Chapitre 3

Sécurisation d'images

Sommaire :

2. Protection des images numériques……..……29
3. Cryptosystème hybride ……...……32
4. Cryptosystème hybride pour sécuriser image numérique……..33
4.1. La méthode de chiffrement et déchiffrement d'image……34
4.2. Chiffrement de clé ……..36

1. Introduction

De nos jours, de plus en plus d'images numériques sont transférées sur les réseaux informatiques. Il se pose donc un réel problème quant à la sécurité d'une image lors de la transmission, les travaux présentés dans ce chapitre montrent comment des algorithmes de cryptage permettent la sécurisation des images.

Pour ce faire, les images peuvent être cryptées au niveau des codages source afin de faire remonter cette fonctionnalité au niveau des couches hautes (applications), **[27]** nous pouvons donc garantir la protection d'une image lors de la transmission, et également protéger le contenu de l'image contre la contrefaçon.

Ce chapitre présente des connaissances sur la sécurité des images. En outre, nous vous proposons l'importance de protection des images, et les domaines d'application, puis aussi nous expliquerons comment appliquons un cryptosystème hybride sur une image pour assurer la confidentialité de l'image numérique et profitante de la vitesse de chiffrement symétrique, et évaluer le niveau de sécurité par le chiffrement asymétrique.

2. Protection des images numériques

Les travaux de recherche sur la protection des images ont principalement débuté vers 1993**[28]**, et aujourd'hui plus d'une centaine d'articles sont annuellement consacrés à ce sujet, les premiers techniques, comme le contrôle d'accès (destiné à autoriser ou à refuser l'accès au document) ou la cryptographie (chiffrer ou signer le document).

2.1. Applications de sécurisation des images

L'utilisation de sécurisation d'images est nombreuse et variées, cela se reflète dans de nombreux domaines, où la nécessité de sécurisé une image numérique urgent, rappelons par exemple :

- **La sécurisation de l'image médicale** : L'évolution des techniques de traitement, de partage et de communication des images médicales et plus généralement de l'information médicale, s'accompagne d'une évolution des risques pour l'information alors sous forme numérique, l'information médicale de manière générale est composée principalement de résultats d'analyses, d'examens cliniques, d'examens par acliniques et de renseignements individuels, les possibilités d'accès distants et de communication de l'information sont améliorées mais les possibilités de fuites, de détournement et de modification de l'information sont aussi plus importantes, voire même facilitées par la mise à disposition d'outils de surveillance des réseaux et d'outils d'édition avancée de l'information comme les logiciels d'imagerie.

  Cependant, ce sont les conséquences liées à la survenance de ces risques qui introduisent le besoin de protection de l'information médicale. Ces conséquences, perceptibles, concernent un individu et en particulier sa santé partie intégrante de sa vie privée. C'est pourquoi de nombreux pays ont traduit ce besoin de manière déontologique et aussi législative en donnant des droits au patient et par conséquent en imposant aux professionnels et aux établissements de santé d'assurer la protection des données qu'ils ont en leur possession.**[27]**

- **La sécurisation des images satellitaires :** Avec la recherche et le développement à grande échelle dans les sciences spatiales, les technologies spatiales et les technologies de communication réseau, il ya une grande demande de système de sécurité de l'imagerie satellite pour fournir le stockage et la transmission de l'imagerie satellitaire sécurisé sur internet et / ou de l'environnement de réseau partagé, cela apporte de nouveaux défis pour protéger l'imagerie satellite sensible et critique de l'accès non autorisé et l'utilisation illégale afin de maintenir le processus de stockage et de transmission sécurisée et fiable, par conséquent, il est absolument nécessaire de chiffrement de l'imagerie satellitaire et l'application de décryptage de la sécurité.

Application de sécurité de l'imagerie par satellite (SISA) est une application de sécurité de l'information mis au point pour l'imagerie par satellite, L'application supporte nouvelle version modifiée et deux normes de cryptage des données les plus populaires désignées comme norme de chiffrement des données (DES) et Advanced Encryption Standard (AES). **[29]**

2.2. Travaux existants sur la sécurisation des images

Concernant le domaine de recherche de sécurisation des images, il y a plusieurs travaux de recherche, ces études ont traités l'utilisation des techniques de sécurité pour protéger les images, on présente quelques travaux:

- **Sécurisation d'image par crypto-tatouage [30]:** Cette étude présente une nouvelle méthode combinant le chiffrement et le tatouage d'images pour le transfert sécurisé. Cette méthode est basée sur la combinaison d'algorithmes de chiffrement à clefs publiques-privées et à clefs secrètes, et de tatouage. L'algorithme de chiffrement d'image utilise une clef secrète, nous chiffrons ensuite cette clef secrète avec un algorithme asymétrique. Cette clef secrète chiffrée est alors insérée par tatouage dans l'image cryptée.
- **Image basée stéganographie et la cryptographie [32]** : cette étude décrit une méthode pour intégrer ensemble de la cryptographie et la stéganographie pour traitement d'image. En particulier, il présente un système capable d'effectuer stéganographie et la cryptographie en même temps en utilisant des images comme des objets de couverture pour stéganographie et de touches pour la cryptographie, montrant tel système est un stéganographie efficacité.
- **Chiffrement d'images par DCT et chiffrement de flux [33]**: ce travail présente une nouvelle approche pour le chiffrement d'image en sélectionnant les hautes fréquences spécifiques de coefficients DCT (transformée en cosinus discrète) qui prises comme des valeurs caractéristiques, et les chiffrant et le conduit blocs cryptés sont mélangées selon une séquence de bits pseudo-aléatoire. Le cryptage sélectif est une approche récente de réduire les exigences de calcul pour les gros volumes d'images**.**
- **Une nouvelle approche pour commutative Watermarking-Encryption [34]:** cet article présente une nouvelle approche de la conception de tatouage de cryptage commutative (CWE). La procédure de chiffrement de permutation est utilisée pour chiffrer les données multimédia, ce qui laisse les statistiques globales des données multimédia stable. Par conséquent, tout

système de Watermarking non localisé qui ne dépend que des statistiques globales des données multimédia peut être combiné avec le chiffrement de permutation pour former un schéma de tatouage de cryptage commutative.

3. Cryptosystème hybride

En combinant cryptographie à clé publique et privée, il est possible de surmonter les inconvénients de chacun. Paires de clés publiques sont utilisées pour mettre en place une session sécurisée, et ensuite les données sont échangées grâce à un système à clé secrète. Cette offre à la fois la sécurité et des processus d'authentification associés aux systèmes de clés publiques et les capacités de chiffrement des données en vrac des systèmes à clé secrète.

Dans notre étude, Nous verrons comment appliquer cryptosystème hybride pour la sécurisation des images numérique, et grâce à l'utilisation des algorithmes variés comprenant les cryptosystèmes symétrique et asymétrique.

3.1. Utilisations

Il existe plusieurs systèmes de protection mélangeant les deux types de chiffrement pour en garder leurs avantages, on appelle les systèmes hybrides. L'exemple le plus probant est PGP mais on peut aussi citer GnuPG et SSL.

PGP (Pretty Good Privacy « Logiciel propriétaire de chiffrement ») et GnuPG (GNU Privacy Guard «développer par Projet GNU »), utilisent des procédés de chiffrement hybride, La clé de session est chiffrée à l'aide du chiffrement à clé publique et le message est chiffré en utilisant le chiffrement symétrique. La clé de session et le message sont combinés dans un paquet. Le destinataire utilise sa clé privée pour déchiffrer la clé de session et la clé de session est utilisée pour déchiffrer le message.

Le procédé de chiffrement hybride est un procédé très fiable. Même si un attaquant arrive à déchiffrer une clé de session d'un message, il ne pourra lire que ce message, pour lire un nouveau message il devra recommencer à déchiffrer la clé de session du nouveau message. **[35]**

4. Cryptosystème hybride pour sécuriser d'image

Cryptosystème hybride de l'image c'est une méthode combinant un algorithme de chiffrement symétrique pour l'image, et un algorithme de cryptage asymétrique pour le chiffrement de la clef secrète.

Prenons le cas d'une personne M souhaitant envoyer de manière sécurisée par réseau une image à une seconde personne S, M utilisera alors un algorithme rapide de chiffrement à clef secrète k pour crypter l'image.

Pour transférer la clef K, M devra alors crypter la clef K en utilisant un algorithme à clefs publique-privée (comme RSA par exemple), Soient pub_m et $priv_m$, les clefs publique et privée de M, et pub_s et $priv_s$, les clefs publiques et privée de S,

Dans un premier temps, M génère une clef secrète K pour cette session et chiffré l'image avec l'algorithme symétrique. Ensuite, M doit chiffrer la clef k avec l'algorithme RSA en utilisant la clef publique pub_s, de son correspondant S afin d'obtenir K'. Finalement M envoie cette image avec clé chiffré K' à S comme présenté Figure 3.1. Reçoit alors l'image, Il peut à ce moment décrypter la clef K' par utilisation de sa clef privée $priv_s$, Avec la clef obtenue K, S peut alors déchiffrer l'image et la visualiser.

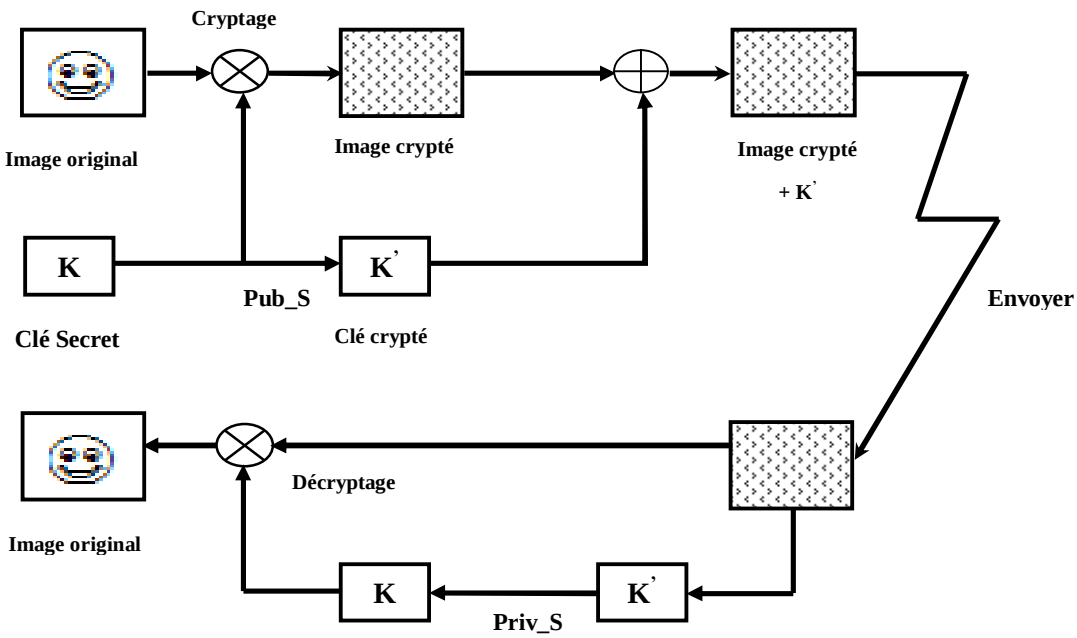

Figure 3.1 chiffrement hybride de l'image.

Si S souhaite envoyer une nouvelle image à M, il utilisera une nouvelle clef secrète K_1, pour cette nouvelle session. La méthode sera ensuite identique, mais les clefs publiques et privées ne seront pas utilisées dans le même ordre. **[30]**

4.1. La méthode de chiffrement et déchiffrement d'image

L'image est un composant multimédia détectée par l'homme, Le plus petit élément d'une image numérique est le pixel, Dans l'image numérique chaque pixel se compose de 32 bits, qui est divisé en quatre parties, à savoir alpha, rouge, vert et bleu, chacune sur 8 bits. Alpha partie représente degré de transparence, Si tous les bits de la partie Alpha sont '0', alors l'image est entièrement transparente. Ceci est représenté dans la figure suivante. **[31]**

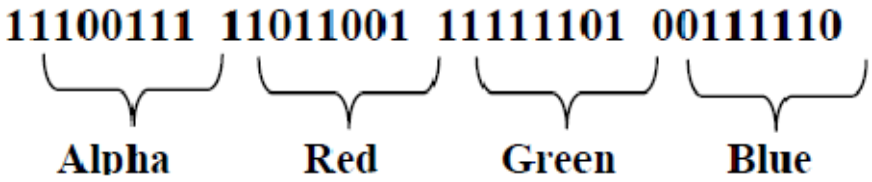

Figure 3.2 Structure d'un pixel de 32 bits. **[31]**

- **Pseudo-code de l'algorithme**

Dans cette section, nous exposons comment il est possible d'appliquer les algorithmes de chiffrement symétrique dans des images numérique. L'objectif du chiffrement d'images est d'obtenir une autre image différente à l'image originale pour les valeurs de pixels :(Voir **Figure 3.3**).

On présente maintenant les différentes étapes de l'algorithme :

- **Entrées :**
  - f : Image hôte (une image de taille n × m).
  - w : Algorithme de cryptage (pour chiffrement ou déchiffrement).
  - k : La clé secrète.
- **Sortie :**
  - f ' : image crypté.

Etapes :

1. lecture une image f
2. Extrait Largeur et la hauteur de l'image (largeur=n, hauteur=m).
3. Créer les tableaux: alpha, rouge, vert, bleu, de la taille [largeur * hauteur] de même taille de l'image hôte.
4. transférer les valeurs de pixels d'image dans des tableaux (alpha, rouge, vert, bleu).
   - Alpha [] Z f. valeurs Alpha.
   - Rouge [] Z f. valeurs Rouge.
   - Vert [] Z f. valeurs Vert.
   - Bleu [] Z f. valeurs Bleu.
5. convertir les valeurs de tableaux en suite binaire 0,1(Alpha, Rouge, Vert, Bleu).
6. Chiffrer les tableaux de valeurs binaires comme suit :
   i. Choisir un algorithme de cryptage symétrique pour le chiffrement.
   ii. Générer une clef secrète.
   iii. Appliquer un algorithme de chiffrement symétrique pour chaque tableau.

        tableau1 ()= crypter (alpha []).

        tableau2 ()=crypter (rouge []).

        tableau3 ()=crypter (vert []).

        tableau4 ()=crypter (bleu []).
7. Maintenant les nombre binaire de huit bits est transformé en son numéro décimal équivalent.

   Alpha () = tableau1 en entier

   Rouge () = tableau2 en entier

   Vert () = tableau3 en entier

   Bleu () = tableau4 en entier
8. Transformation les tableaux (alpha, rouge, vert, bleu) en fichier image
9. **Sortie** : fichier image f'.

La même manière pour déchiffré l'image, en suffisant d'entré la clé secret (pas générer un nouvel clé) ensuite déchiffré l'image.

Le schéma ci-dessous illustre les déférentes étapes de l'algorithme :

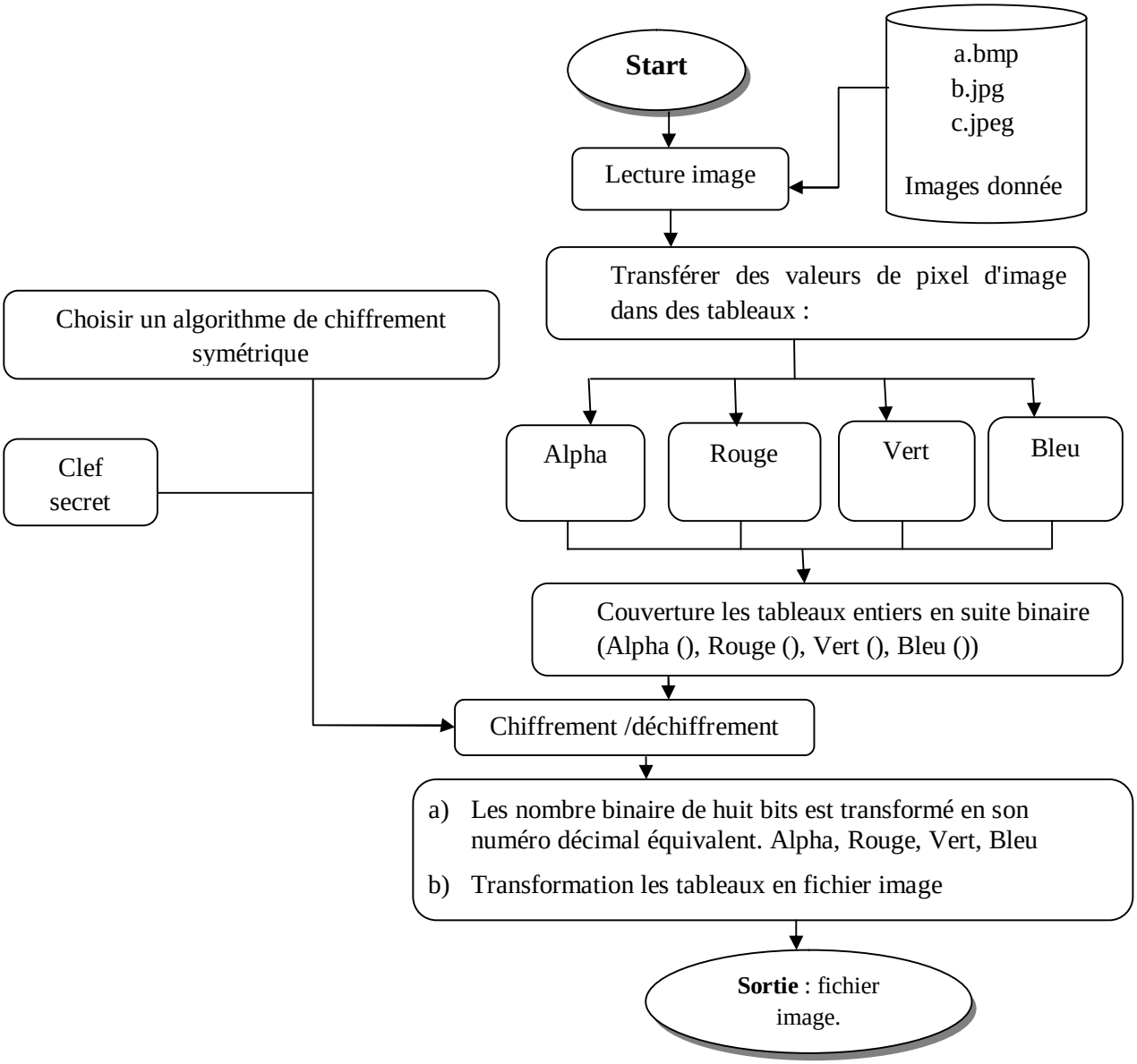

Figure 3.3 Schéma détaillé pour chiffrement/déchiffrement d'image.

4.2. Chiffrement de clé

Après chiffrement symétrique de l'image, on utilise les algorithmes de chiffrement à clé publique : RSA, El Gamal et ECC pour protéger la clé symétrique pendant la transformation des données. La figure 3.4 ci-dessous présente la manière de chiffrement de la clé:

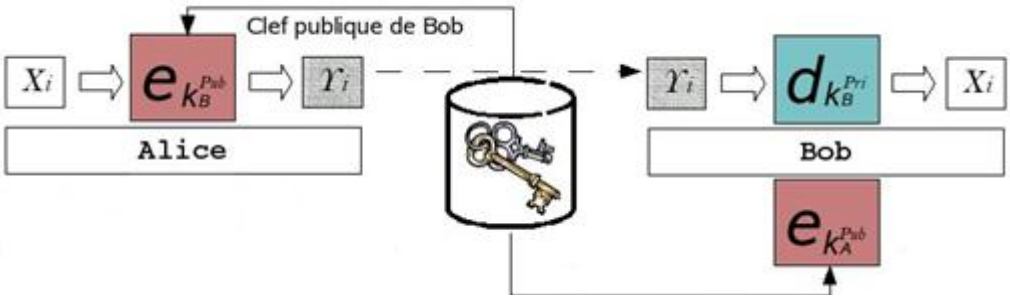

Figure 3.4 principe cryptage/décryptage de la clé.

5. Conclusion

Dans ce chapitre, nous avons présenté différents techniques de chiffrement d'image. Ces techniques sont basées sur la méthode de chiffrement hybride, c.-à-d. on utilise le cryptage symétrique pour sécuriser l'image et le chiffrement asymétrique pour assurer la confidentialité de clé, cette technique permet de sécuriser la transmission d'images.