, so that even if one of the keys is lost or the computer that saves it is damaged, it does not interfere with the revelation process of secret done due to the threshold scheme. In this context, many schemes of visual cryptography have been proposed. However, many drawbacks have been identified as the expanded size of the reconstructed secret, the degraded quality of the revealed secret. Thus, other schemes of visual cryptography allow the secret sharing between a very limited number of participants which restricts the application of visual cryptography. In this thesis, we propose a method of progressive secret sharing based on Booleans operations that ensures a progressive and perfect secret reconstruction at the same time. Perfect reconstruction is achieved when all participants stack their keys, and progressive otherwise. Secret sharing can be done with unlimited number of participants and with all types of images. As an application, we use the secret image sharing scheme of Wang et al. to share an audio secret. Nevertheless, the protection of intellectual property and the integrity of messages still remains an undeniable challenge to address. Consequently, the second part, will be focused on a fragile watermark

technique by applying it on a secret sharing scheme in order to detect any alterations and correct them by using the BCH(16,11) correcting code.

key words : secret sharing, threshold scheme, visual cryptography, multimedia data, watermarking.

Liste de publications

Publication internationale

Nour El Houda Asma Merabet, Redha BENZID, Progressive image secret sharing scheme based on Boolean operations with perfect reconstruction capability. Taylor & Francis, Information Security Journal : A Global Perspective, Volume 27, 2018 - Issue 1, Pages 14-28. https://www.tandfonline.com/doi/abs/10.1080/19393555.2018.1423712.

Communications internationales

MERABET Nour El Houda Asma, Redha BENZID. A Fragile watermark based on shortened BCH (16,11) for n out of n secret sharing scheme. In : Proceedings of International Workshop on Cryptography and its Applications-IWCA'16, 26 & 27 Avril 2016, U.S.T.O-MB, ORAN-ALGERIE. https://www.univ-usto.dz/site_divers/ICCA1/IWCA_programme.pdf.

MERABET Nour El Houda Asma, Redha BENZID. n Out of n Audible Password Secret Sharing Scheme With Unexpanded Share. In : Proceedings of Conference-School on Discrete Mathematics and Computer Science. Algeria, Sidi Bel Abbès November 15 - 19, 2015, pp. 48–51. http://www.lrecits.usthb.dz/Actes%20DIMACOS2015.pdf#page=37.

Table des matières

Table des figures

Liste des tableaux

Glossaire des acronymes

AES : Advanced Encryption Standard.
ARQ : Automatic Repeat Queuing.
ASS : Audio Secret Sharing.
BB84 : Bennett Brassard 1984.
BCH : Bose Hocquenghem Chaudhur.
CRC : Cyclic Redundancy Check.
CPTWG : Copyright Protection Technical Working Group.
CV : Cryprographie Visuelle.
CVP : Cryprographie Visuelle Progressive.
CVI : Cryprographie Visuelle Incrementale.
CMJN : Cyan Magenta Jaune Noir.
CVE : Cryptographie Visuelle Evolutive.
DBP : Decomposition en Bit Plane.
DES : Data Encryption Standard.
DFT : Discrete Fourier Transform.
DOC : Document.
DCT : Discrete Cosine Transform.
DVD : Digital Versatile Disc.
DWT : Discrete Wavelet Transform.
JPEG : Joint Photographic Experts Group.
ICT : Information and Communication Technologie.
IRM : Imagerie par Résonance Magnétique.
LSB : Least Significant Bit.
LDPC : Low Density Parity Check.
MP3 : Music Player 3.
PSNR : Peak Signal Noise Ratio.
PPMC : Plus Petit Multiple Commun.
PDF : Portable Document Format.
RVB : Rouge Vert Bleu.
SVH : Système visuel humain.

SAH : Système Auditif Humain.
SDMI : Secure Digital Music Initiative.
USB : Universal Serial Bus.
TCP : Transmission Control Protocol.
4G : 4 Generations.
VSS : Visual Secret Sharing.

Première partie

Introduction sur le domaine de recherche

Introduction générale

Au cours des dernières années, avec l'arrivée d'Internet, il y a eu une explosion du nombre de personnes connectées à travers le monde, "trois milliards d'internautes ont été atteints en 2017" [21]. En conséquence, la sécurité informatique est devenue un problème critique. Chaque jour, les pirates cherchent à trouver de nouvelles failles de sécurité pour pénétrer les systèmes de chiffrement existants en visant notamment les grandes entreprises en tentant de braquer des banques et de perturber le processus électoral...etc. Selon les statistiques faites par l'entreprise américaine Symantec, le nombre de cyberattaques est en progrès incontestable, un demi-milliard d'informations personnelles ont été perdues ou volées en 2017, soit une hausse de 11,4 % par rapport à l'année 2016 [22]. Par conséquent, il est nécessaire de développer continuellement de nouveaux crypto-systèmes offrants des niveaux de sécurité de plus en plus élevés. La cryptographie est une discipline fondamentale qui utilise les mathématiques pour chiffrer des données sensibles afin d'éviter l'accès non autorisé tout en assurant l'intégrité, la confidentialité et authentification. Les données chiffrées sont généralement envoyées via des réseaux Internet ou stockées sur des ordinateurs. Par conséquent, les pirates informatiques peuvent espionner les informations mal sécurisées, ou elles peuvent être définitivement perdues en cas de l'endommagement de l'ordinateur. En outre, les systèmes cryptographiques les plus sécurisés utilisent un problème mathématique complexe dans le processus de cryptage, comme par exemple le problème du logarithme discret dans le chiffrement d'ElGamal [4] et le problème de factorisation des grands entiers dans le chiffrement de RSA [3], par conséquent, le processus de décryptage peut prendre beaucoup de temps.

Le partage de secret et le partage de secret visuel (la cryptographie visuelle) font une partie de la cryptographie. Ces dernières qui ont bénéficiés d'une attention particulière de la part des chercheurs depuis la création du premier schéma en 1994 [8], peuvent résoudre de tels problèmes en cryptant des informations confidentielles et les partageant en même temps entre des partenaires bien définis grâce au concept de schéma à seuil. Le plus grand avantage populaire dans la plupart de schémas de

partage de secret visuel se situe dans le processus de décryptage qui pourra être effectué par le système visuel humain, sans la nécessité d'outils de calcul matériels ni logiciels pour pouvoir déchiffrer les données cryptées. D'autres schémas utilisent un calcul simple lors de décryptage en utilisant des opérations Booléennes. Cependant il existe des critères importants pour qu'un schéma de partage de secret soit qualifié comme étant valide. Notons le nombre de pixels codés dans chaque transparent qui devrait être de préférence le plus petit nombre possible positif non nul ($m = 1$), le deuxième paramètre est le contraste de l'image reconstruite qui est censée être d'une bonne qualité. Aussi la possibilité de partager le secret avec le plus grand nombre possible des utilisateurs. Un autre paramètre qui rend ce schéma plus pratique c'est la possibilité de partager l'image sécrète progressivement de telle sorte que plus le nombre de personnes superposent leurs transparents plus les détails de l'image révélée apparaissent. Le partage de secret et le partage de secret visuel (la cryptographie visuelle) font une partie de la cryptographie. Ces dernières qui ont bénéficiés d'une attention particulière de la part des chercheurs depuis la création du premier schéma en 1994 [8], peuvent résoudre de tels problèmes en cryptant des informations confidentielles et les partageant en même temps entre des partenaires bien définis grâce au concept de schéma à seuil. Le plus grand avantage populaire dans la plupart de schémas de partage de secret visuel se situe dans le processus de décryptage qui pourra être effectué par le système visuel humain, sans la nécessité d'outils de calcul matériels ni logiciels pour pouvoir déchiffrer les données cryptées. D'autres schémas utilisent un calcul simple lors de décryptage en utilisant des opérations Booléennes. Cependant il existe des critères importants pour qu'un schéma de partage de secret soit qualifié comme étant valide. Notons le nombre de pixels codés dans chaque transparent qui devrait être de préférence le plus petit nombre possible positif non nul ($m = 1$), le deuxième paramètre est le contraste de l'image reconstruite qui est censée être d'une bonne qualité. Aussi la possibilité de partager le secret avec le plus grand nombre possible des utilisateurs. Un autre paramètre qui rend ce schéma plus pratique c'est la possibilité de partager l'image sécrète progressivement de telle sorte que plus le nombre de personnes superposent leurs transparents plus les détails de l'image révélée apparaissent. Le partage de secret et le partage de secret visuel (la cryptographie visuelle) font une partie de la cryptographie. Ces dernières qui ont bénéficiés d'une attention particulière de la part des chercheurs depuis la création du premier schéma en 1994 [8], peuvent résoudre de tels problèmes en cryptant des informations confidentielles et les partageant en même temps entre des partenaires bien définis grâce au concept de schéma à seuil. Le plus grand avantage populaire dans la plupart de schémas de partage de secret visuel se situe dans le processus de décryptage qui pourra être effectué par le système visuel humain, sans la nécessité d'outils de calcul matériels ni logiciels pour pouvoir déchiffrer les données cryptées. D'autres schémas utilisent un

calcul simple lors de décryptage en utilisant des opérations Booléennes. Cependant il existe des critères importants pour qu'un schéma de partage de secret soit qualifié comme étant valide. Notons le nombre de pixels codés dans chaque transparent qui devrait être de préférence le plus petit nombre possible positif non nul ($m = 1$), le deuxième paramètre est le contraste de l'image reconstruite qui est censé être d'une bonne qualité. Aussi la possibilité de partager le secret avec le plus grand nombre possible des utilisateurs. Un autre paramètre qui rend ce schéma plus pratique est la possibilité de partager l'image sécrète progressivement de telle sorte que plus le nombre de personnes superposent leurs transparents plus les détails de l'image révélée apparaissent. Le partage de secret et le partage de secret visuel (la cryptographie visuelle) font une partie de la cryptographie. Ces dernières qui ont bénéficiés d'une attention particulière de la part des chercheurs depuis la création du premier schéma en 1994 [8], peuvent résoudre de tels problèmes en cryptant des informations confidentielles et les partageant en même temps entre des partenaires bien définis grâce au concept de schéma à seuil. Le plus grand avantage populaire dans la plupart de schémas de partage de secret visuel se situe dans le processus de décryptage qui pourra être effectué par le système visuel humain, sans la nécessité d'outils de calcul matériels ni logiciels pour pouvoir déchiffrer les données cryptées. D'autres schémas utilisent un calcul simple lors de décryptage en utilisant des opérations Booléennes. Cependant il existe des critères importants pour qu'un schéma de partage de secret soit qualifié comme étant valide. Notons le nombre de pixels codés dans chaque transparent qui devrait être de préférence le plus petit nombre possible positif non nul ($m = 1$), le deuxième paramètre est le contraste de l'image reconstruite qui est censée être d'une bonne qualité. Aussi la possibilité de partager le secret avec le plus grand nombre possible des utilisateurs. Un autre paramètre qui rend ce schéma plus pratique c'est la possibilité de partager l'image sécrète progressivement de telle sorte que plus le nombre de personnes superposent leurs transparents plus les détails de l'image révélée apparaissent. Le partage de secret et le partage de secret visuel (la cryptographie visuelle) font une partie de la cryptographie. Ces dernières qui ont bénéficiés d'une attention particulière de la part des chercheurs depuis la création du premier schéma en 1994 [8], peuvent résoudre de tels problèmes en cryptant des informations confidentielles et les partageant en même temps entre des partenaires bien définis grâce au concept de schéma à seuil. Le plus grand avantage populaire dans la plupart de schémas de partage de secret visuel se situe dans le processus de décryptage qui pourra être effectué par le système visuel humain, sans la nécessité d'outils de calcul matériels ni logiciels pour pouvoir déchiffrer les données cryptées. D'autres schémas utilisent un calcul simple lors de décryptage en utilisant des opérations Booléennes. Cependant il existe des critères importants pour qu'un schéma de partage de secret soit qualifié comme étant valide. Notons le nombre de pixels codés dans chaque transparent qui devrait

être de préférence le plus petit nombre possible positif non nul ($m = 1$), le deuxième paramètre est le contraste de l'image reconstruite qui est censée être d'une bonne qualité. Aussi la possibilité de partager le secret avec le plus grand nombre possible des utilisateurs. Un autre paramètre qui rend ce schéma plus pratique c'est la possibilité de partager l'image sécrète progressivement de telle sorte que plus le nombre de personnes superposent leurs transparents plus les détails de l'image révélée apparaissent. Le partage de secret et le partage de secret visuel (la cryptographie visuelle) font une partie de la cryptographie. Ces dernières qui ont bénéficiés d'une attention particulière de la part des chercheurs depuis la création du premier schéma en 1994 [8], peuvent résoudre de tels problèmes en cryptant des informations confidentielles et les partageant en même temps entre des partenaires bien définis grâce au concept de schéma à seuil. Le plus grand avantage populaire dans la plupart de schémas de partage de secret visuel se situe dans le processus de décryptage qui pourra être effectué par le système visuel humain, sans la nécessité d'outils de calcul matériels ni logiciels pour pouvoir déchiffrer les données cryptées. D'autres schémas utilisent un calcul simple lors de décryptage en utilisant des opérations Booléennes. Cependant il existe des critères importants pour qu'un schéma de partage de secret soit qualifié comme étant valide. Notons le nombre de pixels codés dans chaque transparent qui devrait être de préférence le plus petit nombre possible positif non nul ($m = 1$), le deuxième paramètre est le contraste de l'image reconstruite qui est censée être d'une bonne qualité. Aussi la possibilité de partager le secret avec le plus grand nombre possible des utilisateurs. Un autre paramètre qui rend ce schéma plus pratique c'est la possibilité de partager l'image sécrète progressivement de telle sorte que plus le nombre de personnes superposent leurs transparents plus les détails de l'image révélée apparaissent.

Néanmoins dans la majorité des schémas de la cryptographie visuelle [23] [24] [25] [26] inclus le premier schéma conventionnel de Naor et Shamir [8], chaque pixel de l'image secrète est divisé en plusieurs blocs ce qui rend l'image reconstruite plus grande que l'image sécrète originale et affecte aussi la qualité de l'image révélée. De plus leur stockage et l'envoi sur le réseau deviennent de plus en plus couteux. Ainsi la plupart des schémas proposés ne garantissent pas la reconstruction progressive de l'image révélée. De nombreuses solutions ont été proposées afin de se débarrasser du problème de l'expansion de pixels en utilisant divers concepts notamment les probabilités, les fonctions Booléennes, les grilles aléatoires...etc. D'autres travaux s'intéressent à assurer un schéma tout en respectant la caractéristique progressive de l'image reconstruite. En effet, beaucoup de solutions proposées dans ce contexte ne satisfaient pas toutes les conditions qui garantissent la construction d'un schéma de partage de secret avec un nombre minimal de pixels codés, un plus grand nombre de personnes avec lesquelles le secret est partagé, un schéma compatible avec plusieurs types d'images

et un schéma qui assure une révélation progressive de l'image reconstruite.

D'autre part, comme toutes informations transmises à travers le réseau, même après le processus de cryptage, elles pourront être diffusées par des personnes malhonnêtes. Le tatouage numérique qui est une technique récente, permet d'intégrer une information au sein d'un signal qui peut être utilisé pour assurer l'identité du propriétaire d'un document. Le mécanisme du tatouage peut être fragile ou robuste, visible ou invisible, aveugle ou non aveugle, il peut être inséré dans le domaine fréquentiel ou spatial, chaque type s'applique selon le besoin de l'utilisateur.

À travers cette thèse nous nous sommes intéressés à deux grands volets différents, le premier volet de recherche concerne la cryptographie visuelle et le deuxième volet concerne le tatouage fragile. Nous avons proposé deux schémas, le premier schéma est un schéma de partage progressif des images secrètes basé sur des opérations Booléennes. L'autre est un tatouage numérique fragile inséré dans le domaine spatial à l'aide d'un code correcteur pour renforcer la sécurité d'un travail de partage de secret existant [10] : Ce dernier est considéré comme l'un des travaux les plus populaires qui a vaincu le problème de l'expansion de pixels tout en détectant toute altération faite sur les clés des participants (transparents) et de protéger l'image reconstruite (cheating problem). La solution consiste à insérer un tatouage fragile dans les bits de poids faibles des transparents générés à l'aide du code correcteur BCH(31,26) tout en réduisant sa taille à une taille plus petite pour qu'elle s'adapte avec la longueur paire des pixels qui sont codés sur huit bits.

Cette thèse est organisée en deux parties. La première partie présente un état de l'art sur les différents concepts utilisés, et dans la deuxième partie, nous présentons notre contribution.
La première partie est divisée en quatre chapitres et elle est organisée comme suit :

- Au cours du premier chapitre (1) nous donnons une introduction de la cryptographie en général.
- Le deuxième chapitre (2) traite le partage de secret et cryptographie visuelle particulièrement.
- Le troisième chapitre (3) est consacré à introduire le tatouage numérique.
- Le quatrième chapitre (4) définit les différents codes correcteurs existants.

La deuxième partie est organisée en elle-même en deux chapitres qui décrivent en détail nos méthodes proposées :

- Le chapitre cinq (5) décrit en détail notre schéma de partage progressif de secret basé sur des opérations Booléennes en montrant toutes les étapes suivies pour la réalisation de notre approche. Nos résultats expérimentaux sont montrés par la suite en les comparant avec les autres approches connexes. Comme applica-

tion nous utilisons le schéma de partage d'images secrètes de Wang et al. [10] pour partager un secret audio.

— Le chapitre six (6) présente un tatouage fragile en utilisant le code correcteur BCH (16,11) réduit pour un schéma (n, n) de partage de secret tout en présentant nos résultats d'évaluation.

Chapitre 1

Aperçu sur la cryptographie

Depuis l'antiquité, l'échange de données entre personnes a toujours été nécessaire. Sans doute chacun de nous a déjà envoyé des messages soit en utilisant les méthodes traditionnelles comme les lettres envoyées main dans la main, ou bien en utilisant des lettres envoyées à travers des personnes intermédiaires (personnes de confiance, facteurs...etc.). Récemment un moyen plus développé a été apparu au grand public au début des années 90 [27]. Il s'agit d'un moyen plus rapide et plus facile à y accéder qui est désormais utilisé pour l'échange de messages par un nombre d'utilisateurs très important. Il s'agit du plus grand réseau informatique accessible par tout le monde, il s'agit de la technologie Internet dite aussi "toile"! Cependant dans les deux cas, plusieurs raisons comme la perte de données et l'intrusion peuvent empêcher l'arrivée des messages à leur bonne destination. Le grand souci se réside donc dans le cas ou nos données captées sont extrêmement sensibles et confidentielles, et qu'on voudrait que seulement les personnes autorisées puissent avoir accès à ces informations.

Pour rendre nos communications plus confidentielles et pour pallier aux problèmes d'insécurité, une technique dite la cryptographie a été utilisée depuis longtemps afin de cacher les données confidentielles. Cette dernière permet de rendre une information illisible de toutes personnes illégitimes grâce aux techniques de chiffrement. Pour répondre aux besoins de l'homme; au fil du temps plusieurs techniques de la cryptographie ont été développées par les chercheurs, en créant des méthodes de chiffrement citons comme exemple la cryptographie classique, la cryptographie visuelle, la cryptographie quantique, et la cryptographie chaotique.

Chaque technique de la cryptographie a ses domaines d'utilisations, ses avantages et ses inconvénients. Les chercheurs n'ont pas cessé d'inventer de nouveaux schémas de cryptographie permettant d'améliorer les travaux de recherches précédents et de créer de méthodes de chiffrement convenables aux besoins de l'homme surtout avec l'essor des nouvelles technologies et l'explosion de l'information numérique. A travers ce chapitre nous allons décrire brièvement la cryptographie, et évoquer son histoire. Ensuite nous citons les différents types de la cryptographie et leurs domaines d'utilisation, en passant par la cryptographie classique [1], la cryptographie quantique (moderne), la cryptographie chaotique [28], et enfin la cryptographie visuelle [8] sur laquelle notre travail de recherche s'est basé.

1.1 Historique de la cryptographie

L'histoire de la cryptographie est ancienne. Au début de son apparition elle était utilisée comme étant un art pour pouvoir cacher les données secrètes, puis après un

certain temps ; elle est devenue une véritable science basée sur les mathématiques qui a attiré l'attention de plusieurs chercheurs dans différents domaines de recherche (mathématique, informatique, électronique...) afin de construire de nouveau schémas de cryptage. Au début, la cryptographie était confinée seulement dans le domaine militaire et diplomatique, mais aujourd'hui elle sert plusieurs secteurs comme le commerce électronique, les communications électroniques, l'industrie de la carte à puce, le domaine bancaire ...etc [27].

Depuis l'antiquité, plusieurs méthodes ont été utilisées pour chiffrer un secret. Notons la méthode utilisée par les grecques nommée la stéganographie qui consiste à changer les positions des lettres dans le message à dissimuler en utilisant un bâton qui s'appelle "skytale" [29]. Une autre méthode de chiffrement des hébreux nommée "Atbash" repose sur la méthode de substitution inversée des lettres du texte en clair par d'autres lettres [1]. Ces méthodes sont considérées maintenant comme étant des méthodes très simples par rapport aux méthodes qui existent aujourd'hui. Le crypto-système de Jules César [30] a été introduit cela fut plus de 2000 ans [31], il consiste à remplacer chaque lettre du texte en clair par une autre en la décalant par trois lettres de l'alphabet. Dans les années 1500 vient le chiffrement poly-alphabétique qui consiste à remplacer chaque lettre par plusieurs lettres dans l'alphabet. Notons le chiffrement le plus connu de Vigenère [30] sur lequel repose la machine Enigma mais avec un changement permanent des clés aléatoires qui a été utilisée par l'armée allemande pendant la deuxième guerre mondiale et qui a été cassé par la grande Bretagne. En 1917 Gilbert Vernam [2] a inventé un système de cryptage nommé le masque jetable en faisant référence à la clé qui doit être utilisée qu'une seul fois pour chaque message à coder. Puis en 1949 vient le mathématicien américain Claude Shannon [32] avec une notion très importante qui est la théorie de l'information [1]. Il s'agissait de donner un sens mathématique précis à la notion d'information et sa transmission à travers un canal de communication. La cryptographie à clé publique est apparue à partir des années 70 avec l'avènement du concept d'échange de clés de Diffie et Hillman en 1976 [33] [1]. Plusieurs crypto systèmes ont été développé notons le RSA (Rivest, Shamir, and Adleman) [3] en 1978, l'ELGamal en 1985 [4]. le système de cryptage DES (Data Encryption Standard) développé en 1998 [6], puis l'AES (Advanced Encryption Standard) [7] en 2001 [1]. La première expérience de la cryptographie quantique dont ses crypto systèmes reposent sur le principe de la mécanique quantiques a eu lieu en 1984 en offrant une sécurité inconditionnelle à ses utilisateurs [34]. De 1999 jusqu'au l'année 2004 un ensemble de protocoles de chiffrements ont pour le chiffrement les communications sans fil (WiFi) notons le WEP, WPA et le WPA2 [35]. Plusieurs crypto-systèmes ont montré des faiblesses et ont été cassés par les casseurs de codes qui tentent chaque jour de pirater le tout, tout en essayant de trouver la moindre lacune de sécurité dans un code

(cryptanalyse).

Probablement tout ce qui a été chiffré aujourd'hui pourra ne pas être en sécurité demain. C'est pourquoi dans les dernières années beaucoup de travaux de recherche en cryptographie ont été publiés en essayant d'améliorer les travaux de recherches précédents et de trouver de nouveaux schémas de cryptage plus sures.

1.2 La Cryptographie

La cryptographie est une science qui permet de garder les secrets en secret en se basant sur la difficulté mathématiques (Figure 1.1) afin de pouvoir chiffrer (crypter) ou bien déchiffrer (décrypter) les données confidentielles. Le cryptage consiste à cacher une information secrète et confidentielle pour la protéger de toutes sorte d'attaques [1] [31]. Le décryptage c'est le processus inverse qui rend un document secret compréhensible seulement par les personnes autorisées à le lire (Figure 1.2). Ces deux opérations se font grâce à des algorithmes de cryptage et de décryptage.
Dans la sécurité informatique, on vise pas à assurer seulement la confidentialité de données, mais aussi on vise aussi à satisfaire les critères suivants [36] :

1. Confidentialité : c'est la propriété qui permet de garder le secret illisible de toutes personnes illégitimes.
2. Intégrité : le récepteur du message doit être capable de vérifier si le message qui lui est destiné a été modifié ou non durant la transmission.
3. Non-répudiation : l'émetteur du message ne doit pas nier que c'est bien lui qui a envoyé le message [37].
4. Authentification : le récepteur du message doit être capable de vérifier son origine. Personne ne peut envoyer un message à quelqu'un et prétendre être quelqu'un d'autre.

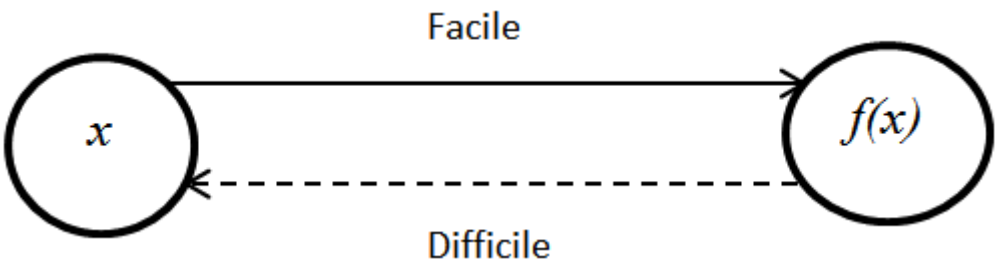


FIGURE 1.1 – Le principe mathématique de la cryptographie.

1.3 La cryptographie et les données multimédias

L'apparition de nouvelles technologies de l'information et de la communication (TIC) au grand public ont entraîné un échange de volume important de documents multimédias. En effet, les risques de modification et de piratage présentent de réelles menaces lors de l'acheminement de données de leur source vers leur destination. Les données multimédias, notons les textes, images, vidéos, les documents sonores et les animations qui sont désormais très envoyés sur les canaux de transmission sont utilisées dans plusieurs secteurs importants notons le domaine médicale, l'armé, l'audio-visuel... etc. Les informations échangées dans ces domaines sont parfois très sensibles et doivent être protégées contre l'intrusion et le piratage. Les images plus précisément sont beaucoup échangées aujourd'hui sur internet, par conséquent leur sécurité est très menacée par les pirates. La cryptographie joue un rôle primordial dans la protection de ces données, d'ailleurs beaucoup de crypto systèmes de cryptage d'images sont développés dans les différents domaines de cryptographie (classique, quantique, audible, visuelle...etc.) afin de faire face aux problèmes d'insécurité des images. D'autre techniques de protection ont aussi un rôle primordial pour garder la confidentialité comme le tatouage et la stéganographie. Chaque technique est utilisée selon le besoin de l'utilisateur et le domaine d'application.

1.3.1 Les données multimédias

Chaque jour plusieurs données sont envoyées sur les canaux de transmission. On peut distinguer deux types de données l'un est statique et l'autre et dynamique.

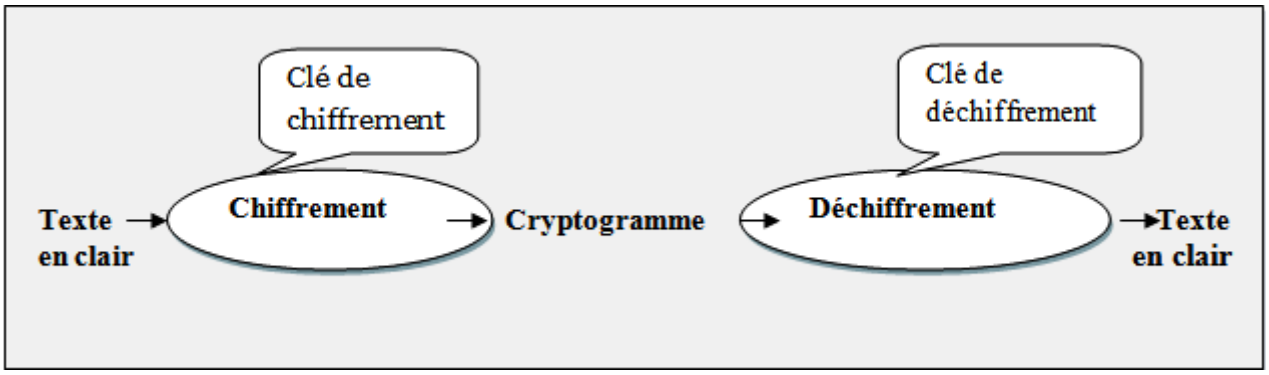


FIGURE 1.2 – Le processus de chiffrement et de déchiffrement de la cryptographie [1].

les données statiques

Ce sont des données dont le contenu n'évolue pas au fil du temps durant la lecture (statique) comme le texte et les images.

les données dynamiques

Ce sont des données dont le contenu n'évolue au fil du temps durant la lecture (dynamique) comme les vidéos et le son.

1.4 Quelques notions importantes de la cryptographie

Le problème d'envoi de messages secrets à travers un canal non sécurisé est le soucis le plus ancien en cryptographie. Les deux interlocuteurs envoient leurs messages à travers un moyen de communication tout en essayant de garder l'adversaire loin. Un schéma de cryptage appelé aussi un crypto système permet à ces deux parties de communiquer entre eux secrètement en utilisant des algorithmes de chiffrement et de déchiffrement pour obtenir un texte crypté (cipher text) et un autre décrypté (plaintext). Les deux communicants devront avoir un truc secret entre eux qui est la clé de décryptage afin de pouvoir décrypter les messages cryptés [31]. Dans cette section nous définissons des concepts populaires utilisés dans la cryptographie (résumé dans le schéma 1.3).

1.4.1 Le chiffrement

On peut l'appeler aussi le cryptage ou bien le codage. C'est le processus qui permet de coder un message en utilisant une fonction mathématique de cryptage [1] [31].

1.4.2 Le déchiffrement

On peut l'appeler aussi le décryptage ou bien le décodage. C'est le processus inverse du chiffrement qui consiste à rendre un texte chiffré en clair en utilisant une fonction mathématique de décryptage [1].

1.4.3 Clé de cryptage

Une clé de cryptage est une clé utilisée pour le chiffrement et le déchiffrement des messages. Elle est unique si le cryptage est symétrique, sinon deux clés sont utilisées l'une est publique et l'autre est privée pour le chiffrement et le déchiffrement respectivement. Une clé de cryptage est choisie parmi un nombre de valeurs appelés espace de clé sur lequel la sécurité de l'algorithme de cryptage est basée [1].

1.4.4 Crypto-système

C'est le terme utilisé pour désigner un algorithme de codage en cryptographie en passant par plusieurs étapes notons par exemple le crypto-système d'Algamal [4], de Rabin [38], de McEliece [39]...etc.

1.4.5 Cryptogramme

C'est tout simplement le message chiffré [37].

1.4.6 Cryptanalyse

Parallèlement, l'homme a mis en place des méthodes pour intercepter le secret des messages qui ne lui étaient pas destinés. C'est la cryptanalyse. La cryptanalyse est une science qui permet de déterminer soit la clé de cryptage soit le texte en clair en cherchant les points faibles dans le crypto-système grâce à différents types d'attaques[31].

1.4.7 Cryptologie

C'est la science regroupant la cryptographie et la cryptanalyse [37].

1.4.8 La stéganographie

C'est l'art qui consiste à dissimuler un message dans un autre message par exemple dans une image ou bien un texte. La différence entre la stéganographie et la cryptographie réside dans l'aspect de sécurité ou la sécurité de la cryptographie consiste à rendre

un message incompréhensible, en revanche la sécurité de la stéganographie consiste seulement à cacher un message. Plusieurs techniques de la stéganographie existent pour pouvoir cacher un message comme par exemple cacher du texte dans une image ou bien utiliser la technique de décomposition en plan de bits pour pouvoir modifier le bit de poids faible des pixels codant l'image [40].

1.4.9 Le tatouage

En cryptographie, une fois le document est décrypté, il n'est plus protégé et peut être modifié par des gens malhonnêtes et il sera presque impossible de le recouvrir. C'est pourquoi il est nécessaire d'insérer une information (marque) à l'intérieur d'un document (image, audio, vidéo... etc.) qu'on souhaite protéger pour assurer l'identité du propriétaire d'un objet. Cette technique s'appelle le tatouage de données [41].

1.4.10 La politique de la sécurité informatique

La définition d'une politique de sécurité vise tout à la fois à définir les besoins de sécurité et à élaborer des stratégies de sécurité an de protéger les biens les plus critiques. Elle vise à satisfaire les critères de sécurité cités avant comme l'authentification, la confidentialité, l'intégrité et la non-répudiation [35].

1.5 La différence entre le tatouage, la stéganographie et la cryptographie

Comme nous avons évoqué dans ce chapitre, la cryptographie sert à crypter des informations afin de les rendre indéchiffrable (secrètes), en effet les personnes ne possédant pas la clé de décryptage ne peuvent pas lire le message secret. Cependant la stéganographie permet de cacher un message secret dans un autre document afin de le rendre discret, celui qui n'a pas de clé de décryptage ne saura même pas qu'il existe un message secret caché, contrairement à la cryptographie où le hacker sait que le message représente un secret. Toutes les deux disciplines servent à résoudre le problème de sécurité de données, donc elles sont complémentaires l'une à l'autre [42].
Le tatouage fait partie de la stéganographie, les deux disciplines se ressemblent, mais le tatouage est destiné beaucoup plus pour l'authentification des images numériques, en effet après avoir décrypter le document, il n'est plus protégé. Le tatouage peut aider

à camoufler un document tout en protégeant les droits de copie, cependant la stéganographie permet de cacher une information. Les informations insérées dans le processus du tatouage peuvent avoir une relation avec le concessionnaire contrairement à la stéganographie où l'objectif consiste juste à cacher le secret. Les pirates des documents tatoués sont généralement conscients de la présence de la marque et tentent de l'extraire ou la modifier [43].

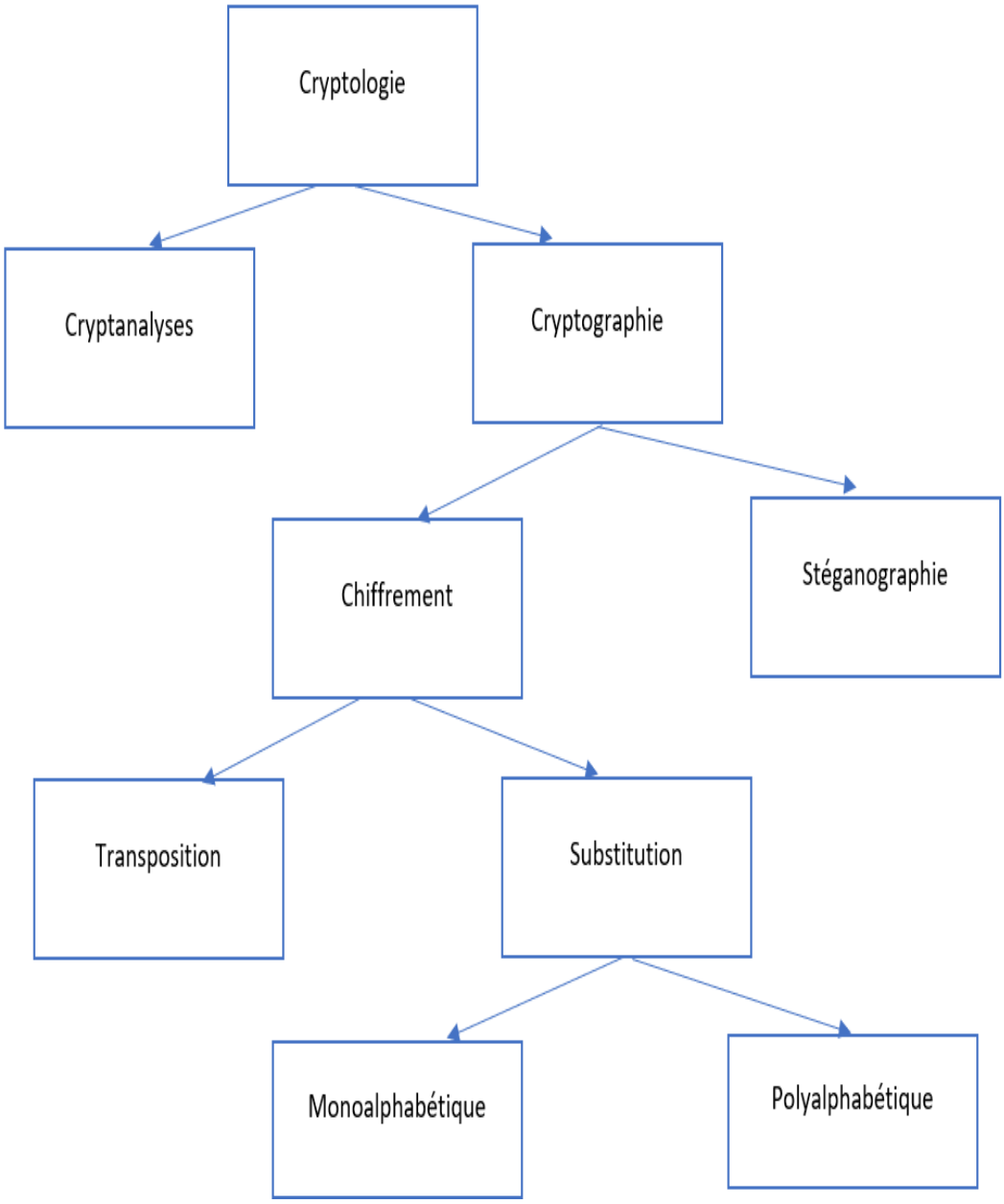


FIGURE 1.3 – Classifications des sciences reposant sur le processus de cryptage

1.6 Les grands axes de la cryptographie

La cryptographie peut être classifiée selon le type de la clé de cryptage utilisée en symétrique et asymétrique, et selon ses domaines d'utilisation en cryptographie classique, quantique, quaotique, et visuelle.

1.6.1 Selon le type de la clé utilisée

Cryptographie symétrique (à clé privée ou secrète)

C'est le mode de cryptographie le plus ancien. La cryptographie à clé privée ou (symétrique/secrète), est un mécanisme selon lequel la même clé est utilisée pour le chiffrement et le déchiffrement. La clé doit être unique et elle ne peut plus être utilisée après la fin de communication (figure 1.4). La transmission sûre de la clé reste le défi majeur de ce mode de cryptage [44].

Propriétés de la cryptographie symétrique

— La clé de transmission doit être envoyer via un canal sécurisé.
— Dans certaines méthodes de chiffrement, un espion peut appliquer une méthode dite force brute qui consiste à essayer toutes les clés jusqu'à l'obtention d'un message ayant un sens.
— La même clé est utilisée pour le chiffrement et le déchiffrement.
— La difficulté de générer des clés aléatoirement réellement, en utilisant les ordi-

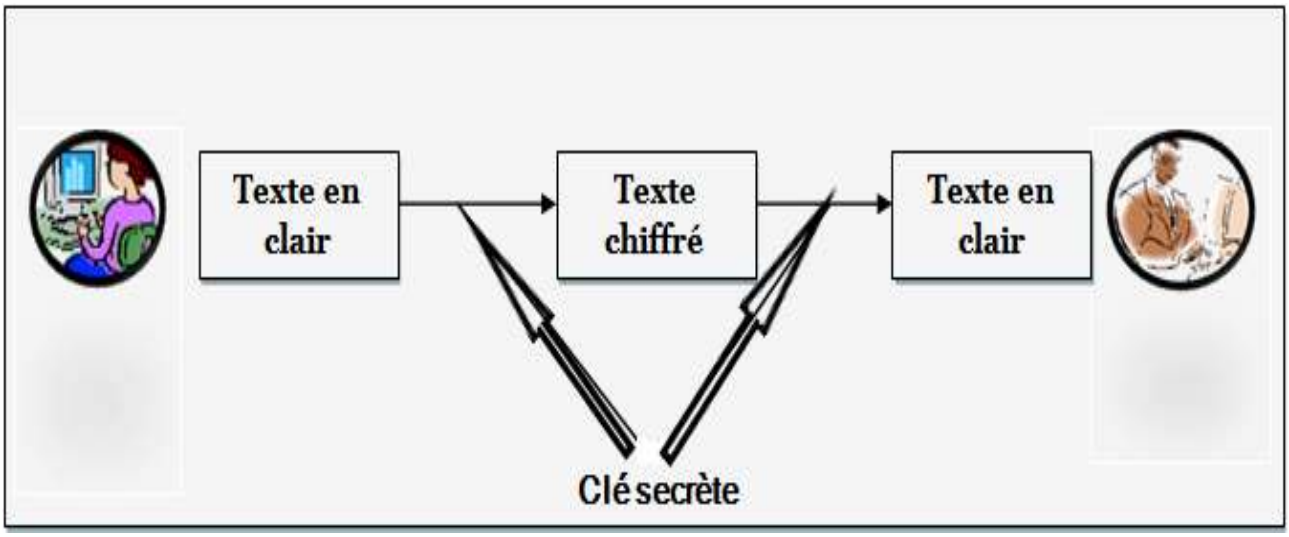


FIGURE 1.4 – schéma de la cryptographie à clé privée

nateurs ordinaires.

Cryptographie asymétrique (à clé publique)

La cryptographie à clé publique (asymétrique), quant à elle, repose sur un concept faisant intervenir une paire de clés (publique et privée) : l'une pour le chiffrement et l'autre pour le déchiffrement. La clé publique est rendue publique et distribuée librement par le destinataire qui sera ensuite utilisée pour crypter les données de l'expéditeur. La clé privée du destinataire est utilisée pour le décryptage et ne doit jamais être distribuée et doit être gardée secrète (figure 1.5). Ce mode de cryptage assure une distribution des clés sûre et l'authentification des messages [44].

Propriétés de la cryptographie asymétrique
- Le temps de déchiffrement est long par rapport au temps nécessaire au cryptage par clé symétrique.
- Deux clés différentes sont nécessaires pour le chiffrement et le déchiffrement.
- Les techniques reposant sur les fonctions à sens unique sont mathématiquement difficiles à inverser.
- L'échange de clés secrètes n'est plus nécessaire.

1.6.2 Selon ses domaines d'utilisation

Selon le besoin de l'homme, au fil des années plusieurs techniques de la cryptographie ont été développées par les chercheurs notons : la cryptographie classique, la

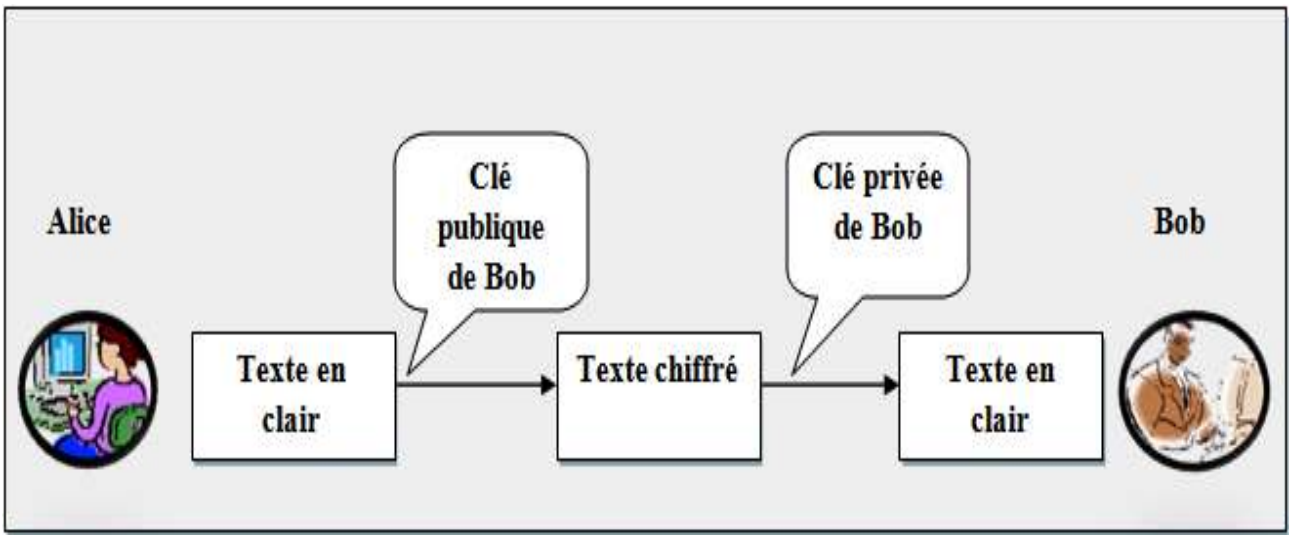


FIGURE 1.5 – Schéma de la cryptographie à clé publique

cryptographie quaotique, la cryptographie quantique et la cryptographie visuelle

La cryptographie classique

C'est le mode le plus général et le plus connu de la cryptographie qui englobe tout les crypto+systèmes standards de la cryptographie. Elle est basée sur le processus de cryptage et de décryptage de données [1].

La cryptographie quantique

La cryptographie quantique ou bien la distribution quantique des clés est une technique apparue réellement en 1984 par les deux chercheurs Bennett et Brassard qui ont mis en place le premier protocole de cryptage quantique BB84 [34]. C'est une technique qui permet de distribuer des clés de cryptage d'une façon très sure entre les deux interlocuteurs. La sécurité de la cryptographie quantique est dite inconditionnelle car elle est liée aux lois de la mécanique quantique contrairement à la cryptographie classique ou la sécurité dépend de plusieurs critères comme la taille de la clé, et la distribution de la clé privée qui doit être sûre [45].

La cryptographie chaotique

C'est un type de cryptographie basé sur la théorie du chaos [28]. Le principal objectif de la cryptographie chaotique est d'offrir un haut niveau de sécurité en se basant sur les propriétés de Chaos, tel que l'aspect aléatoire des nombres qui est l'un des plus grands challenges de la cryptographie [46].

La cryptographie sur courbes elliptiques

Il s'agit d'un concept proposé en 1985 par deux chercheurs Miller et Klob'itz en utilisant les propriétés des courbes elliptiques (collection de points). Ce type de cryptographie asymétrique est souvent employée pour l'échange d'une clé symétrique, elle est aussi utilisée pour le chiffrement des données en améliorant les primitives cryptographiques existantes comme par exemple la taille des clés [47].

La cryptographie visuelle

Des techniques peuvent décrypter le secret en utilisant les sens de l'homme comme la vue et l'ouïe ont attiré l'attention des chercheurs depuis 1994 où Naor et Shamir [8] ont créé le premier schéma de la cryptographie visuelle. Cette dernière peut décrypter le secret en utilisant le système visuel humain sans avoir besoin d'utiliser un ordinateur pour décrypter los données. La cryptographie visuelle est l'objet de notre projet de recherche.

La cryptographie audible

En 1998, Desmedt et al. [48] ont introduit une nouvelle méthode de la cryptographie inspirée de la cryptographie visuelle dont le processus de décryptage de données audibles se fait grâce au sens de l'ouïe de l'homme au lieu d'utiliser un ordinateur pour décrypter les données audibles comme le son.

1.7 Les crypto-systèmes les plus populaires de la cryptographie

Dans cette section, nous définissons quelques crypto- système les plus populaires et qui sont largement utilisés dans le domaine de cryptage.

1.7.1 Le crypto-système de César [1]

C'est un crypto-système de chiffrement par substitution mono-alphabétique le plus populaire et le plus simple qui consiste à chiffrer des lettres de l'alphabet juste en faisant un décalage simple.
Le chiffrement se fait en faisant un décalage grâce à une clé k : C=$((Msg+k) mod(26))$.
Le déchiffrement se fait en utilisant la même clé k, tel que : Msg=$((C-k) mod(26))$.

1.7.2 Le crypto-système de Veram (One Time Pad) [2]

C'est un crypto système de chiffrement par substitutions poly- alphabétique qui a été prouvé mathématiquement comme étant un protocole inviolable si la clé est géné-

rée aléatoirement et n'utilisée qu'une seul fois.
Pour chiffrer un message, on effectue un "OU exclusif (XOR)" entre le message à coder et la clé secrète : C=($message \oplus clé$).
Pour le déchiffrer, on effectue un "OU exclusif (XOR)" entre le message codé et la clé secrète : ($C \oplus clé$)=(($message \oplus clé$) $\oplus clé$)=$message$.

1.7.3 Le crypto-système RSA [3]

C'est l'algorithme de cryptographie asymétrique le plus connu. Il a été inventé en 1978 par Rivest, Shamir et Adleman. Sa sécurité repose sur la factorisation d'un nombre en facteurs premiers.
Le chiffrement se fait a l'aide d'une clé publique (e,n), tel que :

- n est le produit de deux nombres premiers p et q, n=$p*q$.
- $\phi(n)$=$(p-1)*(q-1)$.
- La valeur e est choisie de telle sorte qu'elle soit un nombre premier avec $\phi(n)$ et strictement inférieur à $\phi(n)$.
- Le Chiffrement se fait en effectuant : C=$((Msg)^e mod(n))$.

Quant au déchiffrement, il se fait a l'aide d'une clé privée (d,n), tel que :

- $(e*d=1(mod\phi(n))$.
- $(Msg$=$C^d(modn))$.

1.7.4 Le crypto-système d'El Gamal [4]

Cet algorithme fut inventé par Taher ElGamal en 1984. Il est basé sur la difficulté de trouver λ, tel que h=$g^\lambda modp$ (Problème de logarithme discret).

Les clés se construisent à partir d'un grand nombre premier p et d'un générateur g d'un grand groupe cyclique tel que :

- La clé publique est composée de : (p,y,g).
- s un nombre secret $\in (1\ldots p1)$.
- y=$g^s modp$.
- Le chiffrement du message Msg représenté par un entier modulo p se fait donc par l'émetteur comme suit :
- k un nombre aléatoire.
- C_1=$(g^k(modp))$.
- C_2=$((Msg.y^k)(modp))$.
- C=(C_1,C_2).

Le déchiffrement se fait en utilisant la clé secrète s en calculant :

— Msg=$(C_1^{-s}C_2)(mod p)$).

1.7.5 L'échange de clés Diffie Hellman [5]

C'est une méthode qui permet l'échange d'une clé secrète publiquement. L'échange se fait comme suit (Dans un groupe G d'un générateur g) :

— La personne qui souhaite envoyer la clé génère un nombre xa et calcule A=g^{xa}.
— Le récepteur choisit xb et calcule B=g^{xb}.
— L'émetteur calcule à nouveau $(B)^{xa}$.
— Le récepteur calcule à nouveau $(A)^{xb}$.
— les deux interlocuteurs ont une valeur commune qui est la clé secrète partagée.

1.7.6 Le crypto-système DES [6]

C'est un crypto-système de chiffrement symétrique par bloc en utilisant des clés de 56 bits ou 64 bits. Il a été conçu et validé par IBM en 1977. Les grandes lignes de cet Algorithme se font en ces étapes :

— Le message est découpé en blocs de 64 bits.
— Une permutation initiale est faite sur le bloc de 64 bits (permutation).
— Le bloc de 64 bits est découpé en deux blocs de 32 bits, et ces blocs sont échangés l'un avec l'autre selon un schéma de Feistel.
— Une extension du bloc de taille 32 bits à 48 bits est appliquée.
— Une opération XOR est faite entre la clé de 56 bits et le bloc de 48 bits (Ronde).
— les 48 bits sont ensuite divisés en 8 blocs de 6 bits, chaque vecteur étant finalement traité grâce à une table d'expansion
— Des transpositions sont faites sur des blocs de 32 bits grâce à une table de substitution (S-BOx).
— L'algorithme consiste en fait en 16 itérations de cryptage, et dans chaque nouvelle itération, une nouvelle clé est utilisée. A la fin de la 16ème itération, les deux blocs de 32 bits de gauche et de droite sont réunis en un seul bloc de 64 bits (permutation inverse).

1.7.7 Le crypto-système AES [7]

Vu, la faiblesse de l'algorithme DES ; un autre algorithme qui s'appelle triple DES a été inventé, puis un autre algorithme AES de chiffrement symétrique plus puissant a été développé en 2000. Les étapes de cet algorithme sont résumées en :

— Permutation : Un bloc de données de 16, 24v ou 32 octets sont permutés ensuite placés dans une matrice.
— L'opération SubBytes : consiste à substituer chaque élément de la matrice via une SBox.
— L'opération Shiftrows : cette étape implique un décalage à gauche sur les éléments de la matrice.
— L'opération MixColumns : en effectuant une opération mathématique sur chaque colonne de la matrice de données et mettant le résultat dans une nouvelle matrice.
— L'opération Addroundkey : Cette étape consiste à faire un XOR entre la matrice qui contient la clé et le bloc de donnees.

1.8 Conclusion

Dans ce chapitre nous avons évoqué la cryptographie d'une façon générale, son histoire, son principe, ses domaines d'utilisation, ses diffèrent types selon la clé utilisée notons : la cryptographie symétrique et asymétrique, et selon le domaine d'utilisation en allant de la cryptographie classique, la cryptographie quantique, la cryptographie audible, jusqu'à la cryptographie visuelle. Nous avons évoqué quelques cryptosystèmes populaires et défini des mots clés très populaires que nous allons utiliser tout au long de cette thèse. Dans le chapitre qui suit nous allons parler en détail de la cryptographie visuelle sur laquelle notre sujet de recherche s'intéresse.

Chapitre 2

Etat de l’art de la cryptographie visuelle

La plupart des techniques de la cryptographie impliquent l'envoi de données chiffrées via le réseau Internet ou le stockage de données sur des ordinateurs. Cependant, ces données peuvent être endommagées soit par les pirates qui peuvent avoir accès aux informations confidentielles quand elles sont mal sécurisées, ou bien elles peuvent être perdues en permanence lorsque l'ordinateur tombe en panne. Dans la cryptographie en générale, la plupart des crypto-systèmes utilisent des problèmes mathématiques complexes dans le processus de cryptage pour rendre l'intrusion difficile à faire voire même impossible tel que le problème du logarithme discret utilisé dans le chiffrement d'ElGamal [4] et le problème de factorisation des entiers utilisé dans le processus de cryptage du crypto système RSA [3]. Par conséquent, le processus de chiffrement peut prendre un temps très important ce qui peut être troublant pour de nombreuses applications qui nécessitent un petit espace de stockage et une grande vitesse de transmission sur le réseau. Le partage de secret qui est une technique qui vise à chiffrer les informations confidentielles et à partager un secret en même temps peut résoudre de tels problèmes. Ce concept a été proposé en même temps par Shamir [49] et Blakley [50] indépendamment en 1979. Le partage de secret est basé sur la notion de schéma à seuil.

De nombreux schémas de la cryptographie ont été développés en fonction de la notion du schéma à seuil introduit en 1979. Parmi ces schémas une technique dite la cryptographie visuelle (VC) qui a été introduite par les deux pionniers Naor et Shamir en 1994 [8]. La cryptographie visuelle a un privilège spécifique par rapport aux autres techniques de la cryptographie qui repose dans le processus de décryptage qui se fait grâce au système visuel humain sans avoir besoin d'utiliser un matériel ou bien un logiciel informatique contrairement au partage de secret traditionnel.

A travers ce chapitre nous allons évoquer en détails la cryptographie visuelle qui a reçu une attention considérable par les chercheurs grâce à ses caractéristiques spécifiques, y compris son appui sur le cryptage et le partage de secret (texte, image ...), et sa caractéristique de décryptage en utilisant le système visuel humain. Nous allons expliquer son principe et évoquer le schéma de base de la cryptographie visuelle de Naor et shamir. Nous allons évoquer les points forts et faibles de la cryptographie visuelle et voir comment ces problèmes ont été traités en citant les différents travaux proposés par les chercheurs qui sont liés à notre sujet de recherche depuis l'année 1994 jusqu'a l'année 2017.

2.1 Le partage de secret et la cryptographie visuelle

2.1.1 Le partage de secret

Le partage de secret est une technique qui permet de partager une information confidentielle entre un certain nombre de personnes en se basant sur le concept de schéma à seuil (k,n) ou (threshold scheme, (k,n)). Le concept de schéma à seuil a été proposé par Shamir en 1979 [49], il est basé sur interpolation de Lagrange pour partager un secret en n pièces. La connaissance de k $(2 \leq k \leq n)$, pièces ou plus permet la révélation du secret mais la connaissance de $k-1$, pièces ou moins ne révèle aucune information sur le secret. Bien entendu, les crypto systèmes qui sont basés sur le schéma à seuil sont convenables quand plusieurs participants souhaitent collaborer entre eux et qu'on voudrait qu'aucun utilisateur parmi eux n'ait accès à la totalité du secret.

Le concept de schéma à seuil (k,n) de Shamir [49]

Le schéma de partage de secret de Shamir consiste à diviser un secret S en plusieurs parties $C_1, C_2 ... C_n$ selon un nombre n de participants de telle sorte que ces parties représentent les clés distribuées sur chaque participant. Un nombre k, $k \leq n$ de clés définies sont nécessaires pour reconstruire le secret S de telle sorte que la connaissance d'un nombre k de clés ou plus rend le secret S facile à calculer tandis que la connaissance de $k-1$ nombre de clés rend le secret S impossible à déterminer. Ce schéma est basé sur le principe de l'interpolation de Lagrange :

- E tant donné n participants, et $k \leq n$. On choisit au hasard $k-1$ coefficients $a_1, a_2, ... a_{k-1}$ tel que le coefficients a_0 représente le secret a_0=S pour construire un polynôme $P(x)$=a_0+$a_1 x^1$+...$a_{k-1} x^{k-1}$.
- On attribut à chaque participant un point de coordonnés $(i, P(i))$ tel que pour tout i, $P(x_i)$=y_i.
- On peut trouver les coefficients de $P(x)$ par l'interpolation polynomiale, on a : $P(x)$=$\sum_{i=0}^{k} y_i * l_i$ ou l_i=$\prod \frac{x-x_i}{x_j-x_i}$ et $i \neq j$.
- On peut trouver les coefficients de $P(x)$ par interpolation, puis évaluer le secret S : S=$P(0)$, D'autre part, la connaissance de seulement $k-1$ de ces valeurs ne suffit pas pour calculer le secret S.

2.1.2 La cryptographie visuelle

La cryptographie visuelle (CV) ou bien le partage de secret visuel est une technique proposée par les deux pionniers Naor et Shamir en 1994 [8] . Elle sert à chiffrer et à partager un secret (donnée confidentielle) en même temps entre un certain nombre de personnes de confiance en utilisant le chiffrement de Vernam [2] qui a été prouvé par Claude Shannon [32] en 1949 comme étant un crypto-système incassable si la clé de cryptage est générée aléatoirement. Elle est basée sur le concept de schéma à seuil (k, n) ou threshold (k, n). Le principe de la CV consiste à garder le secret (texte, image, son...ect) dans une image et le diviser en n images aléatoires appelées pièces (shares), ombres (shadows) ou bien transparents (transparencies) de telle sorte qu'aucun transparent ne Révèle des informations secrètes. L'opération de cryptage se fait en partageant le secret entre un nombre de participants de telle sorte que le secret est reconnu à partir de n'importe quelle pièce k $(2 \leq k \leq n)$ ou plus, mais la connaissance de $k-1$ pièces ou moins ne révèle aucune information sur le secret. Le secret est révélé lorsque un nombre k $(2 \leq k \leq n)$ de transparents ou plus sont superposés l'un sur l'autre (opération de décryptage). Le processus de décryptage s'effectue par le système visuel humain qui est similaire à l'opération mathématique booléenne (OR) (ou inclusif), contrairement au partage du secret traditionnel (Blakley, 1979) dont lequel il est nécessaire de disposer d'un outil informatique matériel ou logiciel pour pouvoir décoder les données. La cryptographie visuelle pourra être appliquée dans le domaine de tatouage [51], pour gérer le contrôle d'accès pour l'authentification et l'identification [52], les transactions en ligne [53], dans le processus des élections [54] et pour protéger les droits d'auteurs [55].

2.2 Schéma de base de la cryptographie visuelle (Naor et Shamir 1994 [8])

En 1994, lors de la conférence de EUROCRYPT, Moni NAOR et Adi SHAMIR [8] ont introduit l'idée de base de la cryptographie visuelle qui est basée sur le principe du masque jetable. Dans cette section nous expliquons l'approche de base de la CV proposée par Naor et Shamir qui est baseé sur un masque jetable graphique et nous évoquons le problème principal de ce schéma traditionnel qui est l'expansion des pixels. Figure 2.1 illustre ce schéma :

Pour coder une image secrete binaire de taille $k * l$, Naor et Shamir génèrent deux images aléatoires nommées les transparents : ombre 1 et ombre 2. Mathématique-

ment, le pixel blanc est interprété comme 0 et l'opaque est interprété comme 1. Dans le processus de cryptage, chaque pixel de l'image secrète est divisé en m blocs appelés "sous-pixels". Comme la figure 2.1 le montre, chaque pixel est crypté en quatre sous-pixels, ce qui signifie que le nombre de sous-pixels dans chaque part est m=4, donc la taille de chaque transparent sera quatre fois plus grande que la taille de l'image secrète. Théoriquement, le pixel secret blanc (respectivement noir) est codé au hasard en choisissant l'une des quatre lignes de la figure 2.1 (ces lignes représentent les matrices de base. Le processus de décryptage se fait comme suit : si les pixels des deux shares sont identiques, le pixel secret sera gris, sinon le pixel secret sera noir. Le système visuel humain (SVH) interprète les pixels blancs comme étant des pixels gris, alors que les pixels noirs sont interprétés comme noirs, ce qui équivaut à l'utilisation de l'opération booléenne OR. Cependant, l'expansion de pixel entraîne de nombreux problèmes citons la qualité dégradée de l'image secrète qui perd 50% de contraste, car seuls les pixels noirs restent inchangés, tandis que les pixels blancs changent en demi-noir et demi blanc (interprété par le cerveau humain comme une couleur grise). En outre, la taille de l'image reconstruite sera quatre fois plus grande que la taille de l'image secrète originale ce qui influence sur la vitesse de transmission sur le réseau et le stockage sur les mémoires. La deuxième figure montre un exemple de la méthode de partage de secret $(2,2)$ de Naor et Shamir, sur laquelle deux participants n=2, partagent l'image secrète (Fig2.2 a), en se basant sur la méthode de Naor et Shamir, le concessionnaire fait l'expansion de chaque bit de l'image secrète m=4, ce qui fait que les deux transparents (Fig2.2 b, Fig 2.2 c) respectivement, vont devenir alors de taille quatre fois plus grande que la taille de l'image secrète, par conséquent l'image révélée va être quatre fois plus grande que l'image secrète (Fig 2.2 d).

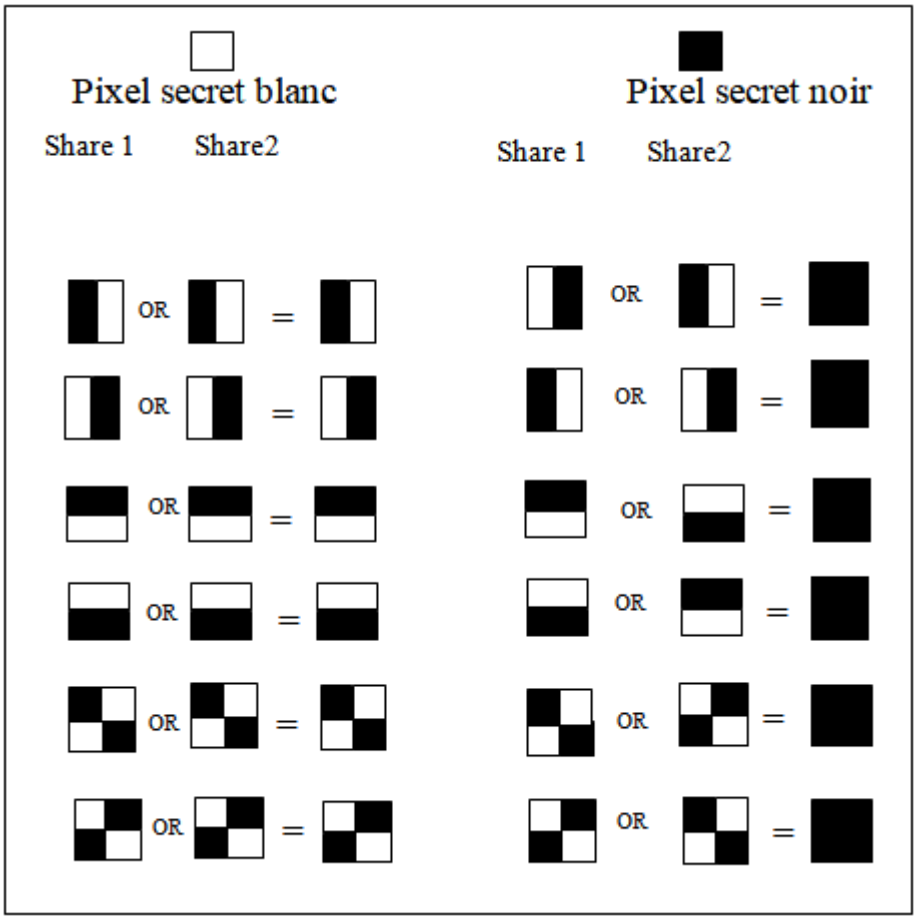
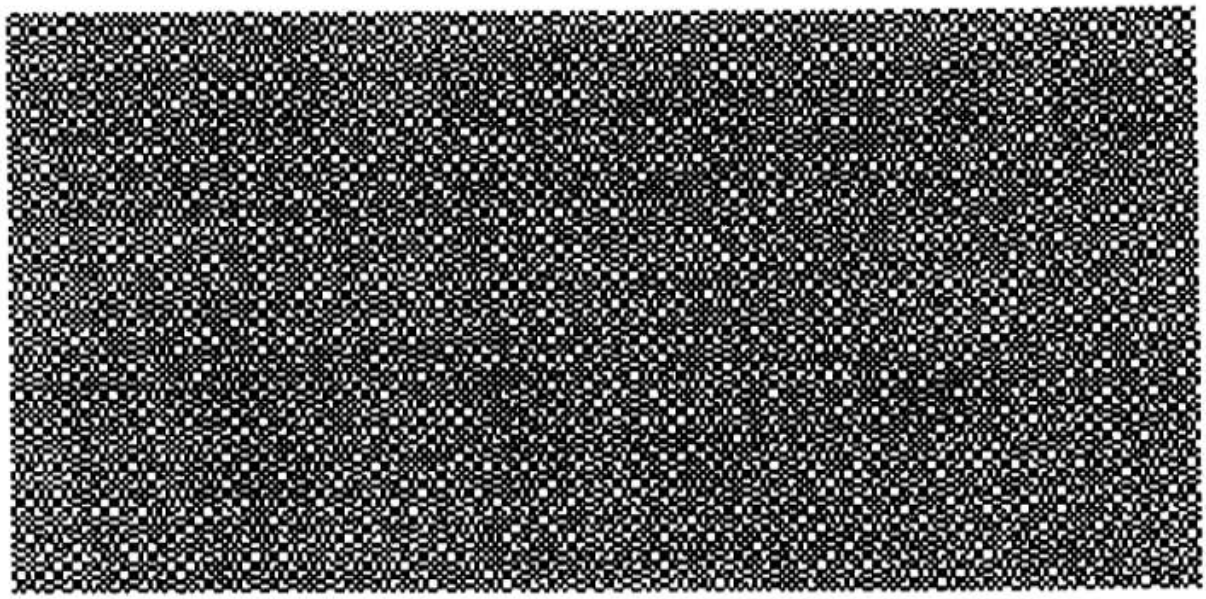
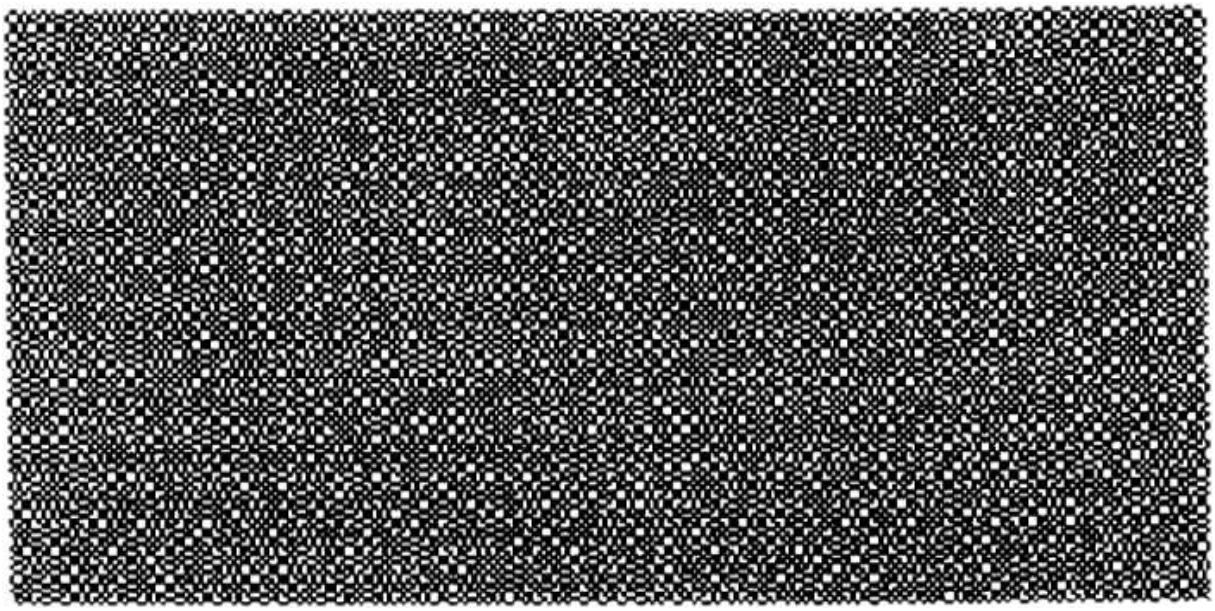


FIGURE 2.1 – La méthode de partage de secret de Naor et Shamir "two out of two" [8]

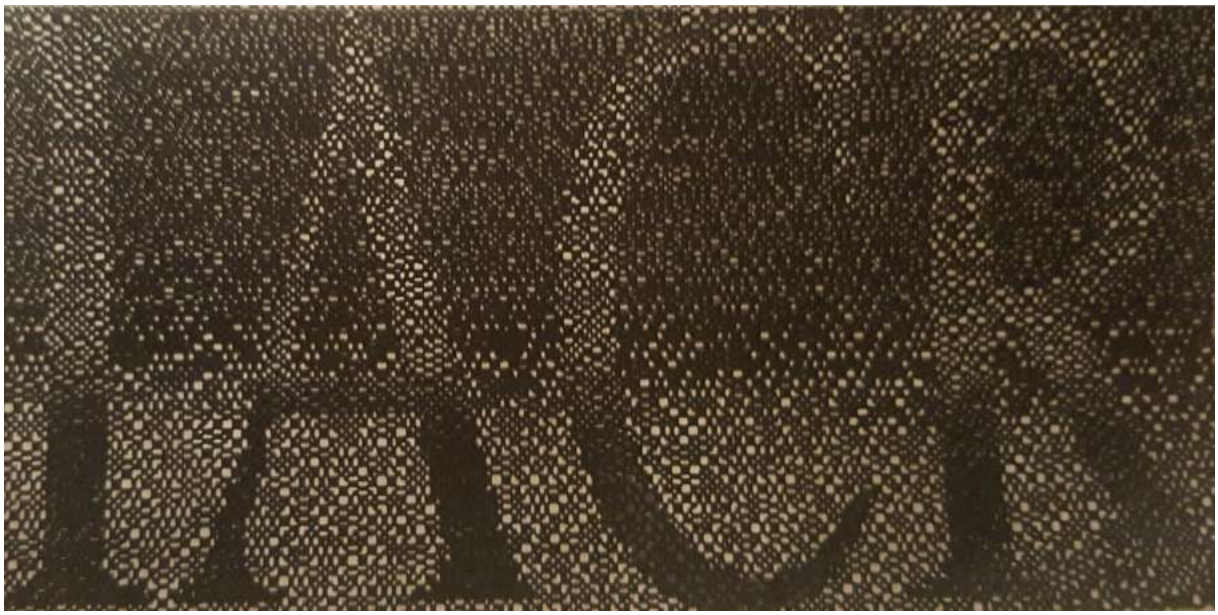
a) Le secret à partager



b) Le premier share imprimé sur un transparent et scanné.



c) Le deuxième share imprimé sur un transparent et scanné.



d) Le secret révélé à partir de la superposition des deux shares.

FIGURE 2.2 – Approche de Naor et Shamir 1994 [8].

2.3 Les principaux critères de la cryptographie visuelle

Tous les schémas de la cryptographie visuelle ont quarte paramètres importants :

1. Le nombre de pixels codés : Dans le schéma de base de Naor et Shamir, chaque pixel de l'image secrète est codé en m blocs appelés mégapixels, donc les shares et le secret reconstruits seront m fois plus grands que la taille de l'image secrète originale et la qualité de l'image originale sera aussi dégradée. En outre, quand le nombre de pixels n'est pas carré, l'image reconstruite sera déformée [56]. Ce problème nommé le problème de l'expansion des pixels est très populaire dans la cryptographie visuelle. En raison de ce problème, l'utilisation de la CV traditionnelle peut être troublante pour de nombreuses applications qui nécessitent un petit espace de stockage et une vitesse de transmission rapide sur le réseau.
2. Le contraste : représente la qualité de l'image reconstruite qui doit être au moins bien lisible, ce paramètre est mesuré en utilisant souvent le PSNR.
3. le nombre de participants n : un bon schéma de la CV doit être flexible en termes de nombre de participants. Dans la CV il existe trois sortes de schémas. Certains schémas sont $(2, n)$ ou bien two out of n, d'autre sont (k, n) ou bien k out of n et d'autres sont (n, n) ou bien n out of n.
   Un schéma $(2, n)$: veut dire que le secret est partagé seulement entre n nombre

de participants et peut-être révèlé par n'importe quel deux utilisateurs parmi n.
Pour le schéma (k,n) : le secret est partagé entre n nombre de participants, et peut-être révèlé par n'importe quel utilisateurs k utilisateurs ($2 \leq k \leq n$), parmi n.
Quant au schéma (n,n) où tous les participants doivent partager le secret entre eux.
Le schéma (k,n) est considéré comme étant le meilleur car il est possible de partager le secret entre n'importe quel nombre de participants voulu.

4. Le type des images utilisé : un bon schéma est censé d'être appliquable sur tous type d'image qu'il existe notons les images binaires, les images en niveaux de gris, les images en couleur, et les images à demi-ton (halftone).

2.4 Les propriétés de la cryptographie visuelle

1. C'est une méthode de partage de secret.
2. Le processus de décryptage est fait en utilisant le système visuel humain dans la plupart de ses schémas.
3. Dans la plupart des schémas de la cryptographie visuelle, aucun outil informatique n'est nécessaire pour pouvoir décrypter le secret.
4. C'est un système utilisé pour le cryptage et le décryptage des images.
5. C'est un système qui est inconditionnellement sécurisé vu son appuie sur l'algorithme de One time Pad [2] (Méthode de Naor et Shamir).

2.5 Quelques problèmes connus de la cryptographie visuelle

1. Le problème de l'expansion de pixel.
2. Beaucoup de schémas de la cryptographie visuelle sont restreints pour partager seulement des images binaires [57], [58].
3. Le problème d'alignement des shares [59].
4. La perte de la qualité de l'image reconstruite [59].
5. Le problème de déformation de l'image reconstruite à partir des transparents quand le nombre des pixels codés n'est pas un nombre pair[56].
6. Le problème d'assombrissement des pixels superposés pour les images en couleurs [60].

7. Le problème de triche causé par les pirates en créant des faux transparents de telle sorte que lors du décryptage, une image autre que l'image secrète originale créé par le concessionnaire est apparue [61], ainsi que la modification de l'information dans les shares [51].

2.6 Le rôle du système visuel humain dans la perception des images dans la cryptographie visuelle "L'œil voit, le cerveau perçoit"

L'œil humain, ou le système visuel humain (SVH) est l'une des modalités sensorielles les plus développées chez l'homme, il joût un rôle primordial pour notre vision, cela est fait grâce aux composants de l'œil qui est un globe d'environ 25 millimètres de diamètre composé de différents éléments [62], dont :

— La cornée : qui agit comme une fenêtre par laquelle la lumière pénètre dans l'œil.
— Le cristallin : il permet d'effectuer les réglages indispensables à la focalisation des objets quel que soit leur distance (zoom).
— La rétine qui capte l'image au fond de l'œil à la manière d'un écran,
— Les cônes : ces derniers permettent de percevoir la lumière du jour et les couleurs.
— Les bâtonnets : donnent une vision des formes dans l'obscurité.
— L'iris : est la partie de l'œil colorée, c'est elle qui donne aux yeux une couleur.

En effet l'œil ne fournit que la base de la perception visuelle. C'est notre cerveau qui fait le travail le plus complexe d'analyse, ce dernier reçoit l'image sous forme d'impulsions électriques et l'interprète par la rétine via le nerf optique.

2.6.1 Perception des images noir et blanc

Les bâtonnets permettent une vision en noir et blanc puisqu'ils ne sont sensibles qu'à l'intensité lumineuse. Ce sont eux qui sont responsables de notre vision nocturne [62].

2.6.2 Perception des images en couleurs

L'œil est capable de percevoir jusqu'à 200 nuances par couleurs grâce à trois types de signaux donnés par trois types de cônes, certains cônes sont principalement sensibles dans le rouge, d'autres dans le vert et enfin les derniers dans le bleu. Les différents contrastes seront perçus par les bâtonnets qui réagissent uniquement à l'intensité lumineuse. [63]

En effet, l'étude de la perception visuelle est intéressante. Elle peut nous mettre sur la voie de nouveaux algorithmes en remettant les mécanismes naturels dans un système naturel, la lumière est captée par l'œil et transmise vers le cerveau par le nerf optique, alors que dans un ordinateur, la lumière est captée par un récepteur, et transmise par les câbles vers l'écran [64].

2.7 Les différents travaux de recherche de la cryptographie visuelle

De nombreuses techniques du partage de secret visuel ont enrichit l'archive de publications tout en essayant d'améliorer les lacunes qui y existent et de proposer de nouvelles approches de la cryptographie visuelle en cherchant à respecter les quatre critères cités en dessus (contraste, le nombre de pixels codés, le nombre possible de participants, type d'images) afin de trouver des schémas (idéaux) répondant aux besoins de l'utilisateur.

2.7.1 Schémas probabilistes de la cryptographie visuelle

Ce modèle de la cryptographie visuelle a été présenté pour la première fois par Yang [65]. Il résout le problème le plus populaire de la CV qui est l'expansion du pixel ainsi que le problème de complexité. Quoique dans ce modèle, la taille de chaque pixel de l'image originale est de même taille que l'image reconstruite de tous les transparents, le principal inconvénient se réside dans la mauvaise reconstruction des pixels noirs. En effet ce schéma calcule la fréquence avec laquelle les pixels blancs apparaissent dans la région blanche (respectivement noire) pour calculer la qualité de l'image reconstruite. La probabilité que les pixels blancs soient reconstruits correctement est plus grande que celle des pixels noirs, d'où le manque de justesse de l'image reconstruite. De nom-

breuses solutions proposées ont été publiées dans le but de pallier au problème de l'expansion du pixel en se basant sur le concept probabiliste introduit par Yang, tel que le schéma de Wang et al.[10] qui ont proposé une méthode probabiliste $(2,n)$ pour les images binaires où la taille de l'image reconstruite est identique à l'image secrète. Notez que le schéma de Wang et al. $(2,n)$ a été revisité par Ulutas et al. [66], D'autre schémas probabilistes de partage de secret visuel ont été présentés notons ceux de : Cimato et al. [67], Wang et al. [68], et YanChing[69].

2.7.2 La cryptographie visuelle basée sur la grille aléatoire

En 1987, trois méthodes de cryptage d'images et de formes basées sur la grille aléatoire ont été présentées par Kafri et Karen [70] pour surmonter le problème de l'expansion des pixels, plusieurs travaux ont été publié dans le même contexte tels que les travaux de Shyu et Shyong en 2007 [71], Chen et al. [72] en 2009, Wu Sun en 2013 [73], et Yan et al. en 2015 [74].

2.7.3 La cryptographie visuelle basée sur l'opération booléenne XOR

L'algèbre de Boole joue aussi un rôle important dans le but de créer des schémas de la cryptographie visuelle sans augmenter le nombre de pixels de l'image secrète. Les opérations booléennes sont connues par leur simplicité et facilité d'implémentation. Le premier schéma qui a été introduit dans ce contexte est fait par Tuyls et al. [25]. Dans les trois schémas $(2,n)$, (k,n) et (n,n) de Tuyls et al. l'opération Booléenne XOR (ou exclusif) est utilisée dans le processus de décryptage au lieu de l'opération OR (ou inclusif) afin d'obtenir un schéma avec un meilleure contraste. Puis en 2007, Wang et al. [10] ont proposé deux schémas : un schéma déterministe (n,n) pour les images en couleurs sans augmenter le nombre de pixels codés. Notez que le schéma de Wang et al. (n,n) était revisité par Chao Lin [75] pour construire un schéma de partage de secret plus général (k,n). Dong et al. [76] suggèrent également un schéma de partage secret $(2,n)$ pour les images binaires afin d'améliorer le contraste du schéma de Tuyls $(2,n)$, et étendre le schéma pour qu'il soit disponible aux images en niveaux de gris et en couleur, l'image secrète est reconstruite précisément en utilisant simplement les opérations XOR et OU. Un autre schéma $(2,n)$ a été proposé par Tapasy et al. [77] pour les images binaires, en niveaux de gris et en couleurs où la taille des transparents et l'image récupérée est identique à l'image secrète originale, et seulement des opérations booléennes XOR et OU sont utilisées pour reconstruire l'image secrète.

2.7.4 La cryptographie visuelle halftone

Une technique dite halftone, trame demi-teintes ou demi-ton qui est très utilisée depuis longtemps dans les applications d'impression et qui a pour but d'obtenir une image avec une résolution d'amplitude moins que celle de l'image originale mais proche d'elle perceptuellement pour le système visuel humain, en faisant la conversion de 8-bits d'une image en niveaux de gris en 1 seul bit. Cette dernière est aussi exploitée pour enrichir le domaine de la cryptographie visuelle, introduit par les chercheurs Zhou et al. [11], Nakajima et al.[78] qui étaient parmi les premiers qui ont proposé une méthode de partage de secret visuel qui consiste à convertir une image secrète en niveaux de gris en une image binaire, puis coder cette image en n halftone transparents significatifs en se basant sur le principe de la distribution d'erreur [79] ou bien le tramage [80] pour appliquer le processus de halftone. Cette méthode a donné une qualité visuelle de l'image reconstruite meilleure que tout les schémas qui en existaient à cette époque (année 2006) [81]. Dans le même contexte de la cryptographie visuelle à demi-ton, beaucoup de schémas ont été publiés mentionnant les travaux de Alex et al. [82], Wang et al. [83], et Chan et al. [84]. La figure 2.3 montre un schéma de cryptographie visuelle halftone dont le secret est révèlé à partir de la superposition des shares c et d.

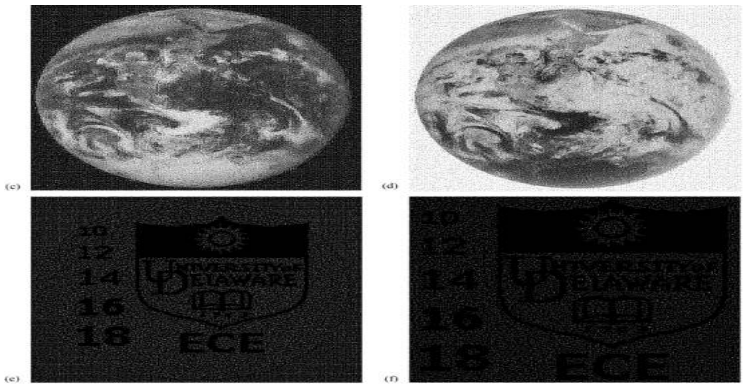


FIGURE 2.3 – Schéma de cryptographie visuelle halftone [11]

2.7.5 La cryptographie visuelle étendue

Contrairement à la cryptographie conventionnelle basée sur le schéma à seuil (k, n) dont lequel n'importe quel nombre de k transparents ou plus sont suffisants pour pouvoir reconstruire le secret et les transparents utilisés dans la cryptographie visuelle traditionnelle sont complètement aléatoires et n'ont pas une signification sémantique.

Les transparents utilisés pour la cryptographie visuelle étendue ont une signification sémantique pour que les participants puissent reconnaitre leur shares ce qui diminue toute tentative d'intrusion. Ce modèle est proposé par Ateniese et al [85] en 1996, puis plusieurs schémas de la cryptographie visuelle étendus sont apparus comme ceux proposés par Nakajima et al.[78], Lee et al. [86] et Kang et al. [87]. La figure 2.4 montre un schéma de cryptographie visuelle étendu dont lequel le secret est révélé à partir des deux shares significatifs (airplane, Lena).

FIGURE 2.4 – Schéma de cryptographie visuelle étendue [12]

2.7.6 La cryptographie visuelle basée sur la décomposition en plans de bits

Lukac and Plataniotis [88] ont présenté un schéma de cryptographie visuelle basé sur la décomposition en plans de bits (DPB), qui consiste à diviser une image en niveaux de gris en huit plans $PL_0, PL_1, ...PL_n$ et puis crypter chaque plan séparément en utilisant l'algorithme de Kafri et Karen[70]. La technique de décomposition en plans de bits est utilisée au lieu d'utiliser la technique du demi-ton. En conséquence, la qualité de l'image reconstruite dans leur schéma est meilleure que celle obtenue en utilisant des techniques de tramage mentionnent les travaux dans : [84], [81]. Cependant, dans ce schéma, l'image récupérée est deux fois plus grande que l'image secrète originale, donc ce schéma souffre du même problème présenté dans la CV traditionnelle. En 2013 Liu et al. [89] ont amélioré le schéma de Lukac et Palestinous en utilisant la technique de base de la grille aléatoire (random grid). Bien que le schéma de Liu et al. n'utilise pas d'expansion de pixels. Il a l'inconvénient de partager une image secrète seulement entre deux nombres de participants. Les techniques basées sur la décomposition en plans de bits prennent un temps important lors de cryptage et de décryptage à chaque fois que la taille de l'image secrète est grande, ce qui contredit le principe de la cryptographie visuelle traditionnelle où ce n'est pas nécessaire de faire un calcul important lors de décryptage dans la majorité des schémas de la CV. La table 2.1 résume les différents travaux de la cryptographie visuelle.

2.7.7 La cryptographie visuelle multiple

La cryptographie visuelle multiples consiste à cacher un secret ou plus dans une image. Cette approche a été initiée par Wu et Chen [90] en 2004 dans laquelle lorsqu'on superpose deux shares le premier secret se révèle, et quand on fait une rotation de 90° sur le premier share et le met sur le deuxième share, le deuxième secret se révèle, sachant que la forme des shares est soit circulaire, rectangulaire ou bien cylindrique. Plusieurs améliorations de la cryptographie visuelle multiples ont été faites, pour pouvoir cacher plus de deux secrets dans la même image et pour obtenir une bonne qualité du secret reconstruit dont lesquelles le secret peut être révélé en faisant n'importe quelle rotation de n'importe quel ongle de 0° jusqu'a 360° et n'ont pas en faisant une rotation précise. Sachant que les shares utilisés dans ce type sont circulaires ou bien cylindrique ce qui rend le processus de décodage un peu difficile contrairement à la CV traditionnelle dont laquelle la forme des shares est rectangulaire ce qui facilite le décodage lors de la superposition des coins des rectangles [60]. Dans ce type de la cryptographie visuelle multiple, le concessionnaire ajoute des informations sup-

plémentaires sur les shares comme un marquage ou des points [59] pour qu'il puisse se rappeler ou aligner les transparents. Des schémas ont été rapportés par : Feng et al. [91] en 2008, Chen et al. [13] en 2011, Chen et al. et [92] en 2014. La figure 2.5 montre un schéma de cryptographie visuelle multiple dont lequel trois secrets se révèlent à partir de la superposition des quatre shares.

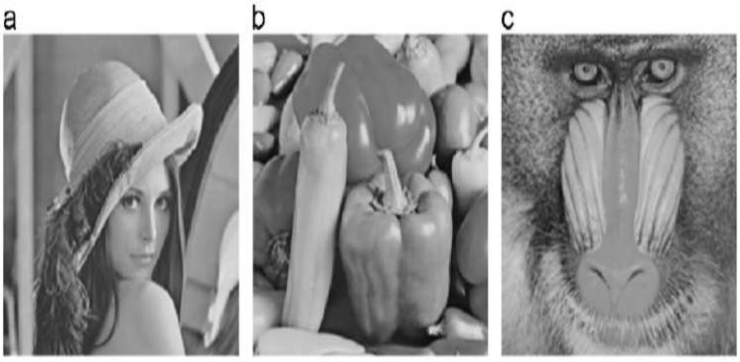


FIGURE 2.5 – Schéma de cryptographie visuelle multiple [13]

2.7.8 La cryptographie visuelle pour les images en couleur

Les images en niveaux de gris et en couleurs sont très utilisées aujourd'hui. Après l'approche de Naor et Shamir [8], les chercheurs ont pensé à créer un schéma de la cryptographie visuelle ou l'image secrète est soit en niveaux de gris soit en couleur, le premier schéma de la cryptographie visuelle en couleur est apparu en 1996 par Droste et Stefan [93]. Comme nous avons montré auparavant que dans la cryptographie visuelle pour les images binaire, le système visuel humain interprète les deux pixels superposés comme étant un pixel noir si au moins un des deux pixels est noir, sinon il interprète le pixel comme étant un pixel blanc si les deux pixels superposés sont blancs. Dans les images en couleur c'est différent puisqu'un pixel est représenté sur plus d'un bit [60]. Le problème le plus connu de la cryptographie visuelle pour les images en couleurs est la couleur qui devient plus foncée que celle de l'image originale dû au fait que lors de l'alignements des deux pixels des transparents de la même couleur, la couleur du pixel superposé devient plus foncée, ce qui résulte une perte de qualité de l'image reconstruite, par exemple dans le cas des deux pixels rouges, on obtient un pixel de couleur rouge bordeaux [94]. Une parmi les approches qui aide à simplifier le travail de la cryptographie visuelle sur les images en couleur c'est d'appliquer un processus halftone [11] sur chacun des trois plans rouge, vert et bleu (RGB) puis faire un traitement de la cryptographie visuelle sur chaque plan noir et blanc, ce processus peut mi-

nimiser le problème de nombre de pixels élevé, mais la qualité de l'image reconstruite reste pauvre, citons les travaux de [14], [95], [96]. Une autre approche qui simplifie le travail sur les images en couleur consiste à convertir les pixels de l'image secrète en binaire et puis crypter l'image secrète en plan de bits, en effet cette méthode nécessite un calcul lors du décryptage et une augmentation du nombre de pixels codés, cependant l'image secrète est reconstruite parfaitement comme dans les schémas discutés dans [97], et [98]. La figure 2.6 montre un schéma de cryptographie visuelle pour partager une image secrète en couleur.

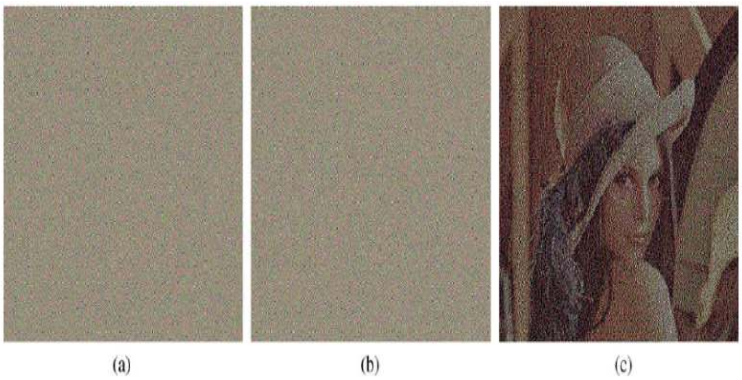


FIGURE 2.6 – Schéma de cryptographie visuelle pour les images en couleur [14]

2.7.9 Le partage progressif de secret

D'autre part, d'autres systèmes de partage de secret utilisent le concept de mécanisme de schéma à seuil différemment afin que le secret puisse être reconstruit progressivement, même s'il y a moins de shares que le seuil fixé k. Ces schémas incluent : la cryptographie visuelle progressive [15], le partage de secret visuel progressif basé sur des blocs avec l'expansion des pixels [99], et le partage de secret visuel progressif basé sur des blocs sans expansion des pixels [17], le partage évolutif des images secrètes [18], et le système de cryptage visuel incrémentale [100], contrairement à la CV conventionnelle qui utilise le concept "tout ou Rien", de telle sorte que si le nombre de shares empilés est inférieur au seuil fixé k, aucune information ne peut être donnée sur le secret. En d'autres termes, le processus de décryptage révèle soit l'image entière, soit rien. Cependant, cette caractéristique peut limiter les applications de la CV lorsque l'utilisateur voudrait partager le secret progressivement. Dans ces méthodes de partage de secret progressives, l'image secrète reconstruite peut être visualisée progressivement en fonction du nombre de shares empilés et chacune de ces méthodes est différente de l'autre dans la manière utilisée pour voir le secret graduellement.

La cryptographie visuelle progressive (CVP)

Ce modèle a été introduit par Jin et al [15] en 2005. Dans les schémas de la CVP, le contraste de l'image secrète reconstruite s'améliore graduellement chaque fois qu'un nouveau participant superpose son share avec un autre. Des approches de la cryptographie visuelle progressive ont été publiées citons les schémas dans [101], [102] et [103]. La figure 2.7 montre un schéma de cryptographie visuelle pour partager une image secrète dont le contraste s'évolue graduellement.

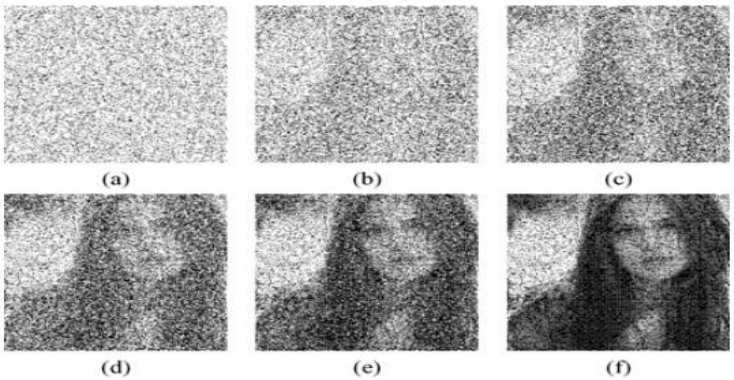


FIGURE 2.7 – Schéma de cryptographie visuelle progressive [15]

La cryptographie visuelle incrémentale (CVI)

Dans certains systèmes de partage progressif de secret, on n'aura pas besoin de révéler toute l'image progressivement en améliorant le contraste, mais on voudrait que seulement des parties bien définies de l'image soient révélées graduellement. C'est le cas de système de cryptage visuel incrémental qui a été introduit par Wang en 2009 [100] dont lequel le concessionnaire de l'image secrète décompose l'image en n niveaux de secret (régions) dont lequel chaque région représente une partie du secret, puis l'image secrète est codée en n+1 shares. Lorsque textit k, ($2 \leq k \leq n$+1) shares sont superposés, $k-1$ niveau secret de l'image secrète peut être divulgué. Toute l'image secrète peut être déchiffrée lorsque tout les shares sont empilés. Des schémas dans le même cadre ont été proposés dans [104], [105] et [106]. La figure 2.8 montre un schéma de cryptographie visuelle incrémentale dont lequel chaque région secrète est apparue à chaque fois le nombre de shares incrémente.

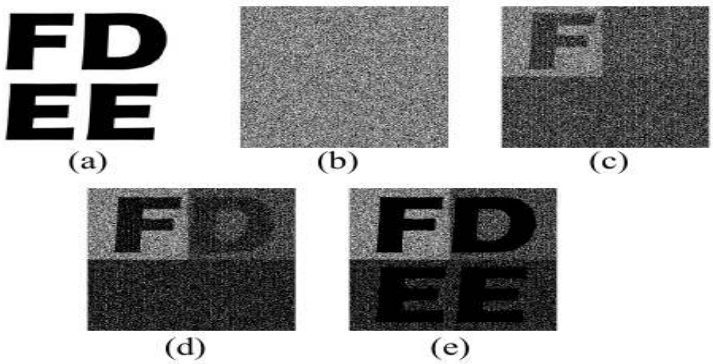


FIGURE 2.8 – Schéma de cryptographie visuelle incrémentale [16]

La cryptographie visuelle progressive basé sur des blocs (CVPB)

Ce schéma de partage de secret visuel progressif basé sur des blocs avec l'augmentation du nombre de pixels est introduit par Wang et al, en 2007 [99], un autre modèle basé sur le même contexte rapporté en 2013 par Hou et al. [17], sans avoir besoin à augmenter le nombre de pixels. Dans la CVPB, l'image secrète est décomposée en blocs non superposés de n'importe quelle taille et à chaque fois qu'un nouveau participant $i, 1 \leq i \leq n$; empile son share, le block secret associé au numéro du participant i sera révélé, et non pas le contraste qui augmentera comme dans le concept de système visuel progressif cité ci-dessus. En 2015, un travail de Das et al. a été publié dans une conférence IEEE dans [107]. La figure 2.9 montre le premier schéma de cryptographie visuelle basé sur des blocs.

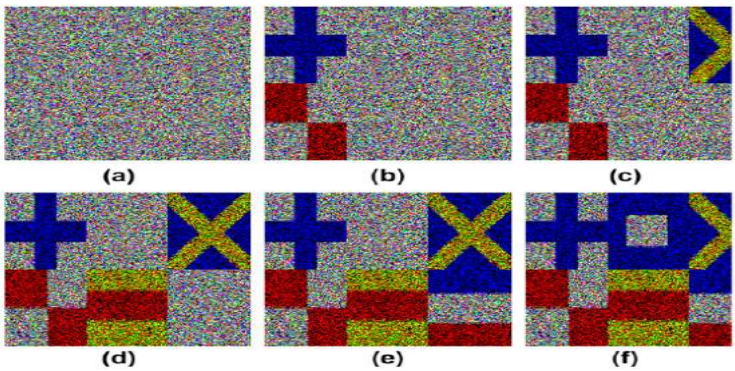


FIGURE 2.9 – Schéma de cryptographie visuelle progressive basé sur des blocs [17]

La cryptographie visuelle évolutive (CVE)

Pour les schémas de partage de secret visuels évolutifs proposé par Wang Shyu, en 2007 [18], la quantité des informations secrètes varie en fonction du nombre de shares superposés en utilisant trois modes de partage : multi-secrets, mode prioritaire ou progressif en fonction des besoins de l'utilisateur. Des schémas de la cryptographie visuelle évolutive ont été publiés notons les travaux dans : [108], [109], et[110]. La figure 2.10 montre un schéma de cryptographie visuelle évolutive.

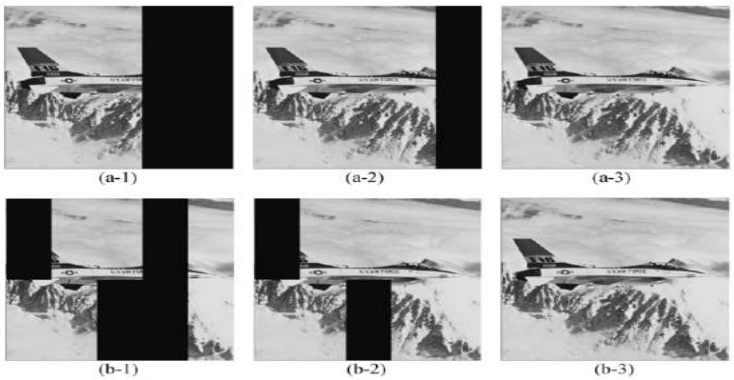


FIGURE 2.10 – Schéma de cryptographie visuelle évolutive [18]

La cryptographie visuelle progressive (friendly)

En 2008, Wen-Pinn et Fang [26] ont suggéré une méthode de la cryptographie visuelle progressive qui combine les privilèges de la cryptographie traditionnelle (la facilité de décodage et la prévention de divulgation du secret quand le nombre de transparents requis n'est pas atteint), les avantages de la cryptographie visuelle progressive (l'image secrète reconstruite peut être vue progressivement) et les vertus de la cryptographie multi-secrets où les transparents sont des images réelles et non pas aléatoires, mentionnant les schémas dans [111], [112], et [113].

Le partage progressif des images secrètes basé sur le seuil essentiel

En 2017 Bhattacharjee et al. [114], ont présenté un schéma de partage de secret basé sur des opérations booléennes pour un contrôle d'accès progressif. Leur approche est basée sur un seuil essentiel ce qui signifie l'utilisation de deux types de transparents. Le premier dit essentiel et l'autre dit non-essentiel afin de reconnaitre le secret.

Ces transparents sont distribués entre un nombre de participants tel que la taille totale de tout les transparents est égale à la taille de l'image secrète, en effet les transparents non-essentiels aident à reconstruire le secret progressivement tant que les transparents essentiels aident à reconstruire le secret complètement. Le principal inconvénient de leur méthode est le nombre de shares, qui ne doit pas être supérieur à quatre n=4.

Les applications du partage progressif de secret

L'obtention d'une image secrète révélée progressivement á multiple résolution est importante dans les applications qui suit :

- E-Commerce : où la somme d'argent délivré dépend de qualité image vue.
- L'extraction d'une image d'une base de données dans les investigations de crime, et le domaine militaire.
- La possibilité d'extraire des images de différentes qualités selon le besoin de l'utilisateur et en fonction des ressources de calcul disponibles.

TABLE 2.1 – Les différents travaux de la cryptographie visuelle

Année	Schéma	Les auteurs initiateurs
1987	La CV basée sur la grille alléatoire	Kafri et Karen, [70]
1994	La CV traditionelle	Naor et Shamir, [8]
1996	La CV étendue	Ateniese et al. [85]
1996	La CV pour les images en couleur	Droste et Stefan, [93]
2002	La CV hlaftone	Nakajima et al. [78]
2005	La CV basée sur XOR pour les images binaires	Tuyls et al. [25]
2005	La CV multiples	Wu et Chen [90]
2005	La CV basée sur la décomposition en plan de bits	Lukac et Plataniotis, [88]
2005	La CV progressive	Jin et al. [15]
2006	La CV halftone avec des transparents significatifs	Zhou et al. [11]
2007	La CV basée sur XOR pour les images en niveaux de gris	Wang et al. [10]
2007	La CV évolutive	Wang et Shyu, [18]
2007	La CV progressive basée sur des blocs	Wang et al, [99]
2008	La CV progressive (friendly)	Wen-Pinn et Fang, [26]
2009	La CV incrémentale	Wang [100]
2017	La CV progressive basée sur le seuil essentiel	Bhattacharjee et al. [114]

2.8 Conclusion

Dans ce chapitre, nous avons évoqué le principe du partage de secret et son utilisation dans la cryptographie visuelle qui est un concept efficace du fait qu'elle permet de partager une information secrète et de la coder en même temps. Nous avons évoqué le schéma de base de partage de secret de Naor et Shamir et nous avons vu son principal inconvénient et cité les paramètres qu'un schéma doit avoir pour qu'il soit faisable pour les applications de la cryptographie visuelle. Ainsi, les différents types de la cryptographie visuelle ont été discutés ainsi que les différents travaux.

Chapitre 3

Le tatouage numérique

La plupart des données comme les images, le son, les vidéos sont stockées sous forme de données numériques. En effet avec l'émergence du monde de l'informatique digitale, et le développement de traitement d'images, ces données sont devenues de plus en plus envoyées sur Internet. Comme toute information transmise à travers le réseau, le bruit du canal de transmission ou les attaques causées par les pirates peuvent détruire ou modifier les données qui ne sont pas protégées. En effet ces données sont donc vulnérables et les protéger de toute tentation d'attaque est nécessaire. Le cryptage, le tatouage et le crypto-tatouage sont les outils les plus utilisés pour garder la confidentialité de données. La cryptographie sert à crypter les données, le crypto-tatouage sert à combiner le tatouage et la cryptographie, quant au tatouage qui va être discuté au cours de ce chapitre, il permet la connaissance de l'origine (propriétaire) de l'objet, afin d'éviter le problème de droit d'auteurs [115]. Le tatouage numérique "watermarking" qui est une technique utilisée pour intégrer une information dans un signal, peut être appliqué pour surmonter ces problèmes et protéger ces données contre la reproduction, l'altération, et permet d'authentifier le propriétaire du document [116]. Les informations intégrées peuvent être soit invisibles (cachées) ou visibles comme le signe du "copyright" ajouté dans certains fichiers. Quel que soit son type, un tatouage robuste ou fragile, aveugle ou non-aveugle, appliqué dans le domaine spatial ou fréquentiel, chacun est utilisé selon le besoin de l'utilisateur et chacun a son objectif pour assurer certaines propriétés de sécurité comme l'intégrité de données, l'authentification, l'interdiction de la copie illégale...etc.

Quoique que beaucoup de pratiques de tatouage ont eu lieu depuis l'antiquité. Le tatouage numérique est un axe de recherche récent dans le domaine scientifique, ses premières réelles apparitions reviennent à l'année 1992 avec l'arrivée du travail de Tanaka et al. [117] qui a publié un article sur le tatouage d'image, et le travail de Cox et al. en 1997 [9], puis les chercheurs se sont penchés sur cet onglet de recherche pour publier plusieurs travaux en essayant d'améliorer ce qui en existent. Aujourd'hui l'usage du tatouage est devenu incontournable dans plusieurs domaines notamment le domaine commerciale et médicale.
Dans ce chapitre, nous évoquons l'histoire du tatouage numérique. Nous présentons également les différents types de tatouage. La méthode conventionnelle d'insertion et d'extraction du tatouage est décrite dans la quatrième section. Nous illustrons quelques méthodes de tatouage fragile basées sur la technique de substitution des bits LSB, ainsi que les attaques et domaines d'application du tatouage numérique.

3.1 Définition

Le tatouage est une technique utilisée pour protéger les droits d'auteurs "copyright", contrairement à la cryptographie ou l'information qu'on souhaite transmettre est complètement illisible pour toute personne qui ne posséde pas la clé de déchiffrement, le tatouage permet de cacher une information au sein d'un document (texte, image, audio, vidéo) pour faire face à toute tentation d'attaque afin d'altérer cette marque [115]. Le processus de tatouage a trois paramètres importants : la marque (le tatouage), la phase de codage (insertion) et la phase de décodage (extraction).

3.2 Apparition du tatouage

Le tatouage est apparu, cela fut très longtemps, les chercheurs ont donné plusieurs lieux de son origine car même s'il s'agit d'une pratique ancestrale ce n'est pas évident de le situer avec certitude. L'information la plus populaire attribut sa date d'apparition à l'année 1282, en Italie. Au début de son apparition, son utilisation était restreinte à des applications minimes en insérant des marques sur des papiers, vers le 18 siècle, ses applications sont devenues de plus en plus importante, en effet l'utilisation du "watermark" s'est propagé de l'Italie vers Europe puis en Amérique, des marques-déposées ont apparu sur des papiers de commerce, pour enregistrer la date de fabrication, ou pour indiquer la taille des papiers, le format du papier et sa qualité, puis en 1779, le tatouage a été utilisé sur les billets d'argent et les factures afin d'éviter la contrefaçon [118]. Le premier exemple de tatouage est apparu en 1954, au monde digital avec l'insertion du message dans une bande sonore par l'entreprise Muzak, cependant, le tatouage numérique a été introduit dans le domaine scientifique en 1990, avec la sortie d'un travail de Tanaka et al. qui consiste à cacher une information au sein d'une image. Le terme digital watermark (tatouage numérique) a été employé pour la première fois en 1992 par Andrew Tirkel et Charles Osborne [119][118]. En effet, la véritable explosion du watermarking s'est produite vers la fin des années 90 où plusieurs organisations ont commencé l'application du tatouage, notons le groupe de travail technique pour la protection contre la copie (CPTWG) qui a utilisé un tatouage pour protéger les disques DVD, et la consortium SDMI (Secure Digital Music Initiative) formé fin 1998, qui a bénéficié du tatouage afin de protéger la lecture, et la distribution des œuvres de musique numériques, comme le MP3, puis plusieurs entreprises ont fait recours au tatouage afin de protéger toute copie illégale de leur documents, par conséquent le tatouage est devenu un véritable outil qui sert plusieurs secteurs notamment le secteur médicale, le domaine de la sécurité, l'empreinte digitale et l'indexation dans les bases

de données.

3.3 Classification des différents types de tatouage

Le tatouage numérique est classifié en plusieurs type : selon la perceptibilité en visible et invisible, Selon l'extraction en (aveugle, semi-aveugle et non-aveugle), selon la robustesse en (fragile, semi-fragile et robuste), et selon le domaine d'utilisation en (spatial et fréquentiel). Le schéma 3.1, montre les différents types de tatouage.

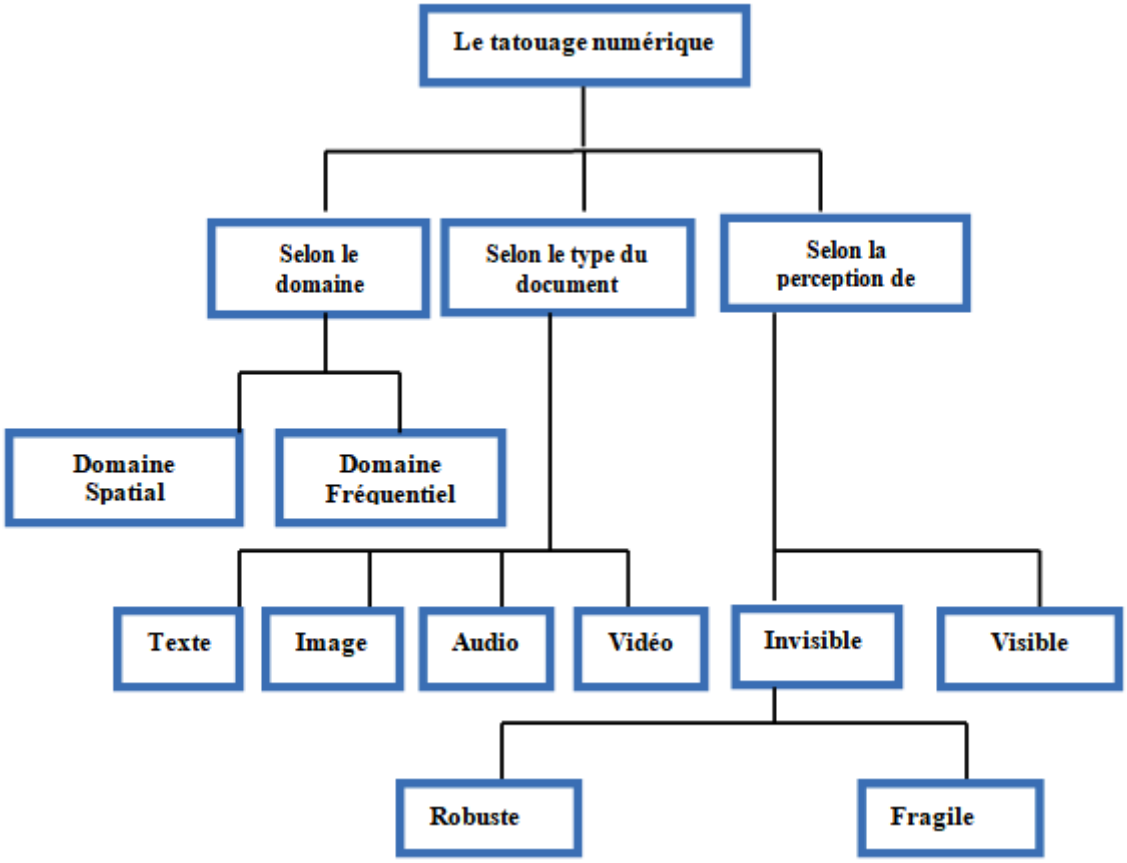


FIGURE 3.1 – Classification des differents types de tatouage

3.3.1 Selon la perceptibilité (visible/invisible)

Selon la perceptibilité, le tatouage est classifié en tatouage visible et invisible :

(a) Image originale.

(b) Image tatouee

FIGURE 3.2 – Tatouage invisible

Le tatouage invisible

Le tatouage invisible est l'approche qui attire beaucoup plus les chercheurs [120] [121] [122], il consiste à insérer une information au sein d'un document de telle sorte qu'elle soit invisible pour l'être humain et pour que cela ne dégrade pas le document modifié afin de détecter si une intrusion a eu lieu en le comparant avec le document tatoué précédemment (avant l'intrusion). Figure 3.2 montre un tatouage invisible.

Le tatouage visible

Dans certaines applications, on demande que le tatouage soit visible [123][124], c'est pourquoi une marque visible aux lecteurs est insérée dans le document qu'on souhaite protéger, citons l'exemple du signe de copyright ©, ou bien les logos utilisés par certains propriétaires indiquant la propriété du propriétaire. Ce type de tatouage est facile à attaquer par rapport au tatouage invisible. Figure 3.3 montre un type de tatouage visible.

(a) Image originale.

(b) Image tatouée

FIGURE 3.3 – Tatouage visible

3.3.2 Selon l'extraction (aveugle/semi-aveugle/non-aveugle)

Selon l'extraction du tatouage on peut le classifier en aveugle, semi-aveugle et tatouage non-aveugle :

Le tatouage aveugle

Ce type de tatouage est connu aussi sous le nom de public-watermark dans lequel l'extracteur du tatouage n'a pas besoin de connaitre ni l'image originale I, ni le watermark W. Seul le document tatoué I' doit être disponible au moment de l'extraction du watermark W', et la clé K n'est pas forcément utilisée. Parmi les schémas de tatouage aveugle citons les travaux de : [125] et [126].

Le tatouage semi-aveugle

Ou le tatouage semi-privé. Ce type ne demande que le document tatoué et de la signature, tandis que la présence du document originale n'est pas nécessaire [127], [128].

Le tatouage non-aveugle

Il est connu aussi sous le nom du watermark privé, ce tatouage a besoin de la connaissance de l'image originale pour pouvoir détecter la présence du watermark dans le document tatoué. Seulement le watermark ou l'image tatouée sont nécessaires dans la phase d'extraction, citons les schémas de : [129],[130].

3.3.3 Selon la robustesse du tatouage (tatouage fragile, semi-fragile et robuste)

Le tatouage fragile

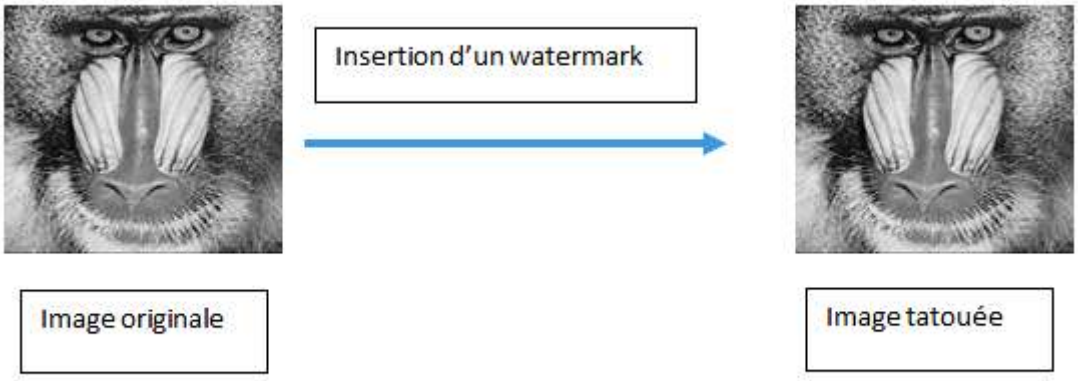
Le tatouage fragile a été proposé premièrement par Mintzer et al [131]. Dans les techniques de tatouage fragile, le watermark inséré doit être sensible aux altérations du document tatoué ce qui permet de détecter toute altération du document tatoué. Ce type de tatouage est utilisé pour assurer l'authentification (la propriété du propriétaire des données) et vérifier l'intégrité du document (schéma 3.4). Une comparaison de la marque extraite et de la marque originale est effectuée afin d'identifier si le document a été modifié ou pas. L'inconvénient majeur des méthodes qui reposent sur le tatouage fragile est la perte d'information du document tatoué. En effet plusieurs méthodes ont été créées [132], [133] en proposant d'insérer un tatouage fragile dans des régions qui affectent l'image d'une façon légère.

Tatouage semi-fragile

Il a les propriétés du tatouage fragile et robuste en même temps. Certaines attaques n'affectent pas ce type de tatouage, tandis que la marque est sensible à d'autres attaques. Ce type de tatouage peut résister à certains types d'attaques comme la compression avec pertes par exemple mais pas toutes les attaques. Parmi les travaux faits dans ce contexte citons les approches proposées par [134] et [135].

Tatouage robuste

Ce type de tatouage est généralement utilisé pour protéger les droits d'auteurs, et pour vérifier la propriété du document. Il doit être résistible contre toutes modifications (compression, rotation, bruit, ...ect), citons l'exemple de [136] [137].



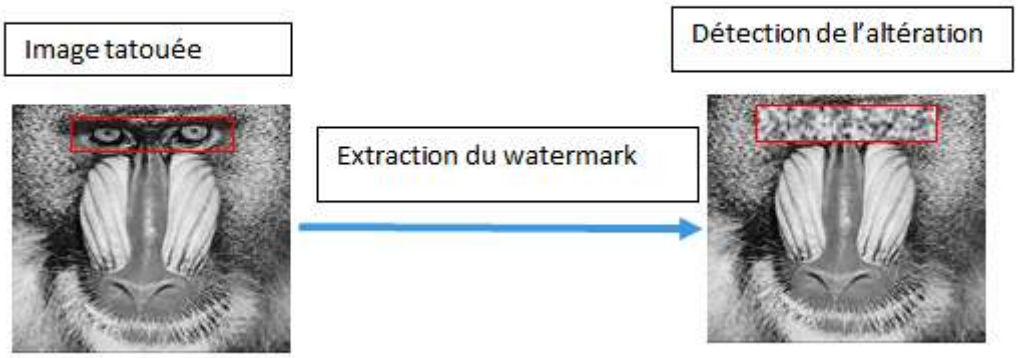


FIGURE 3.4 – Tatouage fragile pour détecter une région altérée

3.3.4 Selon le domaine d'utilisation (spatial et fréquentiel)

le domaine spatial

Il consiste à agir en temps réel sur les valeurs de pixels des images, et ne nécessite aucune transformation du document hôte durant l'insertion du tatouage. Parmi les techniques de tatouage bien connues dans le domaine spacial c'est l'utilisation de la technique des bits les moins significatifs (LSB) proposé par Schyndel et al. [118] et l'algorithme de Patch-Work. En effet le tatouage appliqué sur ce domaine résiste mal à certaines attaques de transformations géométrique comme le recadrage. Aussi, la qualité du signal hôte est dégradée durant l'insertion du tatouage, citons les travaux

de [138] et [139]. Cette faiblesse a poussé la recherche vers d'autres types de schémas résistants à la compression, d'où l'idée des schémas travaillant dans le domaine fréquentiel.

le domaine fréquentiel

Le tatouage s'insère dans le domaine fréquentiel en appliquant l'une des transformée DCT [140], DWT [141] et DFT [142] ...etc. La donnée tatouée dans le domaine fréquentiel résiste mieux aux attaques telles que : la compression, la quantification, le filtre médian, ...etc. citons les schémas dans [143] et [144].

3.3.5 Selon le type de données

Le texte : une marque est ajoutée aux documents textuels par exemple ceux qui ont l'extension PDF, DOC pour pouvoir prévenir tout changement textuel [145].
L'image : est le type de données le plus utilisé dans le domaine du tatouage par les chercheurs, un tatouage est ajouté aux pixels des images afin de protéger les droits d'auteurs [146].
La vidéo : Une vidéo est une suite de séquences d'images, donc le processus de tatouage vidéo est une extension du tatouage d'images, par conséquent le même processus est appliqué sur des vidéos [147].
L'audio : comme les fichiers mp3, et les documents sonores [148].

3.4 La méthode classique de tatouage

Le tatouage a deux phases principales, la phase d'insertion la phase de détection et la phase d'extraction : le processus d'insertion du watermark (appelé aussi la phase de codage) permet d'insérer la marque dans le signal qu'on souhaite tatoué et le processus d'extraction (la phase de décodage) consiste à faire l'opération inverse [118]. La figure 3.5 et 3.6 montrent les processus d'insertion et d'extraction du tatouage successivement.

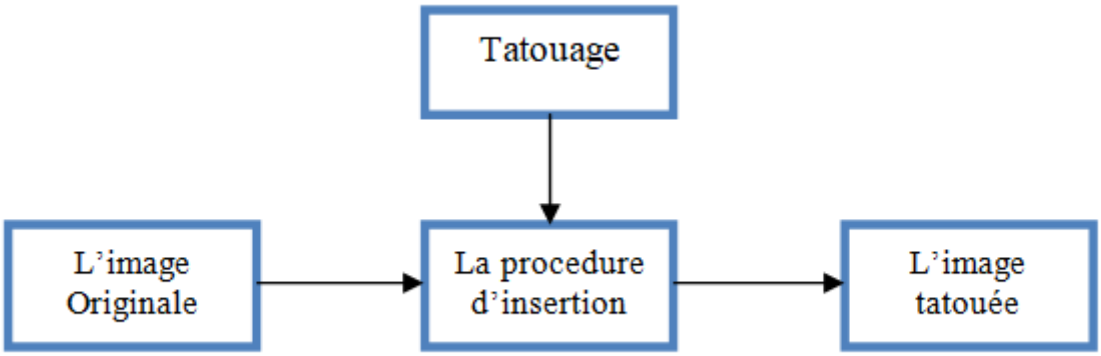


FIGURE 3.5 – Le processus d'insertion de tatouage

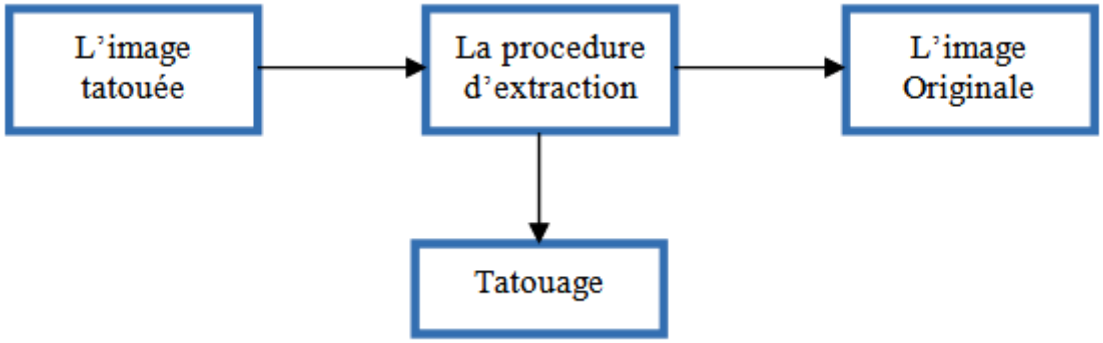


FIGURE 3.6 – Le processus d'extraction de tatouage

3.4.1 La phase d'insertion

Cette opération consiste à introduire une marque (tatouage) dans un document hôte en utilisant un algorithme précis. Dans ce processus on a besoin du document original I, du watermark W et de la clé secrète K. Supposons qu'on veut insérer un tatouage W dans un document I, cela se fait grâce à une clé de codage secrète K ce qui donne un document tatoué I', $C(I,K,W) = I'$.

On distingue deux ensembles dont lesquelles la marque est insérée, le modèle additif et le modèle substantif :
Pour le modèle additif, Cox et al. [149] définissent deux paramètres importants dans leur article "Secure Spread Spectrum Watermarking for Multimedia" ; le premier paramètre appelé la distorsion de l'insertion qui consiste à mesurer la différence entre

le document originale I et le document tatoué I'. Le deuxième paramètre α qui détermine la quantité par laquelle la marque altère le document tatoué en rajoutant un bruit à l'image à tatouer. Trois formules mathématiques ont été présentées par Cox et al :

— $I'_i = I_i + \alpha W_I$.
— $I'_i = I_i(1+\alpha W_i)'$.
— $I'_i = I_i(e^{\alpha W_i})$.

La première équation est utilisée dans **le modèle additif**, la deuxième s'utilise pour le modèle multiplicatif et la dernière pour le modèle exponentielle du tatouage numérique. Quant au **modèle substantif**, qui repose sur le principe que la marque n'est pas ajoutée mais elle substitue les composantes de l'image. Plusieurs méthodes peuvent être utilisées notons la méthode LSB qui a été proposée par Dharwadkar et Amberker [150] et qui consiste a remplacer les bits les moins significatifs par le tatouage a insérer. Une autre méthode du modèle substantif proposé par Chen et Wornell [151] consiste utiliser la technique de quantification par modulation qui permet de quantifier une image en utilisant un ensemble de quantificateurs indexés, le tatouage se fait grâce à l'image quantifiée et le quantificateur correspondant à la marque à insérer.

3.4.2 la phase d'extraction (décodage)

C'est le processus qui consiste à extraire le tatouage inséré du document tatoué. Une phase de détection précède cette phase pour pouvoir prouver la présence d'un watermark au sein du document reçu, puis si cette phase indique la présence d'un watermark on passe à l'extraction et on compare le document originale avec le document tatoué reçu.

La phase de détection nécessite le document tatoué reçu I', (ce dernier qui est probablement altéré ou corrompu par les pirates lors de l'envoie) et la clé de l'algorithme de tatouage K : $D(I', K)$. Notons que dans certains algorithmes le document original I et le tatouage W sont des paramètres nécessaires et l'utilisation de la clé K n'est pas forcement obligatoire. La phase d'extraction sert à extraire le watermark W', à partir du document tatoué. Si les deux marques W et W' sont les mêmes, cela veut dire que le document tatoué n'a pas été modifié : $W'=(I', K)$. D'une manière générale, le tatouage est qualifié comme étant un tatouage aveugle lors de l'utilisation du document original, et qualifié comme non-aveugle quand le document original est absent.

3.5 Méthodes de tatouage fragile basées sur la technique de substitution des bits LSB :

La technique de substitution des bits LSB proposée par Schyndel et al. [118] permet d'insérer des informations de contrôle dans les bits de poids faible d'un pixel en supprimant leur contenu et y insérer des données voulues. L'insertion varie en fonction du nombre de bits dans une image. Pour une image de 8 bits, on peut changer jusqu'à trois bits non significatifs. Pour une image de 24 bits, les couleurs de chaque composant comme RVB (rouge, vert et bleu) sont modifiées. La technique LSB est connu par les propriétés suivantes :

— Les LSB sont sensibles à la moindre modification.
— Le système visuel humain ne peut pas soupçonner les modifications faites sur les bits de poids faible.
— Ne modifie pas la taille de l'image.
— Sa simple manière d'implémentation.

L'une des méthodes qui repose sur ce principe est celle de Walton [133] qui a pour objectif de vérifier l'intégrité d'une image et consiste à détecter les erreurs en utilisant le checksum des bits MSB des pixels sélectionnés de façon aléatoire. Le tatouage consiste donc à insérer dans les bits LSB du document le checksum calculé à partir des sept bits MSB. Dans cette méthode une légère distorsion de l'image tatouée est imperceptible par l'œil humain. Dans l'approche proposée dans [152], le code CRC, est utilisé pour détecter toute modification de l'image tatouée.

Fridrich et Goljan [153] proposent quant à eux une méthode de tatouage fragile qui repose sur l'utilisation des bits de poids faible LSB. La DCT est calculée en prenant les MSB des blocs de taille 8×8 pixels de l'image à tatouer et puis l'insertion aux LSB se fait par les coefficients de la DCT après les avoir quantifiés.
Cette méthode permet non seulement de détecter les altérations subisses, mais aussi elle permet une reconstruction partielle. Ces méthodes sont simples, efficaces avec un impact visuel inaperçu par l'œil humain, mais elles permettent que la détection des erreurs, et non pas la correction, à part la méthode de Fridrich et Goljan [153] qui permet une reconstruction partielle.

3.6 Mesures d'évaluation du tatouage

Plusieurs mesures permettent d'évaluer la faisabilité du tatouage, chacune est utilisée selon l'application de l'utilisateur. Les paramètres les plus populaires sont le PSNR et le SIM qui sont des outils importants mis à disposition pour mesurer la qualité de l'image tatouée :

3.6.1 Le PSNR

Ce paramètre permet de mesurer la différence globale entre l'image originale et l'image tatouée.

$PSNR$=$10 * log_{10} * \frac{255^2}{MSE} dB$.
Et MSE représente l'erreur quadratique moyenne : $MSE = \frac{1}{n*m} \sum_{i=1}^{n} \sum_{j=1}^{m} (a_{i,j} - b_{i,j})^2$.

Une valeur supérieure à 40 dB du PSNR indique que l'image tatouée a subi une faible dégradation invisible à l'œil, tandis qu'une valeur inférieure à 30 dB indique une forte dégradation [154].

3.6.2 Le SIM [9]

Cox et al. définissent le paramètre SIM, qui permet de mesurer la similarité entre le tatouage inséré et le tatouage extrait. La corrélation entre les deux marques est calculée :

$SIM(W, W^*)$=$\frac{W^*.W}{\sqrt{W^*.W^*}}$.
Tel que W et W^* représentent la marque insérée et la marque extraite respectivement. Pour décider si les deux marques sont compatibles, on peut déterminer, $SIM(W, W^*) \geq T$, où T représente un seuil.

3.7 Les propriétés du tatouage

Cox et al. [9] définissent dans leur article en 1997 plusieurs critères pour lesquels un tatouage numérique devrait répondre pour qu'il n'affecte pas la qualité du signal, et pour satisfaire aux règles de sécurité, notons :

— L'imperceptibilité : c'est à dire que la marque insérée ne doit pas être visible et elle ne doit pas affecter la qualité du document tatoue [155] : L'évaluation de la qualité visuelle des documents tatoues est devenu un critère primordiale pour la validation des algorithmes de tatouage.
— Un tatouage doit être robuste contre toute tentation d'attaque [156].
— La capacité : La capacité de tatouage désigne le nombre de données à dissimuler dans un document hôte sans dégrader sa qualité visuelle ou auditive. De façon générale, plus la capacité est faible, plus la robustesse est forte [142].
— La qualité du document tatoué doit être bonne, et non affectée par les informations intégrées.
— Un tatouage visible devrait être visible dans les images couleurs et aussi dans des images monochromes.
— Le tatouage devrait se propager sur une zone importante du document pour rendre la marque assez significative.
— L'extraction du tatouage doit être difficile à enlever.
— l'insertion de la marque doit être dans les zones d'intérêts les moins sensibles à l'œil humain pour garantir la qualité du document tatoué.
— La robustesse : c'est la résistance de la marque insérée aux différentes dégradations. Quel que soit le type du tatouage, robuste, semi fragile ou fragile, chacun doit se manifester aux attaques d'une manière différente a l'autre, selon le besoin de l'utilisateur comme nous avons éclairé dans la section précédente.

3.8 Les attaques les plus populaires du tatouage numérique :

Il existe plusieurs attaques populaires qui peuvent être appliquées pour craquer des documents tatoués :

— **La compression :** Ce type d'attaque consiste à éliminer les composantes perceptuellement moins significatives en gardant les composantes importantes du document ce qui peut provoquer la perte de résolution de l'image tatouée [115].
— **La transformation géométrique** : comme le redimensionnement de l'image, la rotation, le recadrage, ces attaques ont pour objectif de tester la robustesse de la marque [157].
— **Le bruit :** L'ajout d'un bruit a un effet de masquage de la marque et par conséquent rend son extraction difficile comme le bruit provoqué dans un canal de transmission bruité.

— **La rotation :** C'est une transformation qui sert à réaligner des images.
— **Le recadrage ("crop") :** cette attaque consiste à supprimer et/ou remplacer une partie de l'image, pour détruire le marquage qui a été insérée.
— **Les filtres :** En pratique, il s'agit de créer une nouvelle image en modifiant les valeurs des pixels de l'image d'origine afin d'atténuer les composantes de hautes fréquences et dégrader le tatouage inséré dans ces fréquences, comme l'application d'un filtre passe-bas dont lequel on ne laisse passer que les basses fréquences avec une fonction passe-bas.

3.9 Les applications du tatouage numérique

L'utilité du tatouage numérique a rendu ses applications nombreuses et incontournables dans plusieurs domaines notons :

— La surveillance de la retransmission : parmi les premières applications du tatouage c'était la surveillance de la retransmission dans la télévision, des informations contenant le logo du propriétaire sont rajoutées aux vidéos pour indiquer que le contenu à été retransmis grâce à un système de moniteur [115].
— Le copyright : le tatouage peut être utilisé pour interdire la copie illégale, et assurer la propriété du propriétaire du document (images, vidéo, ...).
— La cryptographie visuelle : le tatouage est appliqué dans ces derniers temps dans la cryptographie visuelle, pour protéger le secret partagé entre un certain nombre de participants
— Le domaine médicale : Les noms des malades sont affichés sur des fichiers grâce aux techniques IRM, et rayons-X, en utilisant un tatouage visible, ce qui fait que les données restent confidentielles et les médecins peuvent vérifier que ces documents n'ont pas été modifiés, et altérés [115].
— l'authentification et l'intégrité : le tatouage sert à prouver l'origine du document, et pour assurer que les données n'ont pas été modifiées [158].
— L'empreinte digitale : Pour éviter la duplication non autorisée de copies de l'empreinte digitale : Le tatouage peut protéger la copie illégale et la distribution de l'empreinte digitale en donnant à chacune un numéro de série unique.
— La détection de l'intrusion, et l'échange des informations secrètes.
— L'indexation : cette dernière est exploitée afin de rendre la recherche dans une base de données plus rapide et faciliter l'accès aux données multimédia grâce à une marque insérée au sein d'un document.

3.10 Conclusion

Avec l'implication des médias numériques dans notre vie quotidienne, sa facilité de manipulation, son large domaine d'utilisation et sa simple et rapide transmission à travers Internet, ce qui a fait que ces informations deviennent vulnérables à la falsification, la duplication et la corruption. Tout ça a mené les chercheurs à créer un outil qui permet de protéger ces données contre la copie illégale et de protéger tout droit d'auteurs. Dans ce chapitre nous avons évoqué une méthode de protection de données très répandue qui est le tatouage numérique, nous avons parlé de son historiques, ses différents types, nous avons évoqué le modèle générique d'insertion et d'extraction. Ses différentes attaques ont été évoquées. À la fin du chapitre nous avons cité les différents domaines d'applications du tatouage.

Chapitre 4

Les codes correcteurs : Etat de l'art

L'échange de l'information sur les systèmes de communication s'est beaucoup accru dernièrement comme à travers le téléphone, l'internet, la fibre optique, les ondes-radio...etc. En effet la transmission des données d'un support physique à un autre comme sur les CDs, DVDs, les clés USB peut exposer l'information à des altérations, cependant le nombre des erreurs de transmission qui peuvent survenir peut devenir perturbant [19]. Deux techniques connues sont très répandues pour le contrôle et la correction des erreurs. La première s'appelle la requête automatique de répétition (ARQ) et la deuxième sont les codes correcteurs d'erreurs. Les codes ARQ permettent de solliciter l'émission d'un nouveau message durant la transmission des paquets grâce à un acquittement envoyé par le récepteur vers l'émetteur afin de l'informer que le paquet de données a été correctement reçu, comme dans le protocole TCP, si l'émetteur ne reçoit pas un acquittement à temps, il renvoi le même paquet jusqu'à recevoir un nouvel acquittement ou dépasser un nombre prédéfini de retransmissions [35]. La deuxième technique qui est le sujet de ce chapitre s'appelle : les codes correcteurs, elle permet de détecter et corriger les erreurs survenues durant la transmission en utilisant des codes correcteurs des erreurs.

En 1948, Claude Shannon [159] a donné naissance à deux disciplines jumelles : la théorie de l'information et la théorie du codage dans les laboratoires de téléphone Bell, où le mot "bit" a été utilisé pour la première fois, en donnant une interprétation sur le statut d'un transistor (on et off), de tel sorte que le (off) désigne le nombre 0, et le (on) désigne le nombre 1. Le mot bit (binary unit) ou "Shannon" est une unité pour mesurer la capacité d'information. Dans son article «A Mathematical Theory of Communication» ; Shannon propose de mesurer l'entropie H de la quantité d'information et définit comment on peut la comparer à la capacité C d'un canal de transmission par lequel on souhaite adresser l'information à un interlocuteur. Il montrera que la condition $H \prec C$ (limite de SHANNON) est nécessaire.

Avec l'arrivée de cette invention très importante de Claude Shannon, sans laquelle le monde de communications numériques serait inconcevable et avec laquelle on est passé de l'analogique vers le numérique, la théorie des codes correcteurs qui est une branche de la théorie d'information a vu le jour avec l'invention de Richard Hamming en 1950 [160], qui a développé le code de Hamming, ce dernier qui peut corriger qu'une seule erreur a été utilisé dans des applications où le taux des erreurs est minime, puis au fils des années l'archive des codes correcteurs a été enrichi, citons les deux inventeurs Reed et Muller qui ont inventé un code correcteur et l'ont attribué leur nom (Reed-Muller). Les codes cycliques les plus importants, comme le BCH [161] et Reed-Solomon [162] qui sont appliqués aujourd'hui sur les CD et les DVD, ont été développé entre l'année 1958 et 1960 successivement. Les turbos-codes sont venus en 1933, ces derniers sont appliqués dans la télécommunication et sont utilisés aujour-

d'hui dans les sondes spatiales et les réseaux 4G. En 1955, on a vu l'arrivée des codes convolutionnels comme le code MCEliece, puis les codes concaténés en 1965 [19]. Enfin en 2000 vient les codes LDPC [163] qui sont par ailleurs les codes adoptés dans le nouveau standard de transmission des vidéos numériques par satellite. Le contexte de ce chapitre se situe au niveau des différents types de codes correcteurs. Nous allons évoquer brièvement les différents codes en bloc linéaires et cycliques; leurs caractéristiques, leurs différents paramètres, leur processus de codage et de décodage et leurs domaines d'application.

4.1 Le système de communication et de codage

En générale, l'envoie d'un message à travers un canal de communication peut impliquer des erreurs de transmission, en effet le message peut être changé par le bruit du canal. Supposons que l'émetteur souhaite envoyer le message 0 au récepteur, il est censé envoyé la séquence de bits 000, et la séquence de bits 111 pour le bit 1, cependant l'metteur peut recevoir le bit 1 au lieu de 0 si par exemple les deux premiers bits sont modifiés à 110, et de même il peut recevoir le bit 0 au lieu de 1, si les deux derniers bits sont altérés à 100. Dans ce cas-là le récepteur reçoit le message y(x) constitué du message originale m(x) plus une erreur e(x) : $y(x)=m(x)+e(x)$. D'où la nécessité de détection et correction de telles erreurs.

Grâce à la théorie des codes, on peut diminuer voire même se débarrasser de telles erreurs. La théorie de code est une branche de la théorie ds'information introduite par Claude Shannon en 1948 [159]. A vrai dire, c'est seulement avec l'arrivée de la théorie d'information, et le premier code de Richard Hamming en 1950, que le mot codage est désormais utilisé. La technique de codage consiste à rajouter des bits de redondance à la fin du message grâce à un code correcteur, grâce à ce dernier, on peut détecter et corriger les erreurs de transmission qui peuvent survenir sur le canal de transmission et de les éliminer pour récupérer l'information originale [19].

En effet, le processus de communication qui se compose souvent de l'émetteur, le récepteur, l'information binaire (convertie d'un signal analogique) et le canal de transmission se déroule comme suit (résumé au schéma 4.1) [163] :

— Au début, les données venues d'une source (musique, parole, image...etc.) sont compressées pour minimiser la taille du message et donc éliminer la redondance en utilisant un algorithme de compression.
— Ensuite un algorithme de cryptage est utilisé pour crypter ces données.
— Le codage du canal de transmission (câble, fibre optique, etc.) aura lieu pour

coder l'information en rajoutant des bits de redondance.

— **Le processus de modulation vient pour convertir l'alphabet du message en séries convenables afin de l'envoyer sur le canal (le téléphone ou, les ondes radio ...etc.).**

Cependant les données qui circulent sur les canaux peuvent être corrompues, soit par des pirates, ou par le bruit. Elles peuvent être atténuées, une congestion peut avoir lieu sur le réseau ce qui provoque un retard.

Ainsi si on suppose que la capacité du canal est C, et le taux des informations transmises est R, donc selon le théorème de Shannon, la probabilité d'un code pour qu'il soit erroné est très minimale si le taux (débit d'information) R est inférieure à la capacité du canal de transmission C. Le processus inverse est déroulé pour pouvoir décoder le message comme suit [163] :

— Le message est décompressé afin de trouver son équivalent.
— Ensuite un algorithme de décodage est utilisé pour décrypter les données.
— Le récepteur détecte et corrige les erreurs à l'aide des bits redondants.
— Enfin le démodudxdelateur convertie le signale envoyé de l'émetteur en séquences binaires qui arrivent à la fin à leur destination.

4.2 Les codes correcteurs

Un code correcteur est un processus de codage qui se déroule dont le but de détecter, voire même corriger les erreurs de transmission d'un canal de communication (fibre optique, onde radio, etc.) qui n'est pas toujours fiable et aussi les erreurs qui peuvent survenir sur un support physique comme les CDs, DVDs...etc [45].

4.3 Classification des codes correcteurs

Il existe une grande famille de codes correcteurs, chacun a ses propriétés (longueur du mot, dimension du code, sa distance minimale, sa capacité de correction), et son domaine d'application, notons les codes en blocs linéaires comme le code de Hamming [160], les codes de répétition... etc. Les codes cycliques comme le BCH [161] et le code Reed-Solomon [162]. Le tableau 4.3 donne un résumé sur les propriétés des différents codes correcteurs introduit dans ce chapitre.

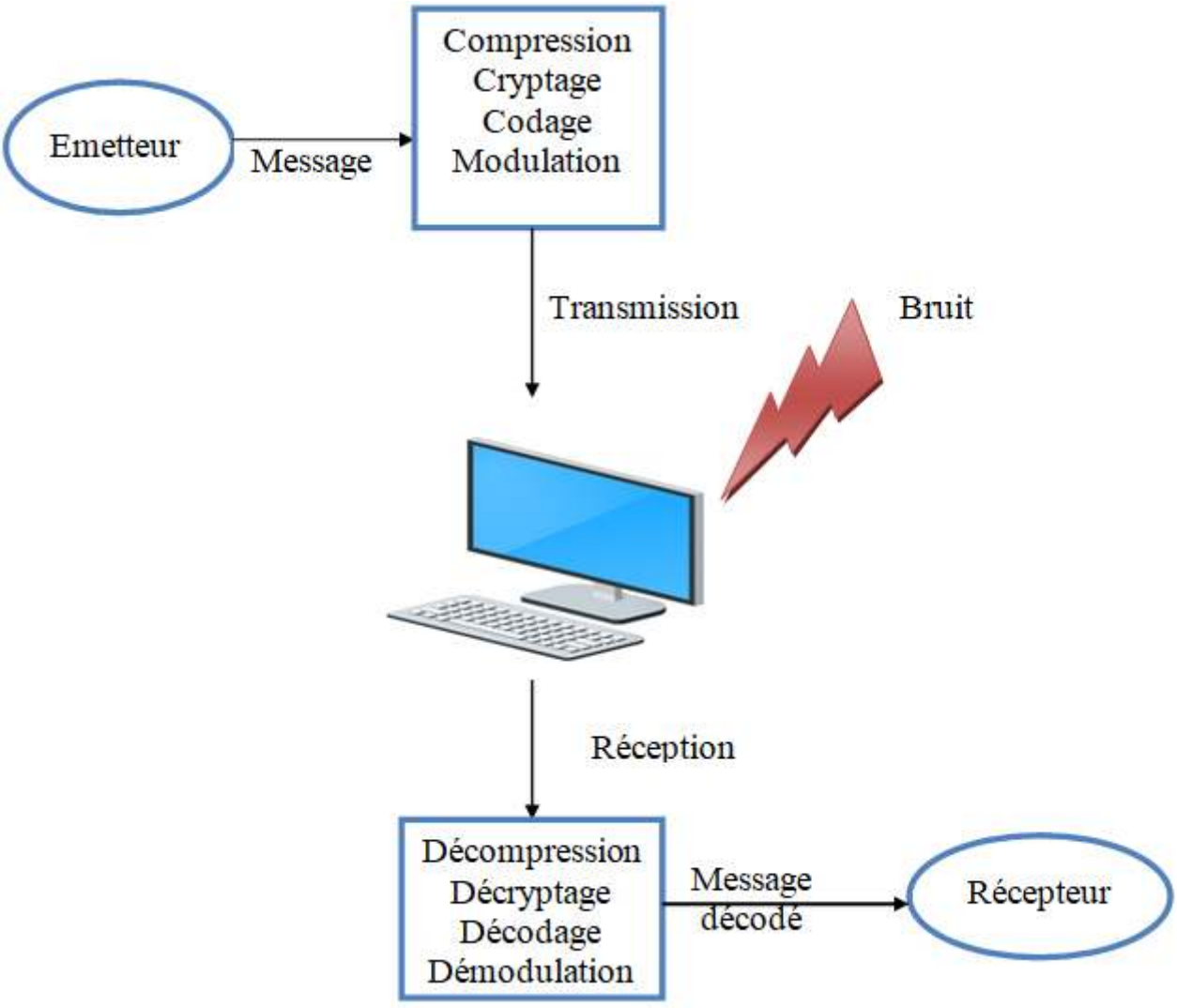


FIGURE 4.1 – Processus de communication via un canal de transmission

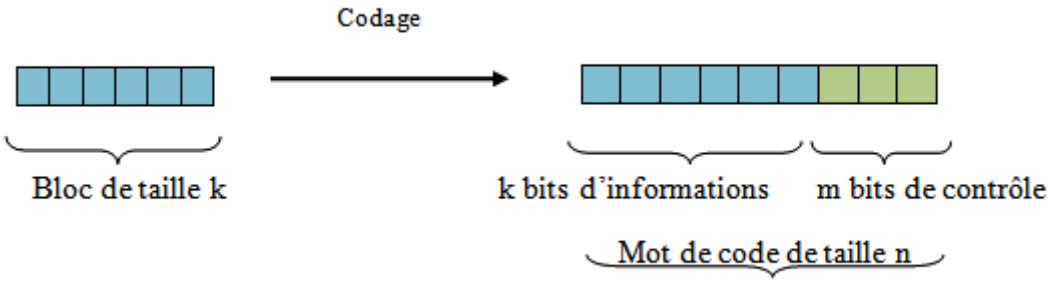


FIGURE 4.2 – Codage d'un code.

4.3.1 Les propriétés d'un code correcteur

— Le nombre d'erreurs ne doit pas être grand.
— L'information ne doit pas être divulguée.
— L'opération de codage doit être suffisamment rapide.
— L'opération de correction doit être suffisamment rapide.

4.4 Les codes linéaires en blocs

Ce sont des codes de correction d'erreurs les plus répandus qui consistent à fractionner le message en blocs de longueur fixe k. Le codage consiste à coder l'information en rajoutant à la fin du message des bits qui s'appellent : les bits de contrôle ou de redondance m [164] (figure 4.2). Les codes en blocs sont définis par un ensemble de propriétés dans un corps qui s'appelle le corps de Gallois F_q tel que :

— d : représente le bloc de données.
— c : c'est le mot codé.
— d_{min} : représente la distance minimale.
— k : c'est le nombre de caractères envoyés.
— n : c'est la longueur du mot après le codage.
— m=$n-k$: représente le nombre de bits de contrôle, où $n \geq k$, et on note le code $C(n,k)$.
— La distance de Hamming d_{min} : représente le nombre de symboles où deux codes se diffèrent (équivalent au poids de hamming de la somme des deux codes).
— Le poids de Hamming : ce sont les éléments non-nuls d'un code.

— La capacité de correction d'un code est $t = (d_{min} - 1)/2$.
— La matrice génératrice G : qui sert à coder un message en le multipliant par la matrice G, c=$d.G$. Où les lignes de la matrice G sont formées par une base du code C.
— Si la matrice génératrice est de la forme G=$[I_k, A]$, où I_k est la matrice identité de rang k, et les colonnes de la matrice A sont la représentation binaires du code, donc le code est considéré comme systématique.
— La matrice de contrôle H. Elle sert pour le décodage d'un code, elle est de la forme : H=$[-A'; I_{n-k}]$, où A' est la transposée de A.

4.5 Flexibilité des codes correcteurs

Les codes correcteurs sont assez flexibles pour raccourcir, étendre leur taille, pour répondre aux besoins de l'utilisateur. On a la possibilité aussi de combiner deux codes correcteurs pour obtenir un nombre de correction plus élevé :

— Les codes étendus : On peut étendre un code $C(n, k)$ à un autre code $C(n$+$1, k)$, en rajoutant 1 ou 0 à la fin de ce code selon la parité trouvée.
— Les codes raccourcis : On peut restreindre un code $C(n, k)$ à un autre code $C(n - s, k - s)$, tel que $s \succ k$, en omettant un nombre de s symbole du code et rajouter des faux bits 0 à partir de la fin pour atteindre la longueur n.
— Pour avoir une distance minimale la plus grande et par conséquent dans le but d'obtenir un code correcteur qui a un taux de correction élevé ; l'idée consiste à combiner des codes correcteurs appelés : codes concaténés, le premier code est utilisé pour coder un message, puis le tout est encodé à son tour par le deuxième code.
— Le produit de deux codes : on peut faire le produit de deux codes $C_1(n_1, k_1, d_{min1})$ et $C_2(n_{,2}, k_2, d_{min2})$, et obtenir un nouveau code $C(n, k)$ tel que k=$k_1.k_2$ et n=$n_1.n_2$, notons que la distance minimale de ce nouveau code est : d_{min}=$d_{min1}.d_{min2}$.

4.6 Les codes en blocs binaires

Les codes en blocs binaires sont définis dans le corps de Galois F_q, q=2, avec deux éléments $(0, 1)$.

4.6.1 Quelques codes linéaires binaires importants :

Dans cette section, nous définissons quelques codes linéaires binaire qui sont les plus utilisés pour détecter et corriger les erreurs de transmission :

Le code Hamming

Ce code a été découvert par Richard Hamming en 1950 [160]. C'est un code qui corrige une seule erreur, et détecte deux. La longueur de la taille de données est n=$2^m - 1$, sa dimension est k=$2^m - m - 1$. Le codage de données consiste à multiplier le mot à envoyer par la matrice génératrice G : c=$d.G$, tandis que le décodage consiste à multiplier les données reçues c par le syndrôme d'une matrice H : p=$c\ ^tH$.
Tel que, les colonnes de la matrice H sont l'écriture binaire de l'entier i allant de 1 jusqu'a 2^{k-1} dans la base 2 [45]. Si $p = 0$, le message est reconnu comme correcte, sinon, si $p \neq 0$; le message contient des erreurs.

Le code Hadamard

C'est un code correcteur binaire qui a été utilisé la première fois en 1971 pour transmettre des photos de Mars à la Terre. Ce code a une distance minimale d_{min}=2^{m-1} , la taille de données est n=2^m, k=m+1, le codage d'un code consiste à le multiplier par une matrice génératrice de Hadamard [19].

Reed-Muller

Ces codes ont été décrit par Reed et Muller en 1954. Ce code a été appliqué dans le domaine spatiale NASA en 1960. Leur avantage c'est la capacité de corriger plus d'une erreur, et leur inconvénient se présente dans la grande capacité de correction seulement dans les codes de longueur réduite [163]. Un code Reed-Muller $R(m,r)$ a une distance minimale d_{min}=2^{m-r}, une longueur de 2^m, une dimension k=2^{m-r}, tel que $0 \leq m \leq r$; et r représente l'ordre du code[20].

Contrôle de parité

Un nombre de symboles est rajouté à la fin du mot à coder de telle façon que la somme de ce code est égale à 0.

Les codes de répétition

C'est le code le plus simple. Il s'agit d'envoyer plusieurs copies (dans le cas générale trois copies) de chaque bit à être transmettre. Ce code permet non seulement de détecter une erreur, mais aussi de la corriger automatiquement. En revanche, ce code est couteux vu sa longueur multipliée.

4.7 Les codes cycliques

Les codes cycliques appartiennent aux codes en bloc, ils ont été découvert entre l'année 1957 et 1959. Ces codes sont les plus utilisés aujourd'hui, vu leur rapidité d'implémentation en utilisant les registres de décalage pour le codage et le décodage [164]. On dit qu'un code en bloc $C(n,k)$ est cyclique si on obtient par un décalage à droite des éléments d'un code c=$[c_0, c_1, \ldots, c_{n1}]$, des éléments dans le même code $c1$=$[c_{n1}, c_0, \cdots c_{n2}]$. Ces codes sont représentés par un polynôme générateur de degré $n-k$:
$g(x)$=g_0+$g_1 x$+...+$g_{n-k} x^{n-k}$.
Les données sont représentées par un polynôme : $d(x)$=d_0+$d_1 x$+...+$d_{k-1} x^{n-k}$.
Le codage de ces codes consiste à multiplier : $d(x)g(x)$=$c(x)$, ou bien en multipliant $d(x).x^{n-k}$ et le diviser sur $g(x)$: $c(x)$=$x^{n-k} d(x)$+$r(x)$, tel que $r(x)$ est le reste de la division. La matrice génératrice est donnée par :
G=

$$\begin{bmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & 0\ldots & 0 & \\ 0 & g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \ldots & g_0 & g_1 & \ldots & g_{n-k} & 0 \\ 0 & 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{n-k} \end{bmatrix}$$

Et la matrice de contrôle H est représentée par un polynôme de contrôle :
$h(x)$=$(x^n-1)/g(x)$, tel que :
H=

$$\begin{bmatrix} h_{n-k} & h_{n-k-1} & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_{n-k} & h_{n-k-1}\ldots & h_0 & 0 & \ldots & 0 & \\ \vdots & & & & & & & \\ 0 & 0 & \ldots & h_{n-k} & h_{n-k-1}\ldots & h_0 & 0 & \\ 0 & 0 & \ldots & 0 & h_{n-k} & h_{n-k-1} & \ldots & h_0 \end{bmatrix}$$

TABLE 4.1 – Définition du polynôme générateur en octal d'un code BCH en fonction de la longueur n [19].

n	k	d_{min}	$g(x)$
7	4	1	13
15	11	1	23
31	26	1	45
63	57	1	103
127	120	1	211
⋮	⋮	⋮	⋮
255	247	1	435561

4.7.1 BCH

Les codes BCH, découverts par Hocquenghem Bose et Chaudhuri en 1959 [161], ils sont la généralisation des codes de Hamming pour la correction des erreurs multiples. Le codage BCH ne nécessite aucune retransmission, ces codes permettent de détecter et corriger sur place les erreurs, en effet les codes BCH permettent de corriger t erreurs et détectent $2t$, erreurs. Un code BCH est de longueur n=$2^m - 1$, pour $m \geq 3$ et d'une distance minimale : $d_{min} \geq 2t$+1, où t est la capacité de correction, et $n - k \leq mt$ [163]. Le processus de codage se fait par :

— En multipliant le message d(x), par x^{n-k} et le diviser par le polynôme générateur $g(x) = ppmc\{m_\alpha(x), m_{\alpha^i}(x), ...m_{\alpha^{2t}}(x)\}$, ou $m_{\alpha^i}(x)$ est le polynôme minimal de l'élément primitif α^i du corps de Galois $GF(2^m)$ (Le tableau 4.1 donne quelques polynômes générateurs d'un code BCH).

— Le mot est encodé comme suit : $c(x)$=$d(x).x^{n-k}$+$r(x)$. Tel que $r(x)$: est le reste de la division.

Le processus de décodage est plus compliqué que le codage, il se fait grâce à trois étapes clés :

1. Le récepteur du message calcule le syndrome à partir du mot reçu : $syndrome$=$v(x).{}^tH$, tel que $v(x)$=$c(x)$+$e(x)$, où $e(x)$ représente l'erreur de transmission.
2. Trouver les coéfficients du polynôme localisateur $L(x)$, en utilisant la méthode directe de Peterson ou bien la méthode itérative de Berlekamp-Massey [3] ou l'algorithme d'Euclide [7]. En fait au-delà de $t \succ 3$, le choix de l'algorithme de décodage le plus complexe est nécessaire.
3. Identifier les erreurs et les corriger à partir de $L(x)$.

4.7.2 Reed Solomon

Ce sont des codes non-binaires découvert en 1960 [162]. Ils s'appliquent dans la plupart des supports de données numériques comme les CDs et les DVDs. Ce code est capable de corriger jusqu'à 4096 bits erronés consécutifs. Ils sont l'extension du code binaire BCH, mais la seule différence entre eux se réside dans les coefficients du polynôme générateur qui ne sont pas binaires. Ces codes peuvent corriger un rafale des erreurs mieux que les codes BCH [19]. Ses paramètres sont comme suit : $C(q-1, n-2t, 2t+1)$.
Le codage se fait de la même manière que les codes BCH avec un polynôme générateur : $G(x)=(x+\alpha^{j})(x+\alpha^{j+1})(x+\alpha^{j+i})...(x+\alpha^{j+d-2})$, tel que :
$d = n-k+1$, $j = 0$ ou $j = 1$ et α : est l'élément primitif du corp de Galois.

Le décodage des codes Reed-Solomon se fait aussi de la même manière que les codes binaires BCH ; mais nécessite une étape supplémentaire qui consiste a calculer les amplitudes des erreurs comme ce n'est pas suffisant de connaitre seulement leur positions [162].

4.7.3 CRC

Les codes correcteurs CRC [165] ont apparu en 1957. Ils ont un domaine d'application important, citons l'exemple d'Ethernet qui utilise un champs CRC à 32 bits, et la Compression ZIP qui utilise un CRC à 16 ou 32 bits. Contrairement aux codes BCH, les codes CRC sont utilisés seulement pour détecter les erreurs de transmission et ils nécessitent une retransmission. Les paramètres d'un code CRC, $C(n,k,d)$ sont $C(2^m-1, 2^m-m-2, 1)$, tel que $m \geq 3$.

- Le codage de ces codes est basé sur des calculs de division de polynôme à coefficient qui consiste à diviser (l'information+ les bits de contrôle) sur un polynôme générateur $g(x)=g_0+g_1x+g_{n-k-1}x^{n-k-1}+x^{n-k}$: $c(x)=d(x).x^{n-k}/g(x)$.
- Si le reste de la division est nulle, on constate qu'il n'y a pas d'erreurs, sinon on constate que le mot reçu contient des erreurs.
- Le choix du polynôme générateur dépend de la qualité du résultat voulu (tableau 4.2 en résume).

TABLE 4.2 – Le polynôme générateur de certains codes CRC [20]

Type du CRC	m	g(x)
CRC-12	12	14017
CRC-16	16	300005
CRC-CCITT	16	210041
CRC-32	32	40460216667

TABLE 4.3 – Propriétés des différents codes correcteurs

Année	Le Code correcteur	La longueur du mot	La dimension	La distance minimale
1950	Hamming [160]	7	4	3
1954	Reed-Muller [163]	2^m	$k = 2^{m-r}$	2^{m-r}
1960	Répétition	2k+1	1	k
1952	Golay [163]	23	12	7
1957	CRC [165]	$2^m - 1$	$2^m - m - 2$	1
1959	BCH [161]	$2^m - 1$,m≥ 3	$\leq mt$	$\geq 2t$+1
1960	Reed Solomon [162]	q-1	n-2t	2t+1

4.8 Conlusion

La théorie de Claude Shannon, était bouleversante dans le monde de la communication, c'est grâce à cette théorie que le code de Hamming était inventé en 1950, puis plusieurs codes correcteurs d'erreurs ont été développé pour accroitre la fiabilité des systèmes de transmission comme les codes BCH, Reed Muller, Reed Solomon... etc. Dans ce chapitre nous avons défini quelques codes correcteurs d'erreurs, nous avons vu leurs paramètres, et leur caractéristique comme la longueur de chaque code, sa dimension, sa distance minimale et sa capacité de correction, chaque code s'applique selon le besoin de l'utilisateur et dans un domaine qui lui est adéquat.

Deuxième partie

Contributions

Chapitre 5

Contribution à la cryptographie visuelle

Approche de partage de secret progressive basée sur des opérations Booléennes avec une reconstruction parfaite

5.1 Introduction

Plusieurs schémas de la cryptographie visuelle ont été proposés afin de répondre à plusieurs paramètres, considérés comme nécessaires pour la construction d'un bon schéma de partage de secret. En effet, il n'est pas toujours facile de trouver un compromis entre un schéma avec un bon contraste, un schéma dont lequel il n'y a pas d'expansion de pixels et qui a la possibilité de partager un secret entre n'importe quel nombre voulu de participants. Dans ce chapitre nous introduisons notre approche de partage progressif de secret (k, n), avec un pixel non expansé. Nous pourrions obtenir jusqu'à $n-1$ images secrètes révélées avec un contraste progressif amélioré de manière de plus en plus évolutive. Du plus faible contraste en cas d'empilement de deux transparents, à un contraste le plus élevé lors de l'empilement de tous les transparents. Contrairement à la cryptographie visuelle traditionnelle basée sur le schéma a seuil dans lequel toute l'image secrète peut être révélée entièrement en empilant $k, (2 \leq k \leq n)$ transparents ou plus [8]. Notre schéma a non seulement l'avantage des transparents non expansés, mais aussi l'utilisation de très simples opérations booléennes XOR et OR pour récupérer parfaitement l'image secrète. De plus, notre schéma proposé n'a pas besoin de matrices de bases pour construire les transparents. Les résultats expérimentaux indiquent le privilège de notre méthode par rapport aux autres travaux connexes.

Notre schéma proposé tire profit des schémas précédents de taille invariable basés sur des opérations booléennes et de la fonctionnalité progressive de la cryptographie visuelle dans laquelle le contraste des images secrètes révélées est amélioré progressivement, en créant un schéma (k, n) qui a les propriétés suivantes :

— La taille des transparents et l'image secrète reconstruite est la même que la taille de l'image secrète originale (pas d'expansion de pixels).
— Notre schéma n'a pas besoin de matrices de base pour créer des shares.
— A partir des transparents générés n $(n \geq 2)$, nous avons pu obtenir $n-1$ images secrètes révélées avec un contraste amélioré progressivement de façon croissante à partir de la qualité la plus basse, dans le cas de deux transparents, à une qualité plus haute dans le cas d'empilement de tous les transparents n.
— La quantité de détails de l'image récupérée (contraste) est proportionnelle aux nombres d'ombres empilés.
— Une reconstruction parfaite et sans perte de l'image secrète révélée peut être obtenue lorsque tous les transparents sont superposés en utilisant les opérations booléennes OR et XOR.
— Notre méthode proposée est adaptée aux images binaires, en niveaux de gris, en couleurs et demi-ton. De plus, elle convient à la fois pour l'empilement d'un

nombre pair ou impair de transparents.

Comparé à d'autres systèmes, notre proposition présente de nombreux avantages. Le reste de cette première partie du chapitre est organisé comme suit : Dans la deuxième section, nous définissons quelques notions de bases utilisées dans notre schéma suggèré. Dans la section trois nous présentons notre schéma proposé (Algorithme de génération des shares et de révélation du secret avec une preuve mathématique. Un exemple et un schéma illustratif sont donnés pour mieux éclairer l'algorithme proposé. Dans la quatrième section, nous donnons nos résultats expérimentaux et nous les comparons avec les autres schémas similaires. Enfin, nous finirons par donner une conclusion de notre travail.

5.2 Des concepts clés utilisés dans notre schéma proposé

Avant d'introduire notre schéma de partage progressif du secret basé sur les opérations booléennes XOR et OR. Nous définissons d'abord quelques concepts utilisés durant la conception de notre approche :

5.2.1 La fonction Booléenne XOR

La fonction XOR, également appelée "Ou exclusif", est un opérateur logique de l'algèbre de Boole. Il prend en entrée deux valeurs booléennes (vrai ou faux) et renvoie une autre valeur booléenne. Tel que : (0= faux) et (1=vrai).

TABLE 5.1 – Table de vérité de l'opérateur XOR.

a	b	$f(a,b)=a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0
1	A	$\overline{A}$
A	$\overline{A}$	1

5.2.2 La fonction Booléenne OR

La fonction OR, également appelée "Ou inclusif", est un opérateur logique de l'algèbre de Boole. Il prend en entrée deux valeurs booléennes (vrai ou faux) et renvoie une autre valeur booléenne.

Le tableau 5.1 et le tableau 5.2 présentent respectivement les tables de vérité des opérations booléennes XOR, et le OR. Le tableau 5.3 montre le bit complémentaire d'un nombre binaire.

TABLE 5.2 – Table de vérité de l'opérateur OR.

a	b	$f(a,b)=a+b$
0	0	0
0	1	1
1	0	1
1	1	1
A	A	A
A	1	1
A	0	A

TABLE 5.3 – Complément d'un bit.

a	$f(a)=\overline{a}$
1	0
0	1

5.2.3 Notion des images numériques

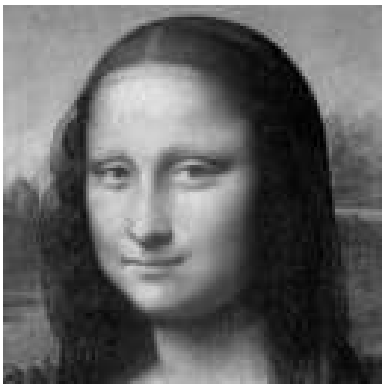
Une image est un ensemble de nombre infini de points appelés pixels. Il existe 2 sortes d'images numériques : les images matricielles et les images vectorielles. Les données des images vectorielles sont représentées par des formes géométriques décrites comportant différents attributs (bordure, fond, forme, coordonnées), tandis qu'une image matricielle est formée d'un ensemble de points ou pixels contenus dans une grille rectangulaire.

1. Les images binaires : ce sont des images ne comportant que 2 niveaux de gris, le noir (0) et le blanc (1).

2. Les images en niveaux de gris : ce sont les images appelées noir et blanc dans le langage courant. Ce type d'image peut avoir n'importe quelle nuance entre le noir et le blanc (gris). Ces valeurs sont appelées niveaux de gris et sont représentés par des entiers de 0 à N-1.
3. Les images couleur : la couleur est représentée par 3 valeurs qui sont les composantes (RVB : Rouge, Vert, Bleu). Le code binaire de l'image est obtenu en indiquant successivement pour chaque pixel le code binaire des 3 composantes, si on code chaque composante sur 8 bits, chaque pixel sera donc représenté par 24 bits. Le mode de codage le plus répandu en traitement numérique des images est le système additif de codage RVB. Ce dernier correspond directement aux systèmes d'affichage sur un écran. En plus, il est plus simple à manipuler au niveau des opérations de combinaison de couleur pour obtenir plusieurs nuances. Cependant il existe d'autres modes de représentation des couleurs comme le modèle soustractif (CMJN :le Cyan, Magenta, Jaune, Noir) utilisé principalement pour l'impression (figure 5.2).
4. Les images à demi-ton : sont des images sur lesquelles le processus de tramage (utilisé par les imprimantes) est appliqué en imprimant côte à côte des points noirs et blancs en créant une lésion optique d'un grand nombre de nuances.

(a) Exemple d'une image binaire

(b) Exemple d'une image couleur



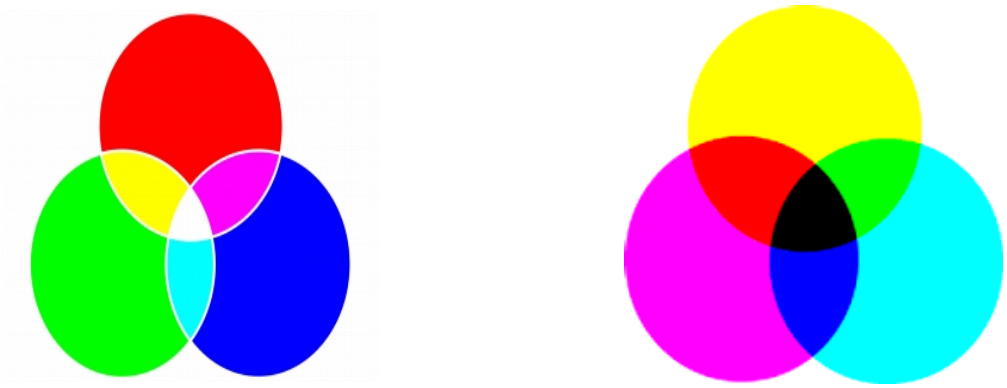
(c) Exemple d'une image en niveaux de gris

(d) Exemple d'une image a demi-teinte

FIGURE 5.1 – Présentation de différents types d'images

5.3 Méthode Proposée

Pour surmonter les problèmes causés par l'expansion du pixel et obtenir un contraste progressif, nous proposons un schéma (k, n) convenable pour les images binaires, en niveaux de gris et en couleurs. L'opération booléenne XOR est utilisée pour générer les transparents, et les opérations booléennes OR et XOR sont utilisées pour reconstruire l'image secrète. Au début de cette section, nous introduisons quelques concepts clés utilisés durant la conception de notre approche. Puis nous introduisons notre schéma de partage de secret progressif. Une preuve est donnée pour éclairer la faisabilité de notre méthode suggérée, puis un exemple démonstratif concret est illustré. A la fin nous donnons nos résultats expérimentaux et les comparons avec les autres schémas connexes.



(a) Le modèle additif RVB (b) Le modèle soustractif CMJN

FIGURE 5.2 – Présentation de différents modèles de couleurs

5.3.1 Conception de la méthode proposée

Les Figures 5.3 et 5.4 montrent la conception de notre méthode proposée dans le cas où le nombre de shares est pair et impair respectivement :

5.3.2 Le schéma proposé (k,n) progressif de partage de secret basé sur des opérations Booléennes

Dans cette section, nous présentons notre schéma de partage de secret (k,n). L'algorithme 1 décrit le processus de génération des transparents et l'algorithme 2 décrit le processus de reconstruction de l'image secrète.

Algorithme 1 (La phase de construction de transparents)
Entrée : Soit SI une image secrète de taille $l * m$, où l indique indice de lignes et m montrel'indice de colonnes.
$n \geq 2$, un entier représentant le nombre de participants et k un nombre qui représente le nombre d'ombres empilées $2 \leq k \leq n$.
Sortie : n transparents S_1,...,S_n.
Étape1 : générer NM, une matrice aléatoire de la même taille que l'image secrète SI où l c'est indice de ligne et m l'indice de colonne.
Étape2 : générer une matrice de définition de régions RDM de la même taille que SI : $l * m$, où l c'est indice de ligne et m l'indice de colonne qui contient des nombres aléatoires i , allant de 1 à n répartis uniformément dans la matrice RDM.
Nous définissons une région R_i dans la matrice RDM comme toutes les positions ou les coordonnées (x,y) dans RDM, où : $RDM(x,y)$=i.

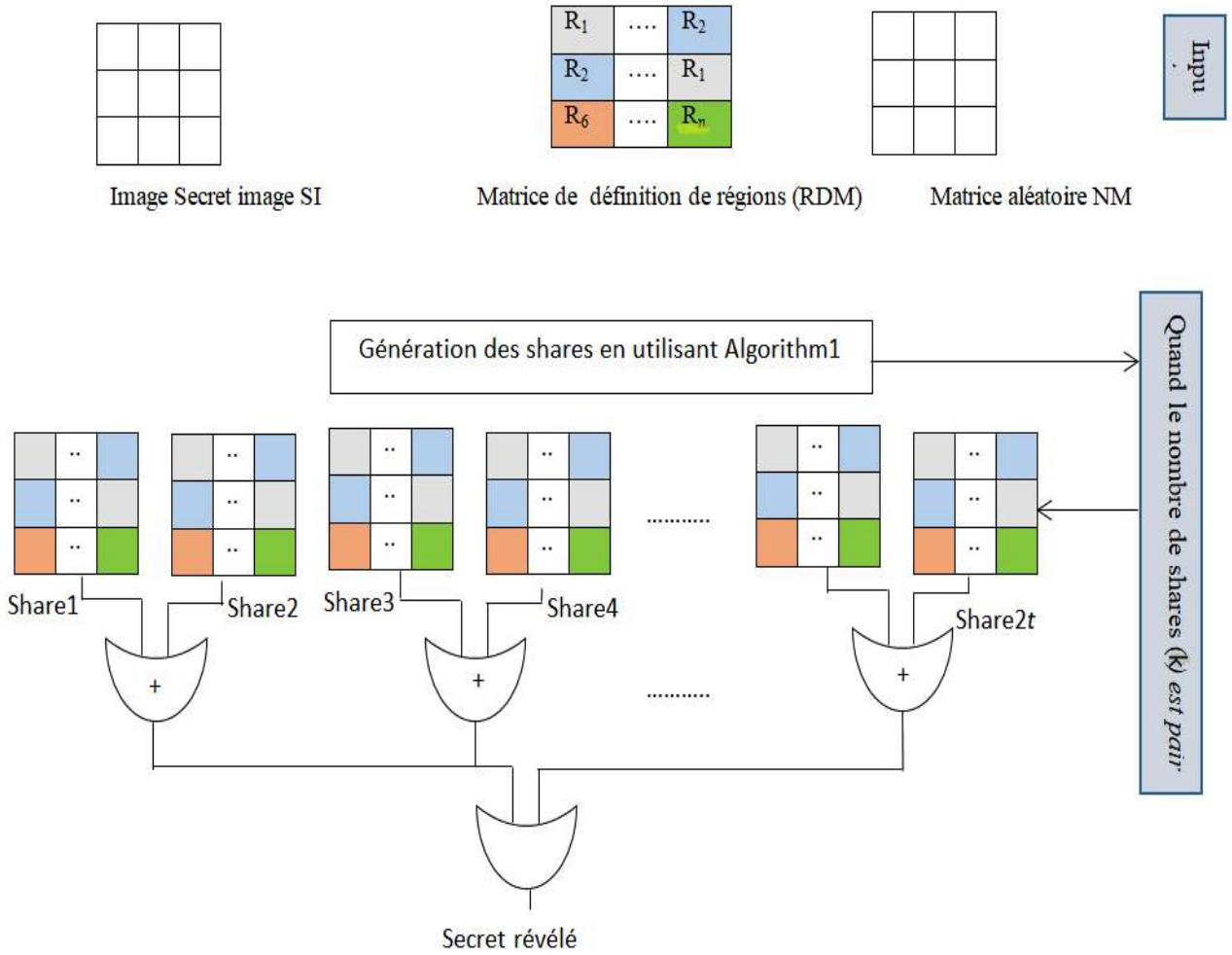


FIGURE 5.3 – Illustration du schéma proposé lorsque le nombre de transparents est pair

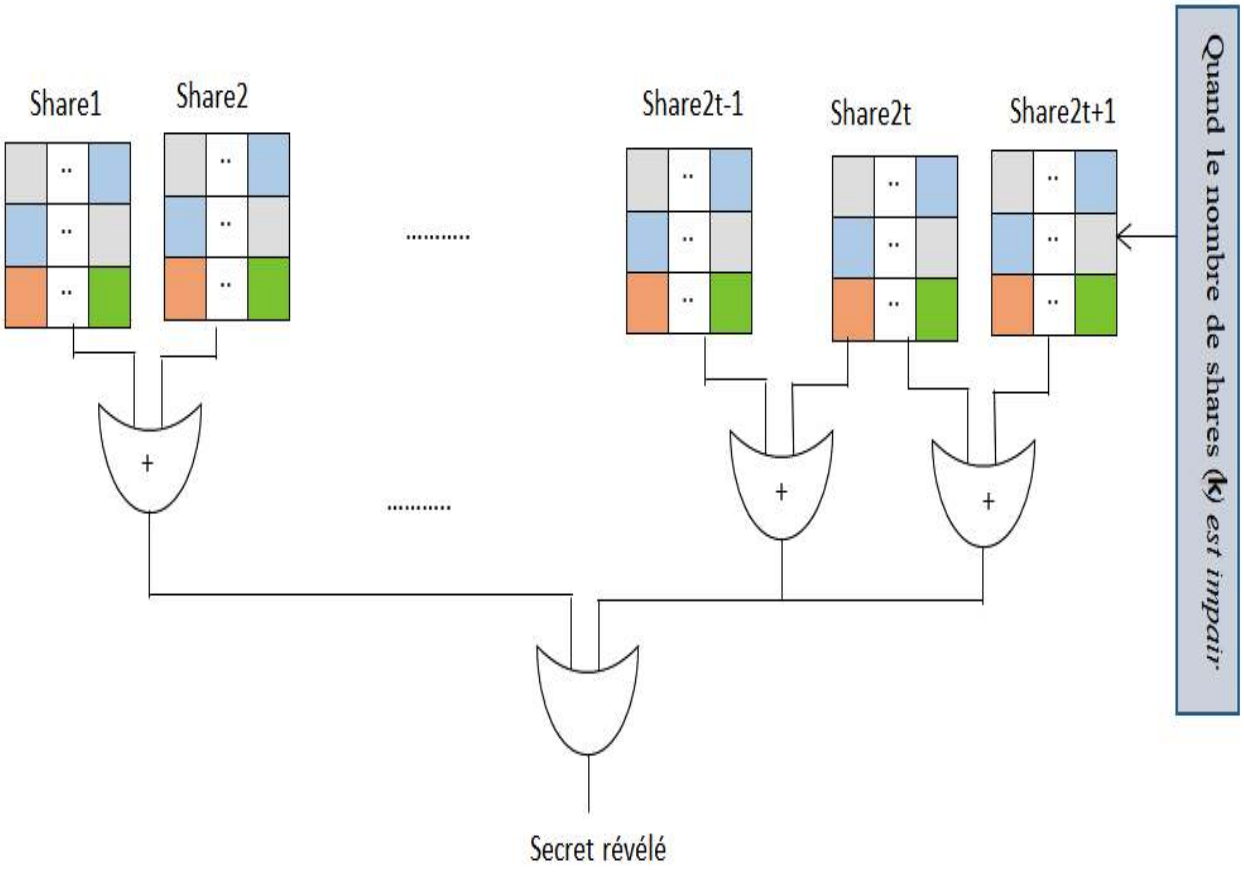


FIGURE 5.4 – Illustration du schéma proposé lorsque le nombre de transparents est impair

Étape3 :

Pour i=: n ;
La région R_i de S_i est remplie par :
$S_i(R_i)$=$NM(R_i) \oplus \overline{SI}(R_i)$;
Pour $1 \leq j \leq n, (i \neq j)$;
La région R_i de S_j est remplie par :
$S_j(R_i)$=$\overline{NM}(R_i)$.
fin,
fin,
fin.

Notons que la matrice RDM de l'étape 2, décrit comment les pixels des transparents S_i sont cryptés et comment ils sont situés dans la région correspondante R_i. Toutes les régions dans RDM sont uniformément distribuées et dispersées sur l'image entière, contrairement aux régions définies dans la méthode de Chen Y & Chen L [99], qui sont dispersées manuellement par le distributeur seulement sur des régions spécifiques qui sont censées être protégées.

Algorithme 2 (Phase de révélation de secret)
Entrée : n transparents S_1, ..., S_n générés en utilisant l'algorithme 1.
Sortie : Révélation complète du secret RS lors de l'empilement de tous les transparents $k, 2 \leq k \leq n$ et une révélation progressive autrement.
L'empilement d'un nombre de transparents k garantit que l'image secrète révélée est d'une qualité visuelle équivalente.
Étape1 : *Si le nombre de shares est pair* k=$2 * p$, *alors :*
Faire un XOR '$\oplus$' de chaque deux transparents successifs (le premier avec le second, le troisième avec le quatrième ... etc.). Puis appliquer l'opération booléenne OR qui est présentée par le symbole'+', entre les résultats obtenus.
$RS_{1,2}$=$S_1 \oplus S_2$.
$RS_{3,4}$=$S_3 \oplus S_4$.
$\vdots$
$RS_{2p-1,2p}$=$S_{2p-1} \oplus S_{2p}$.
RS=$RS_{1,2}$+$RS_{3,4}$+...+$RS_{2p-1,2p}$.
Sinon Si le nombre de transparents est impair $k = 2p+1$, *alors :*
Faire la même opération précédente, et aussi faire un XOR entre le dernier transparent impair et son transparent prédécesseur (le transparent $n-1$ avec le transparent n) puis faire l'opération OR entre les résultats :

$RS_{1,2}$=$S_1 \oplus S_2$.
$RS_{3,4}$=$S_3 \oplus S_4$.
$\vdots$
$RS_{2p-1,2p}$=$S_{2p-1} \oplus S_{2p}$.
$RS_{2p,2p+1}$=$S_{2p} \oplus S_{2p+1}$.
$RS = RS_{1,2} + RS_{3,4} + \ldots + RS_{2p-1,2p} + RS_{2p,2p+1}$.
Notons que si k=n, la reconstruction parfaite est achevée.

5.3.3 Preuve du schéma (k, n) de partage progressif de secret proposé

Nous montrons ci-dessous la phase de construction des transparents décrite dans l'algorithme 1 et la phase de reconstruction du secret décrite dans l'algorithme 2 de notre schéma (k, n) PSS. Les définitions suivantes sont utilisées dans cette preuve :

- SI : représente une image secrète qui sera partagée entre n nombre de participants.
- NM : est une matrice aléatoire bruyante.
- RDM : est une matrice de définition de régions qui contient n régions aléatoires distribuées uniformément comme défini dans l'algorithme 1.
- $SI(R_i)$: représente les pixels secrets appartenant à la région R_i.
- $NM(R_i)$: sont tout les pixels aléatoires dans NM appartenant à la région R_i,
- $0(R_i)$: signifie que l'intensité des pixels appartenant aux régions R_i sont mis à 0.
- $RS_{i,j}$: signifie que le transparent numéro i est empilé avec le transparent numéro j, ainsi tout les pixels correspondants aux régions R_i et R_j sont révélés.
- RS : révélation complète du secret.

On a :

$$\begin{cases} R_1 \cap R_2 \cap \ldots \cap R_n = \phi, \\ R_1 \cup R_2 \cup \ldots \cup R_n = SI. \end{cases} \tag{5.1}$$

Construction des transparents

S_1=$\overline{SI}(R_1) \oplus NM(R_1) \cup \overline{NM}(R_2) \cup \ldots \cup \overline{NM}(R_n)$.
S_2=$\overline{NM}(R_1) \cup \overline{SI}(R_2) \oplus NM(R_2) \cup \ldots \cup \overline{NM}(R_n)$.
$\vdots$
S_k=$\overline{NM}(R_1) \cup \overline{NM}(R_2) \cup \ldots \cup \overline{SI}(R_k) \oplus NM(R_k) \cup \ldots \cup \overline{NM}(R_n)$.

S_n=$\overline{NM}(R_1) \cup \overline{NM}(R_2) \cup \ldots \cup NM(R_n) \oplus \overline{SI}(R_n)$.

Reconstruction du secret :

a) Quand le nombre de transparents est pair k=$2p$, $2 \leq k \leq n$ (cas de reconstruction progressive)

$RS_{1,2}$=$S_1 \oplus S_2$=$SI(R_1) \cup SI(R_2) \cup \ldots \cup 0(R_{2p})$.

$RS_{3,4}$=$S_3 \oplus S_4$=$0(R_1) \cup 0(R_2) \cup SI(R_3) \cup SI(R_4) \cup \ldots \cup 0(R_{2p})$.

$\vdots$

$RS_{2p-1,2p}$=$S_{2p-1} \oplus S_2 p$=$0(R_1) \cup 0(R_2) \cup \ldots SI(R_{2p-1}) \cup SI(R_{2p})$.

RS=$RS_{1,2}$+$RS_{3,4}$+...+$RS_{2p-1,2p}$.

RS=$SI(R_1) \cup SI(R_2) \cup SI(R_3) \cup SI(R_4) \cup \ldots \cup SI(R_{2p-1}) \cup SI(R_{2p})$.

a.1) If k=n (reconstruction parfaite)

RS=$SI(R_1) \cup SI(R_2) \cup \ldots \cup S(R_n)$=$SI$.

b) Quand le nombre de transparents est impair k=$2 * p$+1, $2 \leq k \leq n$ (cas de reconstruction progressive)

$RS_{1,2}$=$S_1 \oplus S_2$=$SI(R_1) \cup SI(R_2) \cup 0(R_3) \cup \ldots \cup 0(R_{2p+1})$.

$RS_{3,4}$=$S_3 \oplus S_4$=$0(R_1) \cup 0(R_2) \cup SI(R_3) \cup SI(R_4) \cup \ldots \cup 0(R_{2p+1})$.

$\vdots$

$RS_{2p-1,2p}$=$S_{2p-1} \oplus S_2 p$=$0(R_1) \cup 0(R_2) \cup \ldots \cup SI(R_{2p-1}) \cup SI(R_{2p})$.

$RS_{2p,2p+1}$=$S_{2p} \oplus S_{2p+1}$=$0(R_1) \cup 0(R_2) \cup \ldots \cup SI(R_{2p-1}) \cup SI(R_{2p}) \cup SI(R_{2p+1})$.

RS=$RS_{1,2}$+$RS_{3,4}$+...+$RS_{2p-1,2p}$+$RS_{2p,2p+1}$.

RS=$SI(R_1) \cup SI(R_2) \cup SI(R_3) \cup SI(R_4) \cup \ldots \cup SI(R_{2p-1}) \cup SI(R_{2p}) \cup SI(R_{2p+1})$.

b.1) Quand $k = 2 * p + 1 = n$ (reconstruction parfaite)

RS=$SI(R_1) \cup SI(R_2) \cup SI(R_3) \cup \ldots \cup SI(R_{2p}) \cup SI(R_{2p+1})$=$RS$

5.3.4 Exemple du schéma $(2,2)$ de la méthode proposée

Un exemple illustrant la méthode proposée est donné dans cette section pour démontrer les étapes de calcul de l'algorithme ci-dessus avec n=2 et de taille $3 * 3$ de l'image secrète SI :

136	33	37
28	35	44
162	26	51

Et la matrice de définition de régions RDM :

2	2	1		R_2	R_2	R_1
1	2	2	→	R_1	R_2	R_2
2	1	1		R_2	R_1	R_1

Comme expliqué dans l'algorithme 1, une région R_i dans RDM représente tous les emplacements ou les coordonnées (x, y) dans RDM, où : $RDM(x, y)=i$. Donc la région R_1 représente les coordonnées $(1,3)(2,1)(3,2)(3,3)\}$ et la région R_2 représente les coordonnées $\{(1,1)(1,2)(2,2)(2,3)(3,1)\}$.

La matrice aléatoire bruyante NM est :

181	178	9
168	82	113
71	211	98

Les transparents $S1$ et $S1$ sont calculés par l'algorithme 1 comme suit :
La région R_1 de S_1 est remplie avec : $S_1(R_1)=NM(R_1) \oplus \overline{SI}(R_1)$:
$S_1(1,3)=NM(1,3) \oplus \overline{SI}(1,3)=9 \oplus \overline{37}=211$.
$S_1(2,1)=NM(2,1) \oplus \overline{SI}(2,1)=168 \oplus \overline{28}=75$.
$S_1(3,2)=NM(3,2) \oplus \overline{SI}(3,2)=211 \oplus \overline{26}=54$.
$S_1(3,3)=NM(3,3) \oplus \overline{SI}(3,3)=98 \oplus \overline{51}=174$.

La région R_2 de S_1 est remplie avec : $S_1(R_2)=\overline{NM}(R_2)$:
$S_1(1,1)=\overline{NM}(1,1)=\overline{181}=74$.
$S_1(1,2)=\overline{NM}(1,2)=\overline{178}=77$.
$S_1(2,2)=\overline{NM}(2,2)=\overline{82}=173$.
$S_1(2,3)=\overline{NM}(2,3)=\overline{113}=142$.
$S_1(3,1)=\overline{NM}(3,1)=\overline{71}=184$.

La région R_1 de S_2 est remplie avec : $S_2(R_1)=\overline{NM}(R_1)$:
$S_2(1,3)=\overline{NM}(1,3)=\overline{9}=246$.
$S_2(2,1)=\overline{NM}(2,1)=\overline{168}=87$.
$S_2(3,2)=\overline{NM}(3,2)=\overline{211}=44$.
$S_2(3,3)=\overline{NM}(3,3)=\overline{98}=157$.

La région R_2 de S_2 est remplié avec : $S_2(R_2)=NM(R_2) \oplus \overline{SI}(R_2)$:
$S_2(1,1)=NM(1,1) \oplus \overline{SI}(1,1)=181 \oplus \overline{136}=194$.

$S_2(1,2)$=$NM(1,2) \oplus \overline{SI}(1,2)$=178 $\oplus \overline{33}$=108.
$S_2(2,2)$=$NM(2,2) \oplus \overline{SI}(2,2)$=82 $\oplus \overline{35}$=142.
$S_2(2,3)$=$NM(2,3) \oplus \overline{SI}(2,3)$=113 $\oplus \overline{44}$=162.
$S_2(3,1)$=$NM(3,1) \oplus \overline{SI}(3,1)$=71 $\oplus \overline{162}$=26.

Ainsi les deux transparents S_1 et S_2 seront respectivement :

74	77	211
75	173	142
184	54	174

194	108	246
87	142	162
26	44	157

Le premier pixel secret est révélé en faisant un XOR entre : 74 $\oplus$ 194 = 136.
Le secret est révélé en superposant les transparents S_1 avec S_2 comme suit : $S_1 \oplus S_2$=RS.

5.4 Résultats expérimentaux et comparaison

Pour analyser les performances du schéma de partage progressif de secret (k,n) proposé et montrer nos résultats expérimentaux, nous appliquons notre schéma pour partager une image en niveaux de gris. Pour cela, nous choisissons l'image de 'Baboon.jpg'. La taille de cette image est $256 * 256$ pixels. Nous chiffrons et partageons l'image entre cinq participants, n=5 en utilisant Matlab R2013a. La figure 5.5 montre l'image secrète originale. Les cinq transparents générés en utilisant l'algorithme 1 sont représentés dans la figure 5.7 (a, b, c, d et e) respectivement.
En utilisant l'algorithme 2, en empilant progressivement un nombre $k, (2 \leq k \leq 5)$ de transparents avec des opérations booléennes OR et XOR, nous obtenons quatre images secrètes ($n-1$=4) avec un contraste amélioré :

1. La première image secrète progressive est représentée sur la Fig 5.6 (a), qui est reconstruite à partir de deux transparents quelconques (S_i, S_j) avec $(1 \leq i, j \leq 5)$ et $(i \neq j)$.
2. La seconde image secrète progressive est reconstruite à partir de n'importe quel trois transparents (S_i, S_j, S_m) avec $(1 \leq i, j, m \leq 5)$ et $(i \neq j \neq m)$ comme le montre la figure 5.7 (b).
3. La figure (c) présente la troisième image secrète progressive qui est reconstruite à partir de quatres transparents (S_i, S_j, S_m, S_k) avec $(1 \leq i, j, k, m \leq 5)$ et $(i \neq$ j $\neq k \neq m)$.
4. Une reconstruction parfaite de l'image secrète est achevée dans la figure 5.6 (d).

L'inspection visuelle des figure 5.7 (a), (b), (c), (d) illustre la capacité de reconstruction progressive qui varie de la plus faible qualité en cas de $(2,5)$ à la plus haute qualité en cas de $(5,5)$. Comme mentionné dans la preuve donnée ci-dessus, en superposant n'importe quel transparent S_i avec n'importe quel transparent S_j $(1 \leq i, j \leq n)$ avec $(i \neq j)$, nous ne pouvons révéler que des pixels secrets dans les régions R_i et R_j et à chaque fois qu'un nouveau transparent S_m $(1 \leq m \leq n)$, $(m \neq j \neq i)$ est superposé, la quantité des informations secrètes est augmentée en révélant tout les pixels secrets correspondants à toutes les régions R_m. Toutes les régions seront divulguées et une révélation parfaite du secret est réalisée en superposant tout les transparents :

— Les transparents partagés S_1 et S_3 révèlent tout les pixels secrets dans les régions R_1 et R_3, alors que les autres pixels des régions R_2, R_4 R_5, sont mis à zéros.
— La superposition des trois transparents, par exemple (S_3, S_5, S_2), révèle chaque pixel secret dans les régions R_3, R_5 et R_2, tandis que les autres pixels appartenant aux régions R_1, et R_4 sont mis à zéros ...etc.
— La superposition de tout les transparents $(S_1, S_2, S_3, S_4, S_5)$ révèle tout les pixels

secrets dans toutes les régions, de telle sorte que l'image secrète soit divulguée complètement.

Dans ce schéma proposé, aucune information n'est obtenue à partir d'un seul transparent. Dans notre schéma proposé le processus de construction des shares est rapide, et le processus de révélation du secret est assez facile et ne nécessite pas d'étapes de calcul complexes. Notre schéma suggéré peut être appliqué à tout les types d'images : binaires, demi-teinte, vrai-gris et vrai-images couleur.

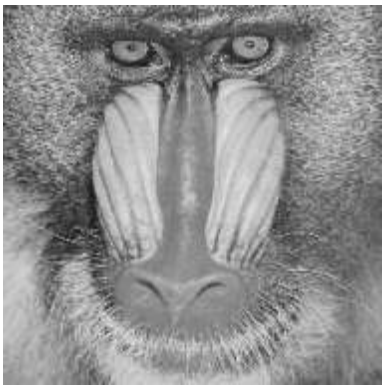
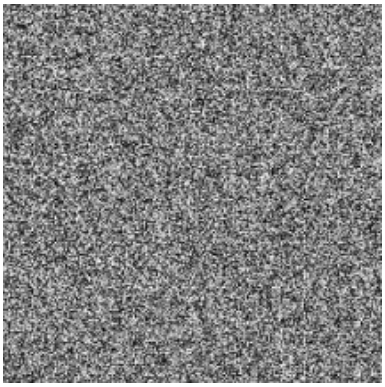


FIGURE 5.5 – Image Secrète.

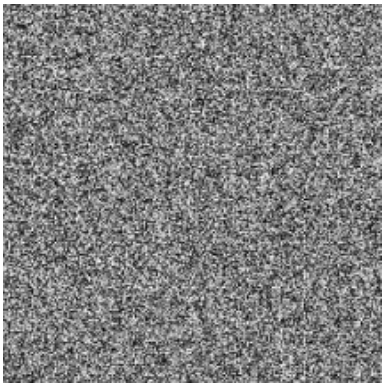
5.4.1 Mesure de la qualité des images récupérées en utilisant le $PSNR$

Nous utilisons le $PSNR$ pour mesurer la similarité entre l'image secrète et les quatre images récupérées, où :
$PSNR$=$10 * log_{10} * \frac{255^2}{MSE} dB$.
Et MSE représente l'erreur quadratique moyenne : $MSE = \frac{1}{n*m} \sum_{i=1}^{n} \sum_{j=1}^{m} (a_{i,j} - b_{i,j})^2$.

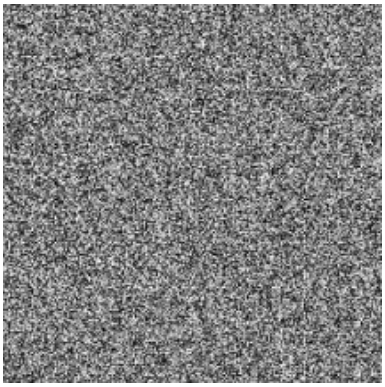
Où : n et m représentent respectivement la valeur des pixels de l'image secrète et de l'image révélée. Une valeur élevée de $PSNR$ indique que les pixels de l'image reconstruite n'ont pas subi de grande altération, plus la valeur $PSNR$ est élevée, plus les deux images sont similaires. Lorsque nous superposons deux, trois, quatre transparents, nous obtenons des valeurs $\{7.90, 9.72, 12.71\}$ de PSNR respectivement. La valeur $PSNR$ est égale à l'infinie lorsque tout les cinq transparents sont empilés, ce qui signifie que l'image reconstruite est exactement similaire à l'image originale secrète. Par conséquent on constate que la qualité de l'image récupérée a une haute qualité. Notons que le contraste de n'importe quelle combinaison de deux transparents super-



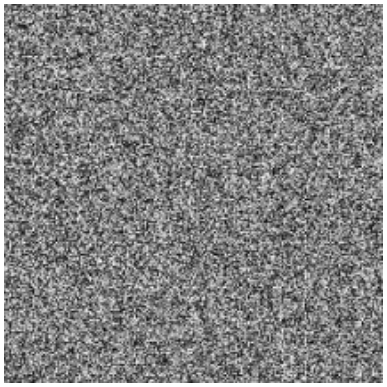
(a) Transparent1.



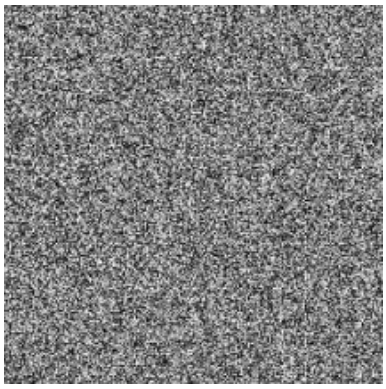
(b) Transparent2.



(c) Transparent3

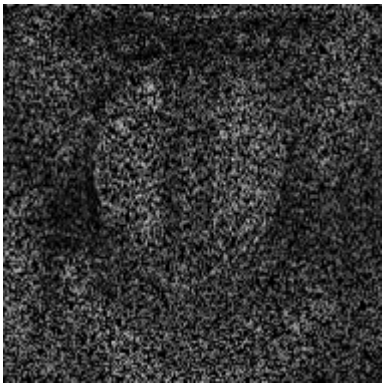


(d) Transparent4

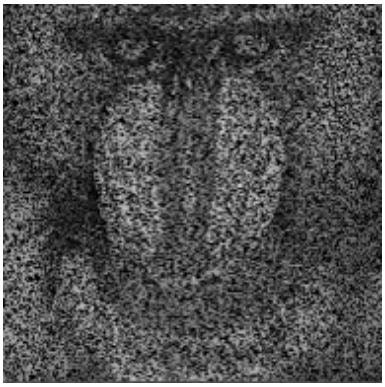


(e) Transparent5

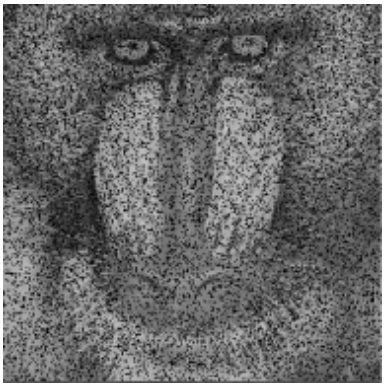
FIGURE 5.6 – Les 5 transparents générés par l'algorithme 1.



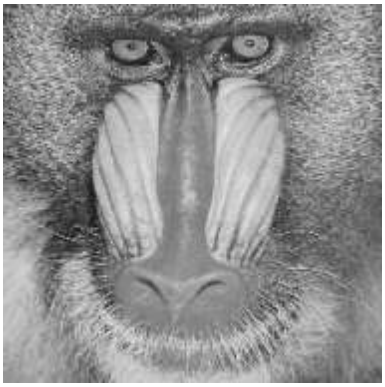
(a) Première construction progressive réalisée par n'importe quels deux transparents.



(b) Deuxième construction progressive réalisée par n'importe quels trois transparents.



(c) Troisième construction progressive réalisée par n'importe quels quatre transparents.



(d) Reconstruction parfaite de tous les shares

FIGURE 5.7 – Construction progressive du secret à partir des transparents générés.

posés est assez similaire parce que toutes les régions sont distribuées aléatoirement. La même chose s'applique lorsqu'on superpose une combinaison de trois ou quatre transparents comme indiqué dans le tableau 5.4.

TABLE 5.4 – Les valeurs PSNR de nos résultats expérimentaux

Nombre de transparents	Toutes les combinaisons possibles	Valeur $PSNR$
(S_i, S_j)	$\{(S_1,S_2),(S_1,S_3),(S_1,S_4),(S_1,S_5),(S_2,S_3)$ $,(S_2,S_4),(S_2,S_5),(S_3,S_4),(S_3,S_5),(S_4,S_5)\}$	$7.90dB$
(S_i, S_j, S_m)	$\{(S_1,S_2,S_3),(S_1,S_3,S_4),(S_1,S_4,S_5),(S_2,S_4,S_3),(S_2,S_4,S_5)$ $,(S_1,S_5,S_3),(S_1,S_2,S_5),(S_2,S_5,S_3),(S_2,S_4,S_1),(S_3,S_4,S_5)\}$	$9.72dB$
(S_i, S_j, S_m, S_h)	$\{(S_1,S_2,S_3,S_4),(S_1,S_3,S_4,S_5),(S_1,S_2,S_4,S_5),(S_1,S_2,S_5,S_3)$ $,(S_2,S_5,S_3,S_4)\}$	$12.71dB$
$(S_i, S_j, S_m, S_h, S_g)$	$\{(S_1,S_2,S_3,S_4,S_5)\}$	infini

5.4.2 La relation entre la propriété progressive et le $PSNR$ du schéma proposé

Pour notre schéma suggéré, supposons que la taille de l'image secrète est $l * c$, où l index de ligne et c index de colonne. $n \geq 2$ un entier représentant le nombre de participants.

Pour deux transparents $(2, n)$, la partie des pixels révélés correctement est $\frac{2}{n}$, donc :

— Le nombre de pixels révélés correctement est $(l * c)(\frac{2}{n})$.
— $(l * c)\frac{(n-2)}{n}$, pixels sont révélés 0 (incorrects). Cela entraînera un $PSNR_2$.

Pour trois transparents $(3, n)$, la partie des pixels révélés correctement est $\frac{3}{n}$, donc :
— Le nombre de pixels révélés est $(l * c)(\frac{3}{n})$.
— $(l * c)\frac{(n-3)}{n}$ pixels sont révélés 0 (incorrects). Cela entraînera un $PSNR_3$.
Pour k transparents schéma (k, n), la partie des pixels révélés correctement est $\frac{k}{n}$, donc :
— Le nombre de pixels révélés est $(l * c)(\frac{k}{n})$.
— $(l * c)\frac{n-k}{n}$ sont révélés 0 (incorrects). Cela entraînera un $PSNR_k$.

Il est clair que $(PSNR_3 \geq PSNR_2)$ parce que le nombre de pixels révélés correctement dans le schéma $(3, n)$ est plus grand que le nombre de pixels révélés correctement dans le cas de deux transparents. De même en suivant le même raisonnement si on prend k, $k \geq \ldots 3 \geq 2$, on aura donc le nombre de pixels révélés correctement pour k transparents $\geq \ldots \geq$ le nombre de pixels révélés correctement pour trois shares $\geq$ le nombre de pixels révélés correctement pour deux transparents, et donc

$PSNR_k \geq \ldots \geq PSNR_3 \geq PSNR_2$. Enfin pour le schéma (n,n), le nombre de pixels révélés correctement est $(l)(\frac{n}{n})$=$l*c$, donc toute l'image secrète est révélée correctement et par conséquent le $PSNR_n$=$infini$. Aussi nous avons prouvé qu'en augmentant progressivement le nombre de transparents, le $PSNR$ et par conséquent la qualité visuelle de l'image révélée augmentera graduellement jusqu'à la révélation entière de toute l'image secrète.

Exemple d'illustration

En supposant que la taille de l'image secrète est de 256 $*$256. n=5 un entier représentant le nombre de participants.

Pour tout deux transparents superposés, la partie des pixels révélés est $\frac{2}{5}$, donc le nombre de pixels révélés est $(256*256)(\frac{2}{5})$=26214 et $(256*256)\frac{(5-2)}{5}$=39322, pixels sont révélés 0 (incorrects). Cela se traduira par un $PSNR_2$=7.90dB.

Pour tout trois transparents superposée, la portion de pixels révélés est correctement $\frac{3}{5}$, donc le nombre de pixels révélés est correctement $(256*256)(\frac{3}{5})$=39322 et $(256*256)\frac{(5-3)}{5}$=26214, pixels sont révélés 0 (incorrects). Cela se traduira par un $PSNR_3$=9.72dB.

Pour tout quatre transparents superposés, la portion de pixels révélés est correctement $\frac{4}{5}$, donc le nombre de pixels révélés est $(256*256)(\frac{4}{5})$=52429 et $(256*256)\frac{(5-4)}{5}$=13107, pixels sont révélés 0 (incorrects). Cela se traduira par un $PSNR_4$=12.71dB.

Pour tout cinq transparents superposés, tous les pixels sont révélés correctement, donc le nombre de pixels révélés correctement est $(256*256)(\frac{5}{5})$=65536. Cela donnera une valeur $PSNR_5$=$infini$.

Il est clair qu'a chaque fois que nous élevons le nombre de transparents superposés, le nombre de pixels révélés correctement est augmenté ainsi que le $PSNR$, ($PSNR_5 \geq PSNR_4 \geq PSNR_3 \geq PSNR_2$). Par conséquent, la qualité visuelle de l'image révélée sera progressivement améliorée jusqu'à l'obtention de la révélation de toute l'image secrète.

5.4.3 La relation entre le nombre des utilisateurs n et le seuil k

Dans notre cas, il existe une relation analytique entre le nombre des utilisateurs n et le seuil k. Au fait; à chaque fois le nombre des utilisateurs augmente, le seuil k change, pour lequel la première reconstruction progressive achève, par exemple pour $n = 5$, le nombre minimum pour lequel la première reconstruction du secret apparue égale à 2 ($k = 2$) avec un $PSNR = 7.90$. Si on change le nombre n; le seuil k va aussi être changé et par conséquent le PSNR du secret reconstruit. Nous comptons donner plus de détails pour un futur travail et amélioration de l'approche proposée.

5.5 Comparaison avec les autres schémas

Nous comparons notre approche proposée en termes d'expansion des pixels, de la reconstruction progressive, de la qualité de l'image reconstruite. Nous comparons

aussi notre approche avec les autres types d'images utilisés dans des travaux similaires, et aussi en termes d'efficacité de calcul avec des schémas basés sur des opérations booléennes. Tout les résultats de la comparaison de notre schéma (k,n) de partage de secret progressif basé sur des opérations booléennes avec d'autres schémas connexes sont résumés dans le tableau 5.5.

5.5.1 Comparaison en termes d'expansion de pixels

L'avantage des transparents non expansés est offert par notre méthode. La taille de tout les transparents et les images reconstruites est la même que la taille de l'image secrète originale, contrairement au premier schéma de Naor et shamir [8], et les travaux de [25], [23], [166] et [26].

5.5.2 Comparaison en termes de reconstruction progressive

La manière progressive de reconstruction du secret est l'un des principaux avantages de notre schéma. Dans le tableau 5.5, nous pouvons voir que notre schéma offre la caractéristique progressive par rapport aux schémas dans [8], [25], [10], [76] et [167]. Dans le schéma rapporté par [167], seuls les transparents dites non essentielles peuvent améliorer la qualité de l'image reconstruite et tout les autres transparents essentiels et non essentiels peuvent reconstruire précisément l'image secrète.

5.5.3 Comparaison en termes d'application sur différents type d'images

Notre schéma peut être appliqué à tout type d'images notons les images binaires, en niveaux de gris, couleurs et demi-teintes comparé avec le schéma progressif de [166] et comparé aux schémas basés sur des opérations booléennes proposés par [8], [25], [10] et [76].

5.5.4 Comparaison en termes de contraste

Notre schéma peut atteindre une excellente qualité visuelle (sans perte) lorsque tout les transparents sont empilés par rapport aux schémas de partage progressifs de secret suivants : [26], [24], [23] , [102], [168].

5.5.5 Comparaison en termes de nombre de participants

De plus, comme nous pouvons le voir dans le tableau 5.5, la plupart des schémas connexes sont disponibles pour un nombre limité de participants et non pour un schéma à seuil général comme dans le schéma de [8], [10], [76] et [167]. Bien que le premier travail de PSS, qui a été fait par Hou et Quan. [102], utilise des shares non expansés et la qualité de l'image récupérée est bonne. Leur schéma n'est pas fait pour un schéma général à seuil (k,n). Quant au travail réalisé par [167] qui présentait un

schéma de partage progressif du secret basé sur le seuil essentiel et la fonction booléenne. Le principal inconvénient de leur schéma est le nombre de transparents utilisés pour construire parfaitement l'image secrète qui ne doit pas être inférieure à quatre n=4.

5.5.6 Efficacité en matière de calcul

Aucunes matrices de base n'est utilisée pour construire des transparents, contrairement aux schémas dans [8], [23] et [24]. Le processus de codage et de décodage n'implique pas des opérations booléennes XOR et OR complexes, contrairement au travail présenté en 2017 par Tapasi et al. [114], où le processus de décryptage basé sur les opérations booléennes affines nécessite de nombreuses opérations par rapport au schéma proposé.

Ref	Schéma	Expansion de pixels	Format d'image	Progressif	Contraste	Décryptage
[8]	$(2,2)$	$2*2$	Binaire	non	avec perte	OR (SVH)
[25]	(n,n)	1	Binaire	non	sans pertes	XOR
[25]	$(2,n)$	$2*2$	Binaire	non	avec pertes	XOR
[23]	(k,n)	$3*3$	tout types	oui	avec pertes	XOR
[24]	(k,n)	$2*2$	Binaire	oui	avec pertes	OR (SVH)
[24]	(k,n)	$2*2$	Binaire	oui	avec pertes	OR (SVH)
[10]	(n,n)	1	niveaux de gris & color	non	sans pertes	XOR
[10]	$(2,n)$	1	Binaire	non	avec pertes	XOR, AND
[26]	(k,n)	$2*2$	Demi-teinte	oui	avec pertes	OR (SVH)
[167]	$(2,n)$	1	Binaire & niveaux de gris	non	sans pertes	XOR, OR
[76]	$(2,n)$	1	Binaire	non	sans pertes	XOR, OR
[102]	$(2,n)$	1	Demi-teinte	oui	avec pertes	OR (SVH)
[168]	(k,n)	1	niveaux de gris & couleur	oui	avec pertes	OR (SVH)
[167]	(k,n)	1	Binaire & niveaux de gris	oui	sans pertes	OB affine
Schéma proposé	(k,n)	1	Tous types	oui	sans pertes	XOR, OR

TABLE 5.5 – Comparaison du schéma proposé avec les autres schémas connexes.

D'après la table 5.5, il est clair qu'on peut avoir un schéma flexible en terme du nombre des utilisateurs (k,n), un schéma où le nombre de pixels codés est $(m=1)$, un schéma avec un contraste parfait, un schéma qui a la caractéristique progressive dans le processus de révélation du secret, et un schéma applicable sur tout type d'images. Cependant, le challenge consiste à trouver une approche de partage de secret qui achève toutes ces fonctionnalités ce qui vérifie notre approche proposée.

Approche de partage de secret audible : cryptographie audio

Les techniques traditionnelles de cryptographie et de partage de secret utilisent un dispositif de calcul pour décrypter des données secrètes, ceci n'est pas très pratiques dans le cas où l'ordinateur n'est pas accéssible. Cet inconvénient a ouvert la porte de la recherche a deux techniques cryptographiques importantes, qui peuvent décoder des données secrètes en utilisant des sens humains, qui sont : le partage de secret visuel (cryptographie visuelle) [8] et le partage de secret audio (cryptographie audible) [48]. Comme nous avons montré dans cette partie que dans la CV, l'utilisateur peut décrypter le secret en utilisant le système visuel humain (SVH), tandis que le partage de secret audio (PSA) [48], on utilise le système auditif humain (SAH) pour pouvoir décrypter le secret.

Le PSA introduit par Desmedt et al en 1998 [48], dans lequel le secret qu'on voudrait partager est sous forme d'audio, dans ce cas le déchiffrement peut être fait par l'ouïe humaine au lieu du système visuel humain. Le processus de cryptage (schéma à seuil) se fait de la même manière que la CV conventionnelle [8], mais les données secrètes et/ou transparents sont des documents sonores. Malheureusement la question des transparents élargies existe également dans le partage de secret audible. Contrairement à la CV où le donneur augmente le nombre de pixels dans chaque transparent, dans le PSA, le concessionnaire augmente le nombre de bips dans chaque transparent ce qui affecte la taille et la qualité des transparents et par conséquent la qualité du secret audio reconstruit. Afin de surmonter le problème des transparents élargies et obtenir un schéma idéal : Lin et al. [169], Ehdaie et al. [170] et Patil et al. [171] proposent des schémas de partage de secret audio avec une taille des transparents non expansée.

Dans cette deuxième partie du chapitre, nous choisissons l'un des articles les plus cités dans la CV qui résout le problème de l'expansion des pixels, simplement en utilisant une simple opération booléenne XOR dans le processus de décryptage et appliquons son schéma à seuil (n, n) pour partager un mot de passe secret entre n nombre de participants. Dans la section deux de cette partie nous présentons le schéma de partage de secret audio modifié de Wang et al. [10], puis dans la section trois nous montrons nos résultats expérimentaux, enfin nous donnons une conclusion.

5.6 Application du schéma de Wang et al. pour le schéma audio secret

Le schéma de partage d'images secrètes de Wang et al. [10] est basé sur l'algèbre booléenne en utilisant l'opération XOR dans le processus de déchiffrement. Avant d'appliquer le schéma de partage d'audio secret de Wang et al., nous devons faire d'abord un pré-traitement sur le fichier audio secret de type (.wav). On commence par quantifier le fichier audio secret en le codant sur des échantillons de huit bits :

SQ=$round(255(Secret - Min(Secret)/Max(Secret) - Min(Secret))$.

Où : Min et Max représentent respectivement la valeur minimale et maximale de l'audio secret, puis nous arrondissons l'audio secret quantifié à l'entier le plus proche, puis au lieu d'utiliser des images aléatoires pour construire des transparents, nous utilisons des données audio pour créer des transparents (mot de passe secret), tel que la taille du secret audio est de même taille que les transparents.

Algorithme de Wang et al. [10] pour le partage de secret audio

Entrée : mot de passe secret audio S, et un entier $n \geq 2$,
Sortie : n transparents / ombres $T_1, \ldots, T_n$.
Phase une : quantification du signal secret S à l'aide d'un quantificateur linéaire bien connu :
Mot de passe secret quantifié SQ=$round(255(S-Min(S)/(Max(S)-Min(S)))$; tel que : $Min(S)$: la valeur minimale de l'audio secret à partager. $Max(S)$ la valeur maximale de l'audio secret à partager.

Phase deux : Construction des transparents audio :

1)générer $n-1$ vecteurs aléatoires $B_1, \ldots, B_{n-1}$,
2) calculer n ombres audio :
T_1=B_1,
T_2=$B_1 \oplus B_2$,
T_{n-1}=$B_{n-2} \oplus B_{n-1}$,
$\vdots$
T_n=$B_{n-1} \oplus A$
Phase trois : reconstruction de l'audio secret "S" :
S=$T_1 \oplus T_2 \oplus ... \oplus T_n$

5.7 Les Résultats expérimentaux

Les résultats expérimentaux de l'utilisation de l'algorithme de Wang et al. sont illustrés aux figures 5.9, 5.10, 5.11 et 5.12 : dans la figure 5.9, l'audio secret est présenté, cependant, dans les figures 5.10 et 5.11, les shares audio sont générés par algorithme mentionné ci-dessus et enfin l'audio secret révélé est montré dans la figure 5.12 lorsque tous les transparents sont joués simultanément. Ces résultats ont été mis en œuvre en utilisant Matlab2013. Grâce au (PSNR) nous mesurons la similarité entre l'audio secret originale et l'audio secret reconstruit, une valeur élevée de $PSNR$ indique que le signal reconstruit a une bonne qualité, tel que :

$PSNR$=$10 * log_{10}(MAX^2/MSE)$ (1)

Où : MSE est l'erreur quadratique moyenne entre le secret audio et l'audio reconstruit, cependant MAX est la valeur maximale du signal, elle est égale à 255 dans notre cas. En utilisant l'équation (1), nous trouvons que la valeur du : $PSNR$=$Infinie$, ce qui veut dire que l'audio secret révélé a été reconstruit avec une haute qualité sans distorsion.
Quant aux similarités statistiques : on calcule la corrélation entre les deux signaux, on

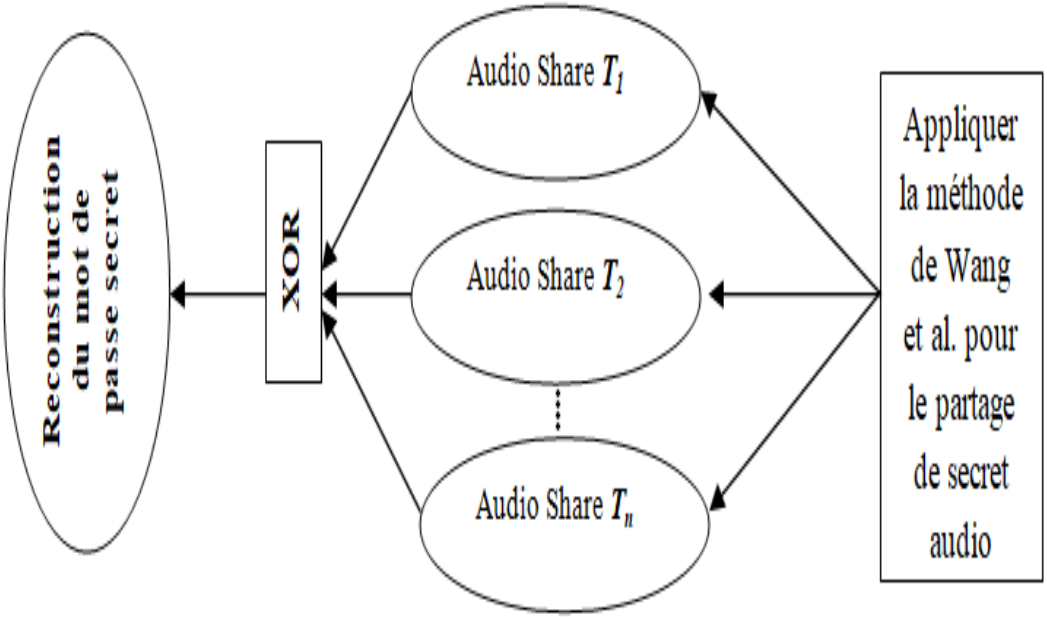


FIGURE 5.8 – Schéma de partage de secret audio Wang et al.

trouve donc la valeur "1", ce qui signifie que l'audio secret a une forte corrélation avec l'audio secret reconstruit, donc aucune perte d'information dans l'audio secret reconstruit n'est trouvée.
Le tableau ci-dessous donne une comparaison entre l'application de la méthode de Wang et al. pour le secret audible et d'autres systèmes de partage de secret audible. Les résultats décrits montrent que le schéma s'applique parfaitement pour partager un secret audio et donne des résultats aussi bons à ce qui en existent.

TABLE 5.6 – Comparaison de notre schéma de partage de secret auditif avec d'autre schémas

Année	Auteurs	Schéma	Shares	Décryptage	Secret
1998	Desmedt et al. [48]	(2,n)	Expansé	(SAH)	Bit string
2005	Ehdaie et al. [170]	(k,n)	non-Expansé	(SAH)	Audio
2012	Yoshida et al. [172]	(n,n)	Expansé	(SAH)	Audio
2014	Abukari et al. [173]	(k,n)	Expansé	Ordinateur	Audio
2015	Pati et al. [169]	(k,n)	non-Expansé	Ordinateur	Audio
2015	Application de Wang et al. [10]	(n,n)	non-Expansé	Ordinateur	Audio

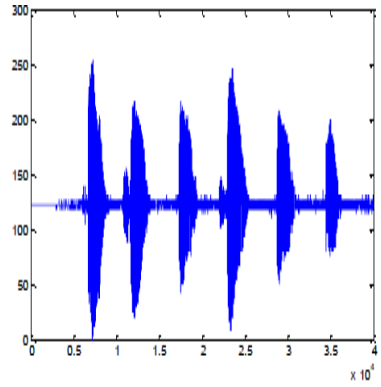


FIGURE 5.9 – Secret audio

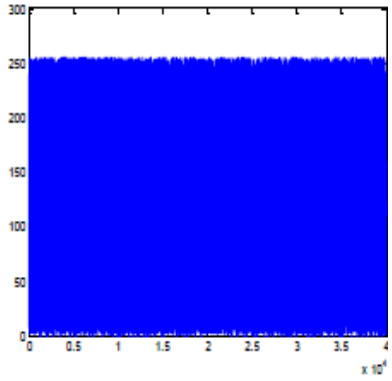


FIGURE 5.10 – Le premier share audio

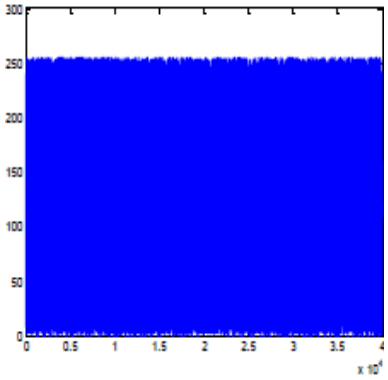


FIGURE 5.11 – Le deuxième share audio

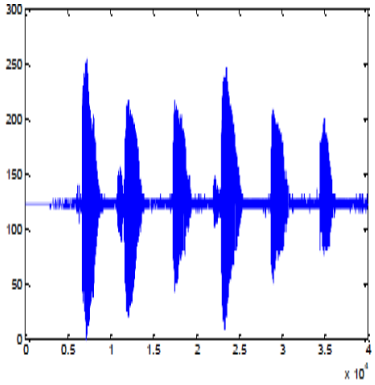


FIGURE 5.12 – Secret audio reconstruit

5.8 Conclusion

Dans la plupart des schémas de partage secrets, il n'est pas toujours facile d'obtenir un équilibre entre de nombreuses caractéristiques souhaitables telles qu'une taille minimale des pixels, une bonne qualité des images reconstruite, une reconstruction progressive, un seuil général k, et aussi l'adaptation du schéma à différents types d'images. Dans ce chapitre nous avons présenté deux schémas de partage de secret l'un pour un partage progressif du secret basé sur des opérations Booléennes et l'autre est une application pour partager un secret audio.
Dans la première partie du chapitre nous avons créé un schéma qui combine deux caractéristiques importantes dans les schémas de partage de secret : la première c'est la taille invariante des shares qu'on a pu atteindre grâce a l'utilisation des opérations booléennes et la deuxième c'est la caractéristique progressive de partage de secret pour créer un schéma (k, n) dont lequel le processus de déchiffrement est effectué grâce aux opérations booléennes XOR et OR. Notre schéma est non seulement de taille invariante mais aussi il a une reconstruction parfaite du secret lorsque tous les participants superposent leurs transparents et un contraste progressif amélioré autrement. Notre modèle proposé est adapté pour les images binaires, niveaux de gris, en couleurs, demi-ton. De plus, notre schéma n'utilise pas des matrices de base pour la construction des shares.

Cependant dans certains cas, nous avons besoin de partager non seulement des

informations visuelles comme le texte et l'image, mais aussi des documents audio secrets, d'où le développement des systèmes de partage de secret audio. En effet le partage de secret audio entre participants est très important notamment dans le domaine militaire. C'est pourquoi dans la deuxième partie du chapitre nous avons choisi l'algorithme de Wang et al. pour appliquer sa méthode pour partager des documents audio. Le choix est porté sur cet algorithme vu ses bonnes propriétés :

— Se débarrasser de la faiblesse du schéma de Naor et Shamir en réduisant le nombre d'expansion de pixels à 1, donc nous pouvons appliquer son schéma pour résoudre le même problème dans la cryptographie audible.
— L'utilisation de l'opération booléenne XOR dans le processus de décryptage.

Les résultats expérimentaux montrent que cet algorithme est parfaitement applicable pour les données audio et le secret audio est parfaitement reconstruit avec une haute qualité. Nous concluons que Wang et al. est applicable aussi pour le partage des secrets audio-visuel, ce qui signifie que leur système est convenable pour partager à la fois des images secrètes et des fichiers audio secrets.

Chapitre 6

Contribution au tatouge

6.1 Introduction

Comme toute information transmise sur le réseau, le bruit du canal de transmission ou les attaques provoquées par les pirates peuvent détruire ou modifier toute donnée non protégée. Afin de résoudre ce problème, le tatouage numérique [149] y joue un rôle primordial. Notre contribution dans ce chapitre consiste à intégrer un tatouage fragile dans l'un des schémas les plus intéressant de la cryptographie visuelle, c'est le schéma de Wang et al. Ce dernier qui résout le principal problème de la cryptographie visuelle [8] qui est l'expansion de pixel, en utilisant une simple opération booléenne XOR dans le processus de décryptage et nous proposons d'améliorer sa sécurité à l'aide d'un tatouage fragile basé sur le code de détection et de correction d'erreur BCH [161] afin de vérifier l'intégrité du secret reconstruit.

La plupart des techniques de tatouage fragile [152] [153] consiste à détecter les erreurs en utilisant différentes méthodes comme le CRC ...etc. En effet il est nécessaire de corriger les erreurs après les avoir détectées : dans notre approche, nous appliquons un code correcteur BCH afin de pouvoir détecter et corriger les erreurs survenues. Pour cela nous appliquons un BCH réduit (16,11) sur chaque deux pixels adjacents de tout les transparents générés par la méthode de wang et al. [10] ensuite, nous utilisons la technique LSB qui consiste à insérer les bits de contrôles générés par le code BCH(16.11) réduit d'un code BCH de longueur (31,26) dans les bits de poids faible de chaque deux pixels. Le $PSNR$ de l'image tatouée est mesuré après l'ajout d'un bruit gaussien sur chaque transparent, puis nous appliquons le code BCH de longueur (16,11), pour détecter et corriger les erreurs et on recalcule le $PSNR$ pour voir le montant de l'information qui a été récupérée par le code BCH. Le reste de ce chapitre est organisé comme suit :
Dans la deuxième section, nous présentons le schéma de partage de secret de Wang et al., puis dans la troisième section, nous présentons toutes les étapes utilisées pour générer le tatouage en se basant sur un code de détection et de correction d'erreur BCH et nous voyons comment l'insérer dans les transparents générés par le méthode de Wang et al. [10]. La quatrième section présente nos résultats expérimentaux. A la fin de ce chapitre nous donnons une conclusion de notre travail.

6.2 L'application du tatouage fragile sur la méthode de Wang et al. [10] en se basant sur le code de détection et de correction d'erreur BCH

Dans cette section, nous allons présenter le schéma de partage de secret de Wang et al. [10], puis nous décrivons comment générer le tatouage en utilisant le code de correction d'erreur BCH et nous voyons la façon d'insertion dans les différents transparents afin de vérifier l'intégrité de l'image secrète.

6.2.1 L'Algorithme de partage de secret de Wang et al. [10]

Le schéma de partage de secret de Wang et al. est basé sur l'utilisation de l'opérations booléenne XOR dans le processus de décryptage. Ce schéma utilise le même concept des schémas à seuil tel qu'une image secrète S destinée à être partager entre les $n \geq 2$ nombre de participants. Pour faire cela, le négociateur (distributeur) crée n images aléatoires appelées transparents générées en utilisant l'algorithme ci-dessous. Lorsque tous les participants superposent leurs transparents, l'image secrète sera reconstruite parfaitement : Si au moins un nombre $n-1$ de participants superposent leurs transparents, aucune information ne peut être donnée sur le secret [49]. Le principal avantage de cette méthode en la comparant avec beaucoup de méthodes existantes de la CV se situe dans la taille des transparents qui est de même taille que l'image secrète originale, contrairement au schéma de Naor et Shamir [8] où la taille des transparents est m fois plus grande que l'image secrète ce qui peut influencer sur le coût et la capacité de mémoire.

Entrée : Image secret S et un entier $n \geq 2$,
Sortie : n transparents : $T_1, \ldots, T_n$.

Phase une : construction des transparents :
1)générer $n-1$ matrices aléatoires $B_1, \ldots, B_{n-1}$,
2) calculer les n transparents comme suit :
T_1=B_1,
T_2=$B_1 \oplus B_2$,
T_{n-1}=$B_{n-2} \oplus B_{n-1}$,
$\vdots T_n$=$B_{n-1} \oplus A$
Phase deux : reconstruction du secret S :
S=$T_1 \oplus T_2 \oplus \ldots \oplus T_n$

6.2.2 Objectif d'insertion du watermark dans les transparents

En pratique, quand le négociateur crée tout les transparents et les envoi sur le réseau, ils peuvent être modifiés soit par les pirates soit par le bruit provoqué sur le canal de transmission, ce qui rend la qualité de l'image reconstruite pauvre et elle pourra même être illisible dans certain cas. Pour vérifier si ces transparents ont été modifiés et par conséquent afin de vérifier l'intégrité de l'image révélée, nous proposons d'insérer un tatouage fragile dans les pixels des transparents à l'aide du code correcteur BCH [160] de longueur réduite pour détecter et corriger les erreurs éventuelles et récupérer une quantité importante d'informations qui a été perdue.

6.2.3 Objectif d'utilisation du code correcteur BCH, et le BCH(16,11) réduit

Comme nous avons expliqué dans le chapitre précèdent des codes correcteurs, les codes BCH et Reed Solomon sont parmi les excellents codes qui sont largement utilisés pour détecter et corriger plusieurs erreurs [19]. Reed Solomon est utilisé en cas de

codes non binaires, cependant le code BCH peut être utilisé parfaitement avec le code binaire.
Sachant que les paramètres du code BCH(n,k) sont :
— z=$2^m - 1$: représente la longueur du message après le codage, $m \geq 3$.
— k : la longueur du message à encoder.
— $z - k$: le nombre de bits de contrôle à rajouter au message.
— t : le nombre de corrections dans chaque block de n symboles que le code BCH peut corriger.
— $2t$: représente le nombre de détections des erreurs.
— $g(x)$: est le polynôme générateur construit sous un corps de Galois GF(2), qui est le multiple le moins commun du polynôme minimal de l'élément primitif α^p,

Comme nous voyons (Table 4.1 du chapitre 4), on constate que la longueur du code BCH est impaire. En effet dans notre cas, nous avons besoin d'une longueur paire du message codé car la longueur d'un pixel en niveaux de gris est codée sur huit bits. Le code BCH raccourci [160] peut résoudre un tel problème et rendre la longueur des données flexible selon le besoin de l'utilisateur.

6.2.4 Réduction de la longueur du code BCH

Nous raccourcissons le code BCH de (z, k) à $(z - s, k - s)$ pour qu'il soit flexible avec notre besoin, pour cela :
— Nous ajoutons dans le processus de codage, un feint bit (des zéro) de longueur s, derrière les $k - s$ bits d'information pour atteindre la longueur de k bits.
— Le code BCH (z,k) encode les k bits en z bits. $k - s$-bits sont obtenus après avoir enlevé les s faux bits rajoutés.
— Pendant le décodage, un nombre s de zéros est ajouté pour atteindre la longueur de n bits,
— k bits sont obtenus par le décodeur BCH (z,k), puis nous nous débarrassons des s zéro ajoutés et obtenons seulement $k - s$ bits d'information.

Codage par le code BCH

Pour encoder un message en utilisant le code BCH, nous avons besoin de générer un polynôme générateur $g(x)$, le message $m(x)$ est ensuite multiplié par x^d, où d est le degré du polynôme générateur $g(x)$. Donc, le message sera codé comme suit : $r(x)$=$(m(x) * x^d)/g(x)$.

Détection des erreurs

Pour vérifier si le message reçu contient des erreurs, le récepteur le divise par le même polynôme générateur. Si le reste de la division est nul, aucune erreur n'a été détectée, sinon le récepteur doit les corriger.

Décodage par le code BCH : [160]

Supposons que $c(x)$=$r(x)$+$e(x)$´ est le code reçu, où $e(x)$ sont les erreurs qui peuvent survenir sur le message transmis :

1. Calculer le syndrome du code reçu en le divisant sur chaque élément primitif du polynôme générateur comme suit : S_p=$c(x)$ mod $mp_p(x)$, où $mp_p(x)$ est le polynôme minimal de l'élément primitif α_p
2. Trouver la position des erreurs et les corriger en utilisant l'algorithme de "Peterson" ou l'algorithme de "Masse de Berlekamp" [20]. Dans notre cas, nous avons utilisé l'algorithme de "Masse Berlekamp" en raison de sa simplicité.

6.2.5 Algorithme de génération du tatouage à l'aide de BCH raccourci (16,11)

Entrée : $T_i, 2 \leq i \leq n$ représente les matrice de transparents générés par l'algorithme de wang et al.
K : la clé secrète qui est le polynôme générateur $g(x)$ utilisé.
Sortie : $W_i, 2 \leq i \leq n$ matrices de tatouage de la même taille que les transparents, dont chaque deux pixels adjacents contiennent cinq bits de contrôle générés par le BCH raccourci (16,11). Parmi ces cinq bits, on va mettre dans le premier pixel de W_i les trois premiers bits de contrôle et dans le pixel adjacent de W_i les deux derniers bits de contrôle. La figure 6.1 montre le processus d'insertion du tatouage aux transparents.
Les Étapes :

— Pour tout pixels de chaque transparent, on prend chaque deux pixels adjacents (le premier avec le deuxième, le troisième avec le quatrième...etc.) et on fait la concaténation des cinq bits de poids le plus fort (MSB) du premier pixel avec les six bits de poids le plus fort du pixel adjacent et on les code en utilisant le code BCH raccourci (16,11).
— Pour coder les 11 bits en utilisant le code BCH (16,11), raccourci du code BCH (31,26), nous ajoutons 15 faux bits, derrière les 11 bits d'informations pour atteindre la longueur de 26 bits.
— En utilisant le code BCH (31,26), les 26 bits sont codes en 31 bits, par conséquent, 16 bits sont obtenus après avoir enlevé les 15 faux bits (zéros) rajoutés.
— Au cours du processus de décodage 15 zéros sont ajoutés pour atteindre la longueur de 31 bits, puis 26 bits sont obtenus en utilisant le décodant BCH(31,26).
— Nous pouvons nous débarrasser des 15 faux bits rajoutés et obtenir seulement 16 bits d'information, donc notre message encodé consiste à multiplier les 11 bits de poids le plus fort MSB par x^{15} et les diviser par le polynôme générateur suivant : $g(x)$=1+x^4+x^5+x^6+x^7+x^8+x^{10}+x^{12}+x^{13}+x^{14}+x^{15}.
— Pour chaque deux pixels adjacents de chaque transparent nous obtenons $z-k$=5 bits de contrôle qui sont le tatouage.
— Les trois premiers bits obtenus sont mis dans le pixel correspondant de la matrice correspondante W_i, tandis que les deux derniers bits sont mis au pixel adjacent de la même matrice.

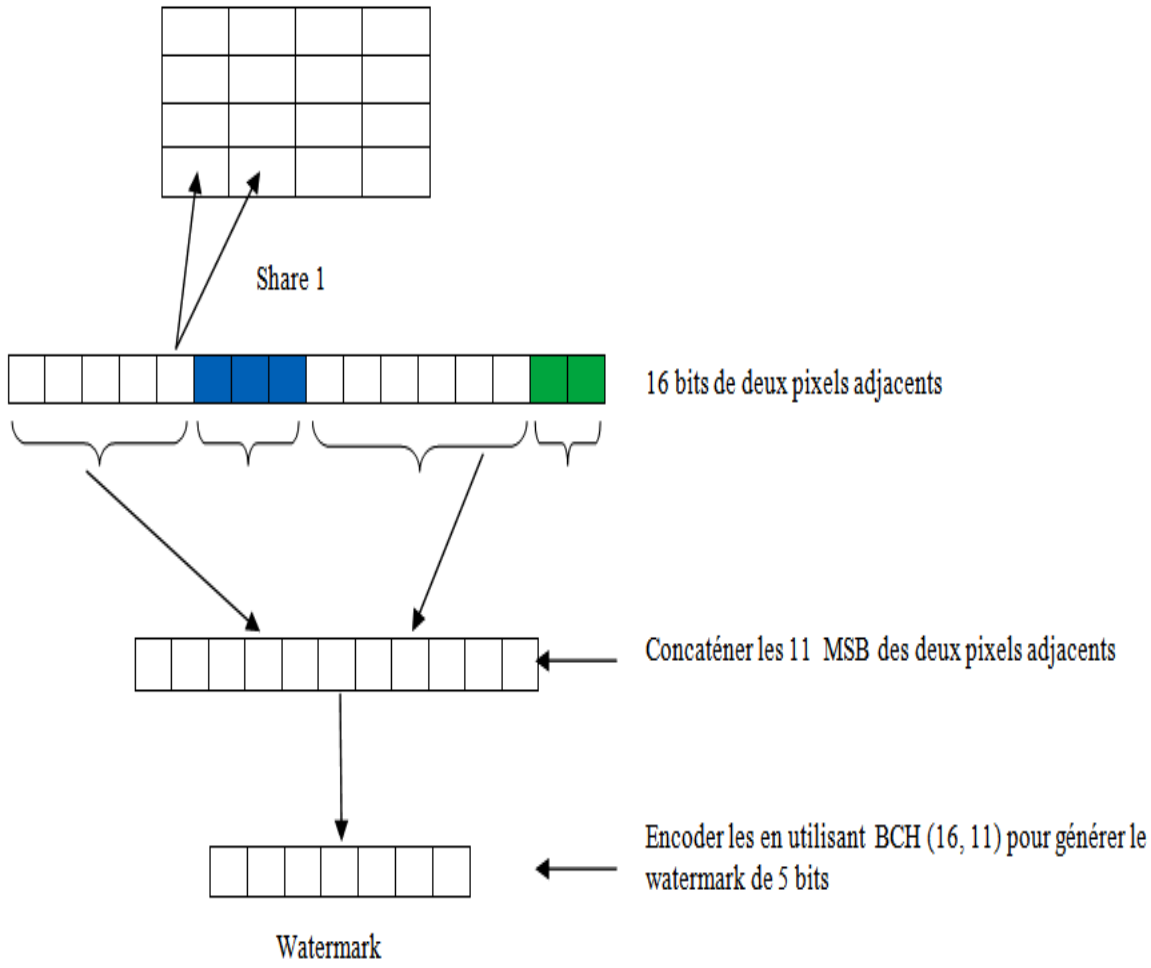


FIGURE 6.1 – Algorithme de génération d watermark en utilisant le BCH(16,11) raccourci.

6.2.6 Algorithme d'insertion du tatouage fragile aux transparents

Nous avons obtenu cinq bits de contrôle en utilisant le code BCH raccourci (16,11), ces bits sont considérés comme étant la marque qui va être insérée dans les bits de poids faible de chaque deux pixels adjacents des transparents. Cette insertion ne va pas beaucoup altérer l'information des transparents et par conséquent, il n'y aura pas de gros changement sur la qualité de l'image secrète. La figure 6.2 montre le processus d'insertion du tatouage aux transparents.

Entrée : Matrices de tatouages : $W_i; 2 \leq i \leq n$, n transparents :

Sortie : Matrices de transparents tatoués $WS_i; 2 \leq i \leq n$,

— Insérer chaque pixel obtenu de la matrice de tatouage W_i dans le pixel correspondant du transparent T_i, l'insertion se fait de telle sorte que :

— Les trois premiers bits de contrôle sont insérés dans les trois LSB du pixel correspondant de la matrice T_i.

— Les deux derniers bits de contrôle sont insérés dans les deux LSB du pixel adjacent de la matrice T_i.
— Apres l'insertion $i, 2 \leq i \leq n$, nombre de transparents tatoués sont obtenues WS_i.

6.2.7 Exemple d'insertion du tatouage dans un transparent

— Pour le premier transparent généré, soit les deux pixels : $s(1,1)$=17, $s(1,2)$=55.
— Conversion des bits ci-dessus en séquence binaires, 17=10001000 , 55=11101100.
— Concaténation des cinq bits du poids fort du pixel s(1,1) avec les six bits du poids fort du pixel $s(2,2)$, c=10001111011.
— Ajout 15 zéros m=10001111011000000000000000 pour atteindre la longueur de 26.
— Encoder l'ensemble des bits en utilisant le BCH(31,26), après on enlève les 15 zéros ajoutés et on obtient seulement 16 pixels, donc le codage(m)= 10001111011 11001.
— Les bits de contrôle à insérer dans la matrice de transparent tatoué sont : 11001, les bits 110 sont insérés dans les bits du poids faible du pixel s(1,1), et 01 sont insérés dans les bits de poids faible du pixel s(2,2).

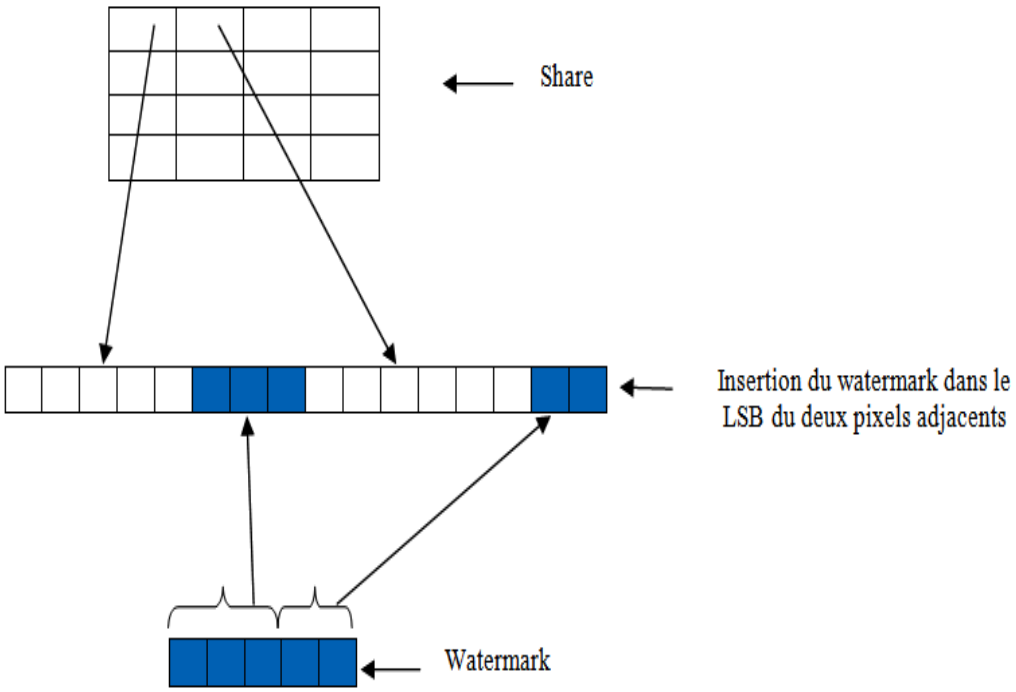


FIGURE 6.2 – Méthode d'insertion du watermark en utilisant un BCH(16,11) raccourci

6.3 Résultats Expérimentaux

Dans le schema de Wang et al. [10], le concessionnaire va créer des transparents pour pouvoir révéler le secret en utilisant l'algorithme ci-dessus. Soit le nombre de

transparents générés est n=2. Supposons que ces transparents vont être envoyés sur un canal de transmission, en effet ces transparents peuvent être affectés par le bruit du canal de transmission, ce qui va influencer sur la qualité de l'image secrète. Nous simulons un bruit gaussien sur les deux transparents puis nous mesurons la qualité de l'image tatouée, avant et après l'application du code correcteur BCH (16,11) pour pouvoir détecter et corriger les erreurs de transmission.

Dans La figure 6.3, l'image secrète est présentée. Les figures 6.4 et 6.5 montrent les deux shares tatoués. Les figures 6.6 montre l'image secrète reconstruite après l'addition d'un bruit gaussien sur les deux transparents, et la dernière figure et 6.7 montre l'image secrète reconstruite après utilisation du BCH raccourci (16,11). Notons que la mise en œuvre de cet algorithme a été effectuée à l'aide de Matlab 2013.

6.3.1 La relation entre la qualité de l'image reconstruite et la capacité de correction des erreurs du BCH(16,11)

Le récepteur divise chaque bloque codé grâce au code BCH (16,11), des transparents constitués de 16 bits, par le même polynôme générateur. S'il trouve que le reste de la division est nul, il constate qu'aucune erreur n'a été détectée, sinon il doit les corriger. Dans notre cas la qualité de l'image reconstruite dépend du BCH choisi, plus le BCH choisi génère beaucoup de bits de contrôle, plus on modifie beaucoup de bits de poids faibles des transparents, plus la qualité de l'image reconstruite sera dégradée. Cependant L'avantage de ce type de BCH qui génère beaucoup de bits de contrôle est la possibilité d'une correction d'erreurs élevée par rapport au BCH qui génère peu de bits de contrôle. En effet, il faut trouver un compromis entre la qualité souhaitable et le nombre des erreurs détectables. Aprés avoir testé différents codes BCH de longueurs différentes, on a constaté que le BCH (16,11) est le plus adéquat pour notre schéma : le nombre des erreurs qui peuvent être détectées dans chaque deux pixels est t=1, et notre code choisit peut corriger jusqu'à t=2 erreurs dans chaque deux pixels.

6.3.2 La qualité de l'image secrète reconstruite (imperceptibilité)

D'après Cox et al. [149], la qualité de l'image tatouée ne doit pas être affectée par le tatouage inséré. Pour tester l'impercibilite de notre approche nous mesurons la qualité de notre image reconstruite a partir de tout les transparents avant et après l'insertion du tatouage dans les transparents. Grâce au PSNR nous mesurons la qualité de l'image reconstruite, une valeur de $PSNR = infini$ est trouvée avant l'insertion du tatouage, et une valeur de $PSNR = 48,83$ est trouvée après l'insertion du tatouage ce qui signifie que l'image tatouée maintient une haute qualité (tableau 6.1).

TABLE 6.1 – Les valeurs du PSNR avant et après l'insertion du tatouage

PSNR avant l'insertion de tatouage	PSNR après l'insertion du tatouage
infini	48,83

6.3.3 Propriété de fragilité

Afin de vérifier si notre méthode a la possibilité de détecter toute anomalie, nous supposons que les transparents sont envoyés sur un canal de transmission, cependant ce dernier peut être bruyant. Pour cela nous simulons un bruit gaussien sur ces transparents. Nous faisons extraire les matrices de reste de division de chaque transparent pour détecter si une erreur a eu lieu.La figure 6.3 montre la matrice de reste de division avant l'application du bruit gaussien. Elle est noire ce qui interprète que les transparents n'ont pas subi une attaque, tandis que la figure 6.4, présente la matrice de reste de division après l'application de bruit gaussien sur les transparents ; Elle n'est plus noire ce qui signifie que la méthode proposée résiste bien aux bruits gaussiens.

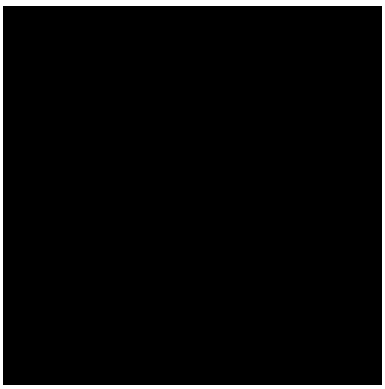


FIGURE 6.3 – Image des restes de division extraite d'un transparent avant l'application du bruit gaussien .

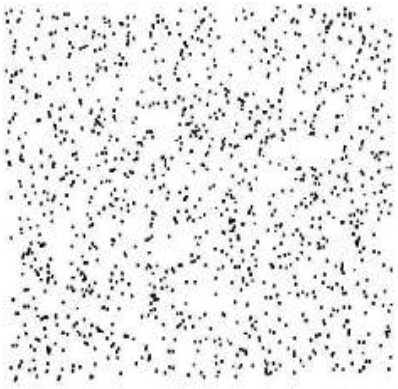


FIGURE 6.4 – Image des reste de division extraite d'un transparent aprés l'application du bruit gaussien.

Le PSNR des transparents tatoués avant et après l'application du bruit gaussien

Grâce au PSNR, nous mesurons la qualité du secret reconstruit après l'application d'un bruit gaussien et avant d'utiliser le décodage par BCH, puis nous mesurons la qualité de l'image secrète reconstruite après avoir utilisé le code BCH(16,11) pour la correction d'erreurs. La table 6.2 donne les valeurs de PSNR avant et après l'application du BCH raccourci (16,11). Nous voyons que l'image secrète reconstruite à partir des transparents attaqués a une valeur $PSNR$=26,36, cependant le $PSNR$ de l'image secrète reconstruite à partir des transparents attaqués après l'utilisation du code correcteur BCH (16,11) est de 39,23, en utilisant ce code BCH (16,11) nous pourrions corriger 5 erreurs sur chaque deux bits de chaque share.

TABLE 6.2 – Les valeurs du PSNR avant et apres l'application du code BCH

La valeur du PSNR après l'attaque, avant le décodage	Valeur du PSNR après le décodage
26,36	39,23

6.3.4 La possibilité de correction après la détection

Un tatouage fragile est connu par la détection des informations modifies. Dans notre cas nous ne contentons pas seulement de détecter les altérations, mais aussi on les corrige grâce au code correcteur BCH.

6.3.5 Résumé de l'approche proposée

Les étapes nécessaires pour la méthode proposée sont résumées comme suit :

— Génération du tatouage fragile à l'aide du code BCH (16,11) à partir des transparents générés par la méthode de Wang et al.
— Cinq bits de contrôle sont obtenus grâce au code BCH (16,11) qui sont considérés comme le tatouage.
— Application du tatouage sur les bits LSB de chaque transparent en insérant les trois premiers bits de contrôle sur les LSB du premier pixel et les deux derniers dans le pixel adjacent.
— Simulation d'un bruit gaussien sur les transparents tatoués.
— Dix erreurs peuvent être détectées et cinq erreurs peuvent être corriges pour tous dix pixels de chaque transparent (tableau 6.3).
— Une valeur de $PSNR$=26,36 trouvée avant la correction des erreurs. Cependant après avoir corrigé cinq erreurs dans chaque dix pixels, la valeur du PSNR s'est améliorée à 39,23.

TABLE 6.3 – Le nombre des erreurs détectables et corrigeables par le BCH(16,11)

Capacité de détection d'erreurs dans chaque 10 pixels	Capacité de correction d'erreurs dans chaque 10 pixels
10	5

FIGURE 6.5 – L'image secrète a partager en utilisant la méthode (n, n) de wang et al.

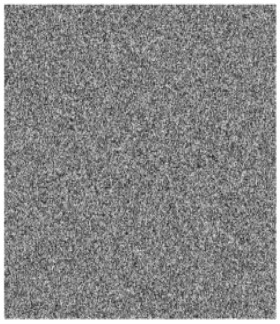


FIGURE 6.6 – Application du bruit gaussien sur le premier share aléatoire généré en utilisant le schéma de wang et al.

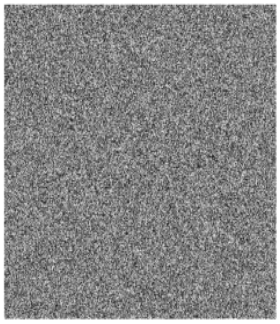


FIGURE 6.7 – Application du bruit gaussien sur le deuxième share aléatoire généré en utilisant le schéma de Wang et al.

FIGURE 6.8 – Image secrète reconstruite à partir des shares attaqués $PSNR$=26,36

FIGURE 6.9 – Image secrète reconstruite à partir des shares attaqués après l'application du code BCH(16,11) avec un $PSNR$=39,23

6.4 Conclusion

Dans cette partie du chapitre, nous avons appliqué un tatouage fragile en améliorant la sécurité de l'une des méthodes les plus citée qui surmonte un problème principal dans la cryptographie visuelle qui est l'expansion des pixels. Le tatouage est inséré sur leurs transparents pour vérifier leur intégrité et corriger les erreurs potentielles en utilisant un code correcteur BCH raccourci de longueur (16,11), réduit d'un code BCH de longueur (31,26). Nos résultats expérimentaux montrent que le BCH choisi peut corriger jusqu'à 5 erreurs et détecter 10 erreurs pour chaque chaque dix pixels (Deux erreurs sont détectées et une seule erreur est corrigée pour chaque deux pixels). Le $PSNR$ de l'image secrète reconstruite à partir des shares tatoués donne de bonnes valeurs après avoir utilisé le code BCH (16,11). Notre méthode est efficace en termes d'imperceptibilité et de fragilité.

Conclusion générale

À travers cette thèse nous avons évoqué deux axes de recherche intéressants dans le domaine de la cryptographie, l'un dans la discipline de la cryptographie visuelle et l'autre dans le tatouage numérique. Bien que les approches de la cryptographie visuelle aient démontré leurs faisabilités, elles ont connu plusieurs inconvénients qui rendent leurs applications moins pratiques et ne répondant pas aux exigences actuelles de l'utilisateur. En effet ; le plus grand défi étant alors de créer un schéma de partage de secret qui a les paramètres suivants :

— Un schéma avec un minimum nombre de pixels codés de l'image secrète.
— Un schéma compatible avec tous types d'images existant binaire, niveau de gris, en couleur, demi-ton...etc.
— Un schéma avec une qualité parfaite de l'image secrète reconstruite à partir de tout les transparents.
— Un schéma de partage de secret qui peut être applicable avec n'importe quel nombre de participants ($n \geq 2$).
— Un schéma de partage de secret dont lequel les détails du secret peuvent se reconstruire progressivement à chaque fois le nombre de participants s'accroît.

Notre première contribution dans la cryptographie visuelle propose un schéma de partage de secret qui a l'avantage d'avoir toutes ces caractéristiques citées ci-dessus. Il combine le modèle de partage de secret sans expansion des pixels avec le modèle progressif des schémas de la cryptographie visuelle pour obtenir un schéma de partage de secret progressif pour $n \geq 2$ nombre de participants en utilisant des simples opérations Booléennes.

Nos résultats expérimentaux indiquent l'efficacité et la faisabilité du schéma suggèré et montrent la haute qualité de l'image reconstruite et la compatibilité de notre méthode avec tous types d'images et avec n'importe quel nombre de coopérants souhaités. Notre deuxième contribution consiste en un tatouage fragile inséré dans le domaine spatial pour renforcer la sécurité du schéma de partage de secret de Wang et al. en intégrant une marque aux pixels de plus faible poids à l'aide d'un code correcteur BCH qui est considéré comme l'un des codes les plus efficaces en matière de nombre de détection et correction d'erreurs afin de détecter toutes modifications malhonnêtes des transparents codés et donc éviter la distorsion de l'image révélée. La souplesse des codes BCH a permis de réduire leur taille pour qu'elle soit compatible avec la longueur paire des pixels.

Dans nos prochains travaux de recherche nous comptons améliorer l'aspect progressif de notre schéma de partage de secret proposé et définir nos propres régions

secrètes au lieu de les définir aléatoirement et analyser aussi son aspect de sécurité en étudiant les différentes attaques qui peuvent survenir à un schéma de partage de secret. Nous envisageons aussi d'intégrer cette approche dans des applications réelles comme par exemple pour renforcer la sécurité du réseau sans fil 802.11 i, ou d'introduire notre schéma dans des applications médicales. Concernant la cryptographie visuelle audio nous projetons de créer notre propre schéma tout en respectant les paramètres essentiels d'un schéma de partage de secret. Comme perspectives, nous comptons développer notre propre méthode de tatouage et de l'intégrer au schéma de partage de secret pour renforcer sa sécurité.

Bibliographie

[1] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[2] Gilbert S Vernam. Cipher printing telegraph systems : For secret wire and radio telegraphic communications. *AIEE, Journal of the*, 45(2) :109–115, 1926.

[3] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2) :120–126, 1978.

[4] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4) :469–472, 1985.

[5] Dan Boneh. The decision diffie-hellman problem. In *International Algorithmic Number Theory Symposium*, pages 48–63. Springer, 1998.

[6] Don Coppersmith. The data encryption standard (des) and its strength against attacks. *IBM journal of research and development*, 38(3) :243–250, 1994.

[7] Vincent Rijmen and Joan Daemen. Advanced encryption standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, pages 19–22, 2001.

[8] Moni Naor and Adi Shamir. Visual cryptography. In *Advances in Cryptology—EUROCRYPT'94*, pages 1–12. Springer, 1995.

[9] Ingemar J Cox, Joe Kilian, F Thomson Leighton, and Talal Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing*, 6(12) :1673–1687, 1997.

[10] Daoshun Wang, Lei Zhang, Ning Ma, and Xiaobo Li. Two secret sharing schemes based on boolean operations. *Pattern Recognition*, 40(10) :2776–2785, 2007.

[11] Zhi Zhou, Gonzalo R Arce, and Giovanni Di Crescenzo. Halftone visual cryptography. *IEEE transactions on image processing*, 15(8) :2441–2453, 2006.

[12] Feng Liu and Chuankun Wu. Embedded extended visual cryptography schemes. *IEEE transactions on information forensics and security*, 6(2) :307–322, 2011.

[13] Tzung-Her Chen and Chang-Sian Wu. Efficient multi-secret image sharing based on boolean operations. *Signal Processing*, 91(1) :90–97, 2011.

[14] Young-Chang Hou. Visual cryptography for color images. *Pattern recognition*, 36(7) :1619–1629, 2003.

[15] Duo Jin, Wei-Qi Yan, and Mohan S Kankanhalli. Progressive color visual cryptography. *Journal of Electronic Imaging*, 14(3) :033019–033019, 2005.

[16] Guan-Shi Zhong and Jian-Jun Wang. Region incrementing visual secret sharing scheme based on random grids. *Circuits and Systems*, (3) :2351–2354, 2013.

[17] Young-Chang Hou, Zen-Yu Quan, Chih-Fong Tsai, and A-Yu Tseng. Block-based progressive visual secret sharing. *Information Sciences*, 233 :290–304, 2013.

[18] Ran-Zan Wang and Shyong-Jian Shyu. Scalable secret image sharing. *Signal Processing : Image Communication*, 22(4) :363–373, 2007.

[19] Claude Berrou. *Codes and turbo codes*. Springer, 2010.

[20] Elwyn R Berlekamp. Algebraic coding theory. 1968.

[21] Internet live stas. `http://www.internetlivestats.com/internet-users/`. Accessed : 2017-04-10.

[22] Symantec. `https://www.symantec.com/`. Accessed : 2018-02-27.

[23] Duo Jin, Weiqi Yan, and Mohan S Kankanhalli. Progressive color visual cryptography. *Journal of Electronic Imaging*, 14(3) :033019, 2005.

[24] W-P Fang and J-C Lin. Progressive viewing and sharing of sensitive images. *Pattern recognition and Image analysis*, 16(4) :632–636, 2006.

[25] Pim Tuyls, Henk DL Hollmann, Jack H Van Lint, and LMGM Tolhuizen. Xor-based visual cryptography schemes. *Designs, Codes and Cryptography*, 37(1) :169–186, 2005.

[26] Wen-Pinn Fang. Friendly progressive visual secret sharing. *Pattern Recognition*, 41(4) :1410–1414, 2008.

[27] Nicholas J Daras and Michael Th Rassias. *Computation, cryptography, and network security*. Springer, 2015.

[28] Monisha Sharma and Manoj Kumar Kowar. Image encryption techniques using chaotic schemes : a review. 2010.

[29] Thomas Kelly. The myth of the skytale. *Cryptologia*, 22(3) :244–260, 1998.

[30] Introduction à la cryptographie. `http://www.ensiwiki.ensimag.fr/images/d/d1/5MMSSI-2011-2012.3-1.cryptography-introduction.pdf`. PublisherIn ENSIMAG, Author : GrenobleHossen, Karim and Duchene, Fabien. Accessed : 2018-02-10.

[31] HX Mel, Doris M Baker, and Steve Burnett. *Cryptography decrypted*. Addison-Wesley Upper Saddle River, 2001.

[32] Claude E Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1) :3–55, 2001.

[33] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6) :644–654, 1976.

[34] Charles H Bennett and Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *Theoretical computer science*, 560 :7–11, 2014.

[35] Aurélien Géron. *WIFI professionnelle*. DUNOD, 2009.

[36] Cédric Llorens, Laurent Levier, Denis Valois, and Benjamin Morin. *Tableaux de bord de la sécurité réseau*. Editions Eyrolles, 2011.

[37] David Kahn. *The Codebreakers : The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster, 1996.

[38] Michael O Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical report, MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE, 1979.

[39] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244 :114–116, 1978.

[40] Stefan Katzenbeisser and Fabien Petitcolas. *Information hiding techniques for steganography and digital watermarking*. Artech house, 2000.

[41] Juergen Seitz. *Digital watermarking for digital media*. IGI Global, 2005.

[42] Eiji Kawaguchi Hannu Jaakkola, Hannu Kangassalo. *Information Modelling and Knowledge Bases X*. IOS Press, 1999.

[43] Frank Y Shih. *Digital watermarking and steganography : fundamentals and techniques*. CRC press, 2017.

[44] Man Young Rhee. *Cryptography and secure communications*. McGraw-Hill, Inc., 1993.

[45] Simon Singh. *The code book : the evolution of secrecy from Mary, Queen of Scots, to quantum cryptography*. Doubleday, 1999.

[46] Ljupco Kocarev. Chaos-based cryptography : a brief overview. *IEEE Circuits and Systems Magazine*, 1(3) :6–21, 2001.

[47] Darrel Hankerson, Alfred J Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[48] Yvo Desmedt, Shuang Hou, and Jean Quisquater. Audio and optical cryptography. In *Advances in Cryptology—ASIACRYPT'98*, pages 392–404. Springer, 1998.

[49] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11) :612–613, 1979.

[50] GR Blakly. Safeguarding cryptographic keys proceedings of the national computer conference, 1979.

[51] Ming Sun Fu and Oscar C Au. Joint visual cryptography and watermarking. In *Multimedia and Expo, 2004. ICME'04. 2004 IEEE International Conference on*, volume 2, pages 975–978. IEEE, 2004.

[52] Moni Naor and Benny Pinkas. Visual authentication and identification. In *Advances in Cryptology-CRYPTO'97 : 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1997. Proceedings*, page 322. Springer, 1997.

[53] Moni Naor and Benny Pinkas. Visual authentication and identification. In *Advances in Cryptology-CRYPTO'97 : 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1997. Proceedings*, page 322. Springer, 1997.

[54] David Chaum. Secret-ballot receipts : True voter-verifiable elections. *IEEE security & privacy*, 2(1) :38–47, 2004.

[55] Amir Houmansadr and Shahrokh Ghaemmaghami. A novel video watermarking method using visual cryptography. In *Engineering of Intelligent Systems, 2006 IEEE International Conference on*, pages 1–5. IEEE, 2006.

[56] Feng Liu and Wei Qi Yan. *Visual Cryptography for Image Processing and Security*, volume 2. Springer, 2014.

[57] Mausumi Bose and Rahul Mukerjee. Optimal (k, n) visual cryptographic schemes for general k. *Designs, Codes and Cryptography*, 55(1) :19–35, 2010.

[58] Eli Biham and Ayal Itzkovitz. Visual cryptography with polarization. 1998.

[59] Jonathan Weir and WeiQi Yan. Resolution variant visual cryptography for street view of google maps. In *Circuits and Systems (ISCAS), Proceedings of 2010 IEEE International Symposium on*, pages 1695–1698. IEEE, 2010.

[60] Stelvio Cimato and Ching-Nung Yang. *Visual cryptography and secret image sharing*. CRC press, 2011.

[61] Gwoboa Horng, Tzungher Chen, and Du-Shiau Tsai. Cheating in visual cryptography. *Designs, Codes and Cryptography*, 38(2) :219–236, 2006.

[62] John R Jensen and Kalmesh Lulla. Introductory digital image processing : a remote sensing perspective. 1987.

[63] Andrew B Watson and Cynthia H Null. Digital images and human vision. 1997.

[64] Mark S Nixon and Alberto S Aguado. *Feature extraction & image processing for computer vision*. Academic Press, 2012.

[65] Ching-Nung Yang. New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4) :481–494, 2004.

[66] Mustafa Ulutas, Vasif V Nabiyev, and Guzin Ulutas. A pvss scheme based on boolean operations with improved contrast. In *Network and Service Security, 2009. N2S'09. International Conference on*, pages 1–5. IEEE, 2009.

[67] Stelvio Cimato, Roberto De Prisco, and Alfredo De Santis. Probabilistic visual cryptography schemes. *The Computer Journal*, 49(1) :97–107, 2006.

[68] Daoshun Wang, Feng Yi, and Xiaobo Li. Probabilistic visual secret sharing schemes for grey-scale images and color images. *Information Sciences*, 181(11) :2189–2208, 2011.

[69] Ching-Nung Yang. New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4) :481–494, 2004.

[70] Oded Kafri and Eliezer Keren. Encryption of pictures and shapes by random grids. *Optics letters*, 12(6) :377–379, 1987.

[71] Shyong Jian Shyu. Image encryption by random grids. *Pattern Recognition*, 40(3) :1014–1031, 2007.

[72] Tzung-Her Chen and Kai-Hsiang Tsao. Visual secret sharing by random grids revisited. *Pattern Recognition*, 42(9) :2203–2217, 2009.

[73] Xiaotian Wu and Wei Sun. Random grid-based visual secret sharing with abilities of or and xor decryptions. *Journal of visual communication and image representation*, 24(1) :48–62, 2013.

[74] Xuehu Yan, Shen Wang, Ahmed A Abd El-Latif, and Xiamu Niu. Threshold visual secret sharing with comprehensive properties based on random grids. *Signal, Image and Video Processing*, 9(7) :1659–1668, 2015.

[75] Kun-Yuan Chao and Ja-Chen Lin. Secret image sharing : a boolean-operations-based approach combining benefits of polynomial-based and fast approaches. *International Journal of Pattern Recognition and Artificial Intelligence*, 23(02) :263–285, 2009.

[76] Lin Dong, Daoshun Wang, Min Ku, and Yiqi Dai. (2, n) secret image sharing scheme with ideal contrast. In *Computational Intelligence and Security (CIS), 2010 International Conference on*, pages 421–424. IEEE, 2010.

[77] Tapasi Bhattacharjee, Jyoti Prakash Singh, and Amitava Nag. A novel (2, n) secret image sharing scheme. *Procedia Technology*, 4 :619–623, 2012.

[78] Mizuko Nakajima and Yasushi Yamaguchi. Extended visual cryptography for natural images. J.WSCG 10(2) :303–310, 2002.

[79] LRW FLOYD. An adaptive algorithm for spatial greyscale. In *Proc. of the SID*, volume 17, pages 75–77, 1976.

[80] Bryce E Bayer. An optimum method for two-level rendition of continuous-tone pictures. In *IEEE Int. Conf. on Communications*, volume 26, pages 11–15, 1973.

[81] Chang-Chou Lin and Wen-Hsiang Tsai. Visual cryptography for gray-level images by dithering techniques. *Pattern Recognition Letters*, 24(1) :349–358, 2003.

[82] Nitty Sarah Alex and L Jani Anbarasi. Enhanced image secret sharing via error diffusion in halftone visual cryptography. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, volume 2, pages 393–397. IEEE, 2011.

[83] Zhongmin Wang, Gonzalo R Arce, and Giovanni Di Crescenzo. Halftone visual cryptography via error diffusion. *IEEE transactions on information forensics and security*, 4(3) :383–396, 2009.

[84] Yuk-Hee Chan and Sin-Ming Cheung. Feature-preserving multiscale error diffusion for digital halftoning. *Journal of Electronic Imaging*, 13(3) :639–645, 2004.

[85] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R Stinson. Visual cryptography for general access structures. *Information and Computation*, 129(2) :86–106, 1996.

[86] Kai-Hui Lee and Pei-Ling Chiu. An extended visual cryptography algorithm for general access structures. *ieee transactions on information forensics and security*, 7(1) :219–229, 2012.

[87] InKoo Kang, Gonzalo R Arce, and Heung-Kyu Lee. Color extended visual cryptography using error diffusion. *IEEE Transactions on image processing*, 20(1) :132–145, 2011.

[88] Rastislav Lukac and Konstantinos N Plataniotis. Bit-level based secret sharing for image encryption. *Pattern recognition*, 38(5) :767–772, 2005.

[89] Chiang-Lung Liu, Kai-Ping Wang, and Der-Chyuan Lou. Pixel expansion-free grey-scale image sharing method. *The Imaging Science Journal*, 61(5) :403–407, 2013.

[90] Tzung-Her Chen, Kai-Hsiang Tsao, and Chang-Sian Wu. Multi-secrets visual secret sharing. In *Communications, 2008. APCC 2008. 14th Asia-Pacific Conference on*, pages 1–5. IEEE, 2008.

[91] Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang, and Yen-Ping Chu. Visual secret sharing for multiple secrets. *Pattern Recognition*, 41(12) :3572–3581, 2008.

[92] Chien-Chang Chen and Wei-Jie Wu. A secure boolean-based multi-secret image sharing scheme. *Journal of Systems and Software*, 92 :107–114, 2014.

[93] Stefan Droste. New results on visual cryptography. In *Crypto*, volume 96, pages 401–415. Springer, 1996.

[94] Stelvio Cimato, Roberto De Prisco, and Alfredo De Santis. Colored visual cryptography without color darkening. In *SCN*, volume 3352, pages 235–248. Springer, 2004.

[95] Tu SF Hou YC, Chang CY. Visual cryptography for color images based on halftone technology. *Proc. of SCI2001*, 13 :441–445, 2001.

[96] YC Hou and CF Tu. Visual cryptography techniques for color images without pixel expansion. *journal of information, technology and society*, 1 :95–110, 2004.

[97] Carlo Blundo, Alfredo De Santis, and Douglas R Stinson. On the contrast in visual cryptography schemes. *Journal of Cryptology*, 12(4) :261–289, 1999.

[98] Matthias Krause and Hans Ulrich Simon. Determining the optimal contrast for secret sharing schemes in visual cryptography. In *LATIN*, pages 280–291. Springer, 2000.

[99] Shyong Jian Shyu, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang, and Kun Chen. Sharing multiple secrets in visual cryptography. *Pattern Recognition*, 40(12) :3633–3651, 2007.

[100] Ran-Zan Wang. Region incrementing visual cryptography. *Signal Processing Letters, IEEE*, 16(8) :659–662, 2009.

[101] W-P Fang and J-C Lin. Progressive viewing and sharing of sensitive images. *Pattern Recognition and Image Analysis*, 16(4) :632–636, 2006.

[102] Young-Chang Hou and Zen-Yu Quan. Progressive visual cryptography with unexpanded shares. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(11) :1760–1764, 2011.

[103] W-P Fang and J-C Lin. Progressive viewing and sharing of sensitive images. *Pattern recognition and Image analysis*, 16(4) :632–636, 2006.

[104] Ankit Gupta and Kshitiz Saxena. Region incrementing visual cryptography. In *Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014 International Conference on*, pages 247–250. IEEE, 2014.

[105] Ching-Nung Yang, Hsiang-Wen Shih, Chih-Cheng Wu, and Lein Harn. *k* out of *n* region incrementing scheme in visual cryptography. *IEEE Transactions on Circuits and Systems for Video Technology*, 22(5) :799–810, 2012.

[106] Ching-Nung Yang, Hsiang-Wen Shih, Yu-Ying Chu, and Lein Harn. New region incrementing visual cryptography scheme. In *The 2011 International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV 2011) in conjunction with WORLDCOMP*, pages 323–329, 2011.

[107] Sujit Kumar Das and Bibhas Chandra Dhara. An image secret sharing technique with block based image coding. In *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*, pages 648–652. IEEE, 2015.

[108] Ran-Zan Wang, Yin-Fang Chien, and Yung-Yi Lin. Scalable user-friendly image sharing. *Journal of Visual Communication and Image Representation*, 21(7) :751–761, 2010.

[109] Ching-Nung Yang and Yu-Ying Chu. A general (k, n) scalable secret image sharing scheme with the smooth scalability. *Journal of Systems and Software*, 84(10) :1726–1733, 2011.

[110] Yung-Yi Lin and Ran-Zan Wang. Scalable secret image sharing with smaller shadow images. *IEEE Signal Processing Letters*, 17(3) :316–319, 2010.

[111] Tzung-Her Chen and Kai-Hsiang Tsao. User-friendly random-grid-based visual secret sharing. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(11) :1693–1703, 2011.

[112] Chih-Ching Thien and Ja-Chen Lin. An image-sharing method with user-friendly shadow images. *IEEE Transactions on circuits and systems for video technology*, 13(12) :1161–1169, 2003.

[113] Tzung-Her Chen and Yao-Sheng Lee. Yet another friendly progressive visual secret sharing scheme. In *Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on*, pages 353–356. IEEE, 2009.

[114] Tapasi Bhattacharjee, Ranjeet Kumar Rout, and Santi P Maity. Affine boolean classification in secret image sharing for progressive quality access control. *Journal of Information Security and Applications*, 33 :16–29, 2017.

[115] Christian Rey and Jean-Luc Dugelay. A survey of watermarking algorithms for image authentication. *EURASIP Journal on Advances in Signal Processing*, 2002(6) :218932, 2002.

[116] Christian Rey and Jean-Luc Dugelay. A survey of watermarking algorithms for image authentication. *EURASIP Journal on Advances in Signal Processing*, 2002(6) :218932, 2002.

[117] Kiyoshi Tanaka, Yasuhiro Nakamura, and Kineo Matsui. Embedding secret information into a dithered multi-level image. In *Military Communications Conference, 1990. MILCOM'90, Conference Record, A New Era. 1990 IEEE*, pages 216–220. IEEE, 1990.

[118] Ron G Van Schyndel, Andrew Z Tirkel, and Charles F Osborne. A digital watermark. In *Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference*, volume 2, pages 86–90. IEEE, 1994.

[119] http ://www.watermarkingworld.com/digital _watermarking. Accessed : 2018-01-15.

[120] Yongjian Hu, Sam Kwong, and Jiwu Huang. Using invisible watermarks to protect visibly watermarked images. In *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, volume 5, pages V–V. IEEE, 2004.

[121] Gordon W Braudaway. Protecting publicly-available images with an invisible image watermark. In *Image Processing, 1997. Proceedings., International Conference on*, volume 1, pages 524–527. IEEE, 1997.

[122] Wenjun Zeng and Bede Liu. On resolving rightful ownerships of digital images by invisible watermarks. In *Image Processing, 1997. Proceedings., International Conference on*, volume 1, pages 552–555. IEEE, 1997.

[123] Mohan S Kankanhalli, KR Ramakrishnan, et al. Adaptive visible watermarking of images. In *Multimedia Computing and Systems, 1999. IEEE International Conference on*, volume 1, pages 568–573. IEEE, 1999.

[124] Yongjian Hu and Byeungwoo Jeon. Reversible visible watermarking and lossless recovery of original images. *IEEE Transactions on Circuits and Systems for Video Technology*, 16(11) :1423–1429, 2006.

[125] Salwa AK Mostafa, Naser El-Sheimy, AS Tolba, FM Abdelkader, and Hisham M Elhindy. Wavelet packets-based blind watermarking for medical image management. *The open biomedical engineering journal*, 4 :93, 2010.

[126] Hemin Golpira and Habibollah Danyali. Reversible blind watermarking for medical images based on wavelet histogram shifting. In *Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on*, pages 31–36. IEEE, 2009.

[127] Jieh-Ming Shieh, Der-Chyuan Lou, and Ming-Chang Chang. A semi-blind digital watermarking scheme based on singular value decomposition. *Computer Standards & Interfaces*, 28(4) :428–440, 2006.

[128] Mitsuo Okada, Yasuo Okabe, and Tetsutaro Uehara. A web-based privacy-secure content trading system for small content providers using semi-blind digital watermarking. In *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*, pages 1–2. IEEE, 2010.

[129] Nagaraj V Dharwadkar, BB Amberker, and Avijeet Gorai. Non-blind watermarking scheme for color images in rgb space using dwt-svd. In *Communications and Signal Processing (ICCSP), 2011 International Conference on*, pages 489–493. IEEE, 2011.

[130] Nagaraj V Dharwadkar, BB Amberker, and Avijeet Gorai. Non-blind watermarking scheme for color images in rgb space using dwt-svd. In *Communications and Signal Processing (ICCSP), 2011 International Conference on*, pages 489–493. IEEE, 2011.

[131] Fred Mintzer, Gordon W Braudaway, and Minerva M Yeung. Effective and ineffective digital watermarks. In *Image Processing, 1997. Proceedings., International Conference on*, volume 3, pages 9–12. IEEE, 1997.

[132] Jiri Fridrich, Miroslav Goljan, and Arnold C Baldoza. New fragile authentication watermark for images. In *Image Processing, 2000. Proceedings. 2000 International Conference on*, volume 1, pages 446–449. IEEE, 2000.

[133] Raymond B Wolfgang and Edward J Delp. Fragile watermarking using the vw2d watermark. In *Security and Watermarking of Multimedia Contents*, volume 3657, pages 204–214. International Society for Optics and Photonics, 1999.

[134] Gaurav Aggarwal, Pradeep K Dubey, Ashutosh Kulshreshtha, Marco Martens, Charles P Tresser, and Chai W Wu. Semi-fragile watermarks, December 21 2004. US Patent 6,834,344.

[135] Radu O Preda. Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. *Measurement*, 46(1) :367–373, 2013.

[136] Jiang-Lung Liu, Der-Chyuan Lou, Ming-Chang Chang, and Hao-Kuan Tso. A robust watermarking scheme using self-reference image. *Computer Standards & Interfaces*, 28(3) :356–367, 2006.

[137] AV Subramanyam, Sabu Emmanuel, and Mohan S Kankanhalli. Robust watermarking of compressed and encrypted jpeg2000 images. *IEEE Transactions on Multimedia*, 14(3) :703–716, 2012.

[138] Santi P Maity and Malay Kumar Kundu. Robust and blind spatial watermarking in digital image. In *ICVGIP*, 2002.

[139] Ibrahim Nasir, Ying Weng, and Jianmin Jiang. Novel multiple spatial watermarking technique in color images. In *Information Technology : New Generations, 2008. ITNG 2008. Fifth International Conference on*, pages 777–782. IEEE, 2008.

[140] Eckard Koch, Jochen Rindfrey, and Jian Zhao. Copyright protection for multimedia data. In *Proc. of the Int. Conf. on Digital Media and Electronic Publishing*, volume 32, 1994.

[141] Deepa Kundur and Dimitrios Hatzinakos. A robust digital image watermarking method using wavelet-based fusion. In *Image Processing, 1997. Proceedings., International Conference on*, volume 1, pages 544–547. IEEE, 1997.

[142] Vidyasagar M Potdar, Song Han, and Elizabeth Chang. A survey of digital image watermarking techniques. In *Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on*, pages 709–716. IEEE, 2005.

[143] Shinfeng D Lin and Chin-Feng Chen. A robust dct-based watermarking for copyright protection. *IEEE Transactions on Consumer Electronics*, 46(3) :415–421, 2000.

[144] Ryutarou Ohbuchi, Akio Mukaiyama, and Shigeo Takahashi. A frequency-domain approach to watermarking 3d shapes. In *Computer Graphics Forum*, volume 21, pages 373–382. Wiley-Blackwell, 2002.

[145] Jack T Brassil, Steven Low, Nicholas F. Maxemchuk, and Lawrence O'Gorman. Electronic marking and identification techniques to discourage document copying. *IEEE Journal on Selected Areas in Communications*, 13(8) :1495–1504, 1995.

[146] Joseph JK O'Ruanaidh, WJ Dowling, and FM Boland. Watermarking digital images for copyright protection. *IEE Proceedings-Vision, Image and Signal Processing*, 143(4) :250–256, 1996.

[147] Frank Hartung and Bernd Girod. Digital watermarking of raw and compressed video. In *Proc. European EOS/SPIE Symposium on Advanced Imaging and Network Technologies*, volume 2952, pages 205–213, 1996.

[148] Laurence Boney, Ahmed H Tewfik, and Khaled N Hamdy. Digital watermarks for audio signals. In *Multimedia Computing and Systems, 1996., Proceedings of the Third IEEE International Conference on*, pages 473–480. IEEE, 1996.

[149] Ingemar Cox, Jeffrey Bloom, and Matthew Miller. Digital watermarking : Principles & practice, 2001.

[150] Nagaraj V Dharwadkar and BB Amberker. Secure watermarking scheme for color image using intensity of pixel and lsb substitution. *arXiv preprint arXiv :0912.3923*, 2009.

[151] Brian Chen and Gregory W Wornell. Quantization index modulation : A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 47(4) :1423–1443, 2001.

[152] Nour El-Houda Golea. A fragile watermarking scheme based crc checksum and public key cryptosystem for rgb color image authentication. In *International Conference on Image and Signal Processing*, pages 316–325. Springer, 2012.

[153] Jiri Fridrich. Protection of digital images using self embedding. In *Symposium on Content Security and Data Hiding in Digital Media, May 1999*. New Jersey Institute of Technology, 1999.

[154] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul Mc Kevitt. Digital image steganography : Survey and analysis of current methods. *Signal processing*, 90(3) :727–752, 2010.

[155] Ali Jabeur Bouzidi. *Développement de techniques de marquage d'authentification pour la protection de données multimédias*. PhD thesis, Université du Québec en Outaouais, 2009.

[156] Franco Bartolini, Anastasios Tefas, Mauro Barni, and Ioannis Pitas. Image authentication techniques for surveillance applications. *Proceedings of the IEEE*, 89(10) :1403–1418, 2001.

[157] George Voyatzis, Nikolaos Nikolaidis, and Ioannis Pitas. Digital watermarking : an overview. In *Signal Processing Conference (EUSIPCO 1998), 9th European*, pages 1–4. IEEE, 1998.

[158] Christian Rey and Jean-Luc Dugelay. A survey of watermarking algorithms for image authentication. *EURASIP Journal on Advances in Signal Processing*, 2002(6) :218932, 2002.

[159] Claude Elwood Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1) :3–55, 2001.

[160] Eric Y Sheu and Oliver C Mullins. *Fundamentals and Applications*. Springer, 1995.

[161] James Massey. Step-by-step decoding of the bose-chaudhuri-hocquenghem codes. *IEEE Transactions on Information Theory*, 11(4) :580–585, 1965.

[162] Stephen B Wicker and Vijay K Bhargava. *Reed-Solomon codes and their applications*. John Wiley & Sons, 1999.

[163] Rino Micheloni, Alessia Marelli, and Roberto Ravasio. *Error correction codes for non-volatile memories*. Springer Science & Business Media, 2008.

[164] W Peterson. Encoding and error-correction procedures for the bose-chaudhuri codes. *IRE Transactions on Information Theory*, 6(4) :459–470, 1960.

[165] Fabrice Monteiro, Abbas Dandache, Amine M'sir, and Bernard Lepley. A fast crc implementation on fpga using a pipelined architecture for the polynomial division. In *Electronics, Circuits and Systems, 2001. ICECS 2001. The 8th IEEE International Conference on*, volume 3, pages 1231–1234. IEEE, 2001.

[166] W-P Fang and J-C Lin. Progressive viewing and sharing of sensitive images. *Pattern Recognition and Image Analysis*, 16(4) :632–636, 2006.

[167] Tapasi Bhattacharjee, Jyoti Prakash Singh, and Amitava Nag. A novel (2, n) secret image sharing scheme. *Procedia Technology*, 4 :619–623, 2012.

[168] Xuehu Yan, Shen Wang, and Xiamu Niu. Threshold construction from specific cases in visual cryptography without the pixel expansion. *Signal Processing*, 105 :389–398, 2014.

[169] Chen-Chi Lin, Chi-Sung Laih, Ching-Nung Yang, et al. New audio secret sharing schemes with time division technique. *J. Inf. Sci. Eng.*, 19(4) :605–614, 2003.

[170] Mohammad Ehdaie, Taraneh Eghlidos, and Mohammad Reza Aref. A novel secret sharing scheme from audio perspective. In *Telecommunications, 2008. IST 2008. International Symposium on*, pages 13–18. IEEE, 2008.

[171] T. Chavan V. Shastri. S. Pati, P. R. Deshmukh. Reduced size share audio secret sharing. International Conference on Pervasive Computing (ICPC), 2015.

[172] Kotaro Yoshida and Yodai Watanabe. Security of audio secret sharing scheme encrypting audio secrets. In *Internet Technology And Secured Transactions, 2012 International Conference for*, pages 294–295. IEEE, 2012.

[173] M Abukari Yakubu, Namunu C Maddage, and Pradeep K Atrey. Audio secret management scheme using shamir's secret sharing. In *International Conference on Multimedia Modeling*, pages 396–407. Springer, 2015.