République Algérienne Démocratique et populaire
Ministère De L'enseignement Supérieur et de la Recherche Scientifique

Université Mentouri de Constantine (UMC)

Faculté des sciences de l'ingénieur

Département d'électronique

Mémoire

Présenté pour l'obtention du diplôme de Magister (école doctorale)
en Electronique

Spécialité : Télécommunications spatiales

Thème : Fonction logistique et standard chaotique pour le chiffrement des images satellitaires

Présenté par

Goumidi Djamal Eddine

Devant le jury

Président	K. Benarbi	Professeur (Université de Constantine)
Rapporteur	F. Hachouf	Maître de conférence (Université de Constantine)
Examinateur	M. Benslama	Professeur (Université de Constantine)
Examinateur	A. Bennia	Professeur (Université de Constantine)

Année 2010

Remerciements

En préambule à ce mémoire, je souhaite adresser ici tous mes remerciements à mon encadreur Hachouf Fella pour l'aide et le temps qu'elle a bien voulu me consacrer et sans qui ce mémoire n'aurait jamais vu le jour.

Je remercie profondément les professeurs K. Benarbi, M. Benslama, A. Bennia d'avoir accepté de juger ce travail.

J'exprime mes gratitudes à tous les enseignants qui n'ont pas ménagé leurs efforts pour nous assurer une bonne formation.

Dédicaces

Merci au Noble « Allah» Dieu le tout puissant qui m'a donné le courage, l'intelligence, la force et la patience pour réaliser ce travail.

À celle qui m'a indique la bonne voie en me rappelant que la volonté fait toujours les grands hommes…

Merci ma Mère

À celui qui a attendu avec patience les fruits de sa bonne éducation…

Merci mon Père.

J'aimerais dédier ce travail tout spécialement à l'esprit de ma grand-mère car c'est elle qui nous a orienté au savoir vivre et à la loyauté. Que dieu tout puissant la protège et la bénisse INCHALLAH.

J'exprime ma gratitude à tous mes frères « Mohammed», « Yasser » et à tous mes sœurs « Noudjoud », « Sara » et « khaoula ».

J'adresse également mes plus sincères remerciements à tous mes proche et amis qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce mémoire. Entre autre « salim saad azzem », « Hichem Alloui», « Hamza Channef » et « Hassan Brahimi », ainsi que tous les autres.

Table des matières

Table des matières

Chapitre 03 Les images satellitaires

Chapitre 04 Un crypto-système pour les images satellitaires

Liste des figures

La liste des tableaux

Introduction générale

Introduction générale:

Depuis le début des civilisations, le besoin de dissimuler préoccupe l'humanité. La confidentialité apparaissait notamment nécessaire lors des luttes pour l'accès au pouvoir. Puis elle a été énormément développée pour les besoins militaires et diplomatiques. Aujourd'hui, de plus en plus d'applications dites **civiles** nécessitent la sécurité des données transitant entre deux interlocuteurs via un vecteur d'information comme les réseaux de télécommunications actuels et futurs. Ainsi les banques l'utilisent pour assurer la confidentialité des opérations avec leurs clients, les laboratoires de recherche s'en servent pour échanger des informations dans le cadre d'un projet d'étude commun, les chefs militaires pour donner leurs ordres de bataille, etc.

La cryptologie, étymologiquement la science du secret, ne peut être vraiment considérée comme une science que depuis peu de temps. On peut dire que la cryptologie est un art ancien et une science nouvelle. Cette discipline est liée à beaucoup d'autres, par exemple la théorie des nombres, l'algèbre, ou encore la théorie de l'information. Cette science comporte deux branches ; la cryptographie et la cryptanalyse.

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clé.

La cryptanalyse à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses et, en particulier, de pouvoir décrypter des textes chiffrés. Le décryptage est l'action consistant à retrouver le texte en clair sans connaître la clef de déchiffrement.

La révolution numérique a engendré des moyens plus faciles pour le traitement, le stockage et la transmission des images numériques. Cependant elle a aussi engendré des moyens de falsification, de contrefaçons et d'espionnage très avancés. Le risque est encore plus grand dans un environnement ouvert tel que la transmission des images satellitaires au sol.

Dans ces circonstances, il est devenu nécessaire de crypter ces images avant de les transmettre. Les algorithmes de chiffrement traditionnels tels que le *DES* et la *RSA* ne sont pratiquement pas appropriés au chiffrement d'images dû à quelques caractéristiques intrinsèques des images comme la taille (image de grande taille), la

redondance élevée, la forte corrélation entre les pixels adjacents, etc. Pour fournir une meilleure solution aux problèmes de sécurité d'images, un certain nombre de techniques de chiffrement d'images ont été proposées telles que les techniques basées sur les systèmes chaotiques qui fournissent une bonne combinaison entre la vitesse d'exécution et la haute sécurité

Le travail réalisé dans ce mémoire s'inscrit dans ce contexte particulier. Son objectif est de proposer un crypto-système (algorithme de chiffrement et de déchiffrement) basé sur les systèmes chaotiques pour chiffrer des images satellitaires. Il s'organise autour de quatre chapitres :

Le premier chapitre est constitué de rappels sur les systèmes chaotiques.

Le deuxième chapitre aborde la notion de la cryptographie. Les deux principaux schémas de chiffrement en cryptographie standard, le chiffrement a clef publique et le chiffrement symétrique sont décrits. Plusieurs modes de chiffrement de l'information incluant une dynamique chaotique proposés dans la littérature sont présentés.

Dans le troisième chapitre, quelques notions importantes concernant les images satellitaires notamment : les différents types d'images satellitaires, la structure de représentation des pixels et les différents formats des données images sont cités.

Dans le dernier chapitre un algorithme de chiffrement et de déchiffrement des images satellitaires utilisant un comportement dynamique chaotique sont donnés en détail. Leur sécurité et leur performance sont analysées et évaluées.

Chapitre 01

Les systèmes chaotiques

1.1. Introduction

Depuis la nuit des temps, le chaos était synonyme de désordre et de confusion, s'opposait à l'ordre devait être évité. La science était caractérisée par le déterminisme, la prévisibilité et la réversibilité. La vision déterministe, qui était celle notamment de Newton (1642-1727) ou de Laplace (1749-1827), reposait sur le fait que l'univers serait régi par des lois immuables et qu'il serait possible de connaître l'avenir et le passé à partir du simple présent. Poincaré (1854-1912) fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes. En effet, l'étude de l'interaction de deux corps peut facilement être menée par les lois de Newton, mais la considération d'un troisième corps implique des comportements complexes s'apparentant au hasard. La sensibilité aux conditions initiales est l'une des caractéristiques du chaos. Elle correspond au fait que de petites causes entraînent de grands effets. Plus tard, en 1960, le phénomène a été mis en évidence par un météorologiste, Lorenz. Il implémenta un programme informatique simplifié, impliquant trois équations différentielles, pour modéliser quelque élément météorologique. Ce phénomène, qui traduit cette sensibilité aux conditions initiales, est connu sous le nom d'effet papillon. Le battement d'ailes d'un papillon, engendrerait une tempête.

Le terme "chaos" définit un état particulier d'un système dont le comportement ne se répète jamais, est très sensible aux conditions initiales, est imprédictible à long terme. Des chercheurs d'horizons divers ont alors commencé à s'intéresser à des problèmes non linéaires jusqu'alors sans solution parce qu'imprédictibles et regroupés sous la dénomination de chaos. Ils ont cherché à répondre à des questions telles que : Les arythmies cardiaques ou les variations d'une population animale obéissent-elles à des règles? Les mouvements commerciaux ou les marchés financiers peuvent-ils s'expliquer? Le modèle du biologiste Robert May [1] décrit l'évolution de la population d'une espèce en fonction des contraintes du milieu (famines, épidémies, ...) et obéit à une dynamique chaotique (équation logistique). Richard Cohen, physicien et cardiologue, a montré lors de simulations que le caractère chaotique du rythme cardiaque pourrait expliquer l'apparition de crise cardiaque. William Baumol et Jess Benhabib [1], économistes, se sont intéressés à la théorie du chaos et à ses applications à l'économie. Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physique que biologique, chimique ou économique, par exemple.

1.2. La théorie du chaos est-elle née dans les années 1970 ?

La réponse à cette question est : oui et non.

Non, car le phénomène de sensibilité aux conditions initiales a été découvert dès la fin du XIXe siècle par Henri Poincaré, puis par Hadamard avec un modèle mathématique abstrait aujourd'hui baptisé « flot géodésique sur une surface à courbure négative ». Cette découverte a entraîné un grand nombre de travaux importants, principalement dans le domaine des mathématiques. [2]

Oui, car ce n'est véritablement dans les années 70 que la théorie du chaos s'est progressivement imposée sur le devant de la scène scientifique. Le terme suggestif de « chaos » n'a d'ailleurs été introduit qu'en 1975 par les deux mathématiciens Tien-Yien Li et James A. Yorke. La théorie du chaos doit sa popularisation aux progrès de l'informatique. Cette nouvelle technologie a rendu possible la visualisation de l'incroyable complexité de ces systèmes dynamiques, auparavant réservée aux seuls « initiés » capables d'absorber le formalisme mathématique idoine. [3]

1.3. Les Conditions d'obtention du chaos [2]

- **La non-linéarité :** un système chaotique est un système dynamique non linéaire. Un système linéaire, ne peut pas être chaotique.
- **Le déterminisme :** un système chaotique a des règles fondamentales déterministes et non probabilistes. Le déterminisme est la capacité à « prédire » le futur d'un phénomène à partir d'un évènement passé ou présent. L'évolution irrégulière du comportement d'un système chaotique est du aux non linéarités
- **La sensibilité aux conditions initiales :** de très petits changements sur l'état initial peuvent mener à des comportements radicalement différents dans son état final.
- **L'imprévisibilité:** En raison de la sensibilité aux conditions initiales.

1.4. La sensibilité aux conditions initiales

D'après James Gleick [1], le premier scientifique à s'être intéressé aux systèmes complexes serait le météorologue Edward LORENZ. Dans les années 60, Lorenz travaillait au M.I.T sur les questions de prévisions météorologiques. Il avait réussi à réduire la météorologie à sa plus simple expression en décrivant les mouvements de l'air et de l'eau par de simples équations, puisque c'est l'interaction de ces deux éléments qui fait la pluie et le beau temps. L'ordinateur se faisait alors une joie de régurgiter à Lorenz des bulletins météo. Son raisonnement était le suivant : puisque la météorologie est régie par les lois de la nature, et que le monde suit une trajectoire déterministe, il suffit d'introduire des données plus ou moins précises dans un

ordinateur pour que celui-ci donne une projection climatique plus ou moins précise. Ce faisant, Lorenz marchait encore sous la bannière de Newton : " étant donné une connaissance approximative des conditions initiales et une compréhension des lois de la nature, on peut déterminer le comportement approximatif du système ".

Un jour d'hiver 1961, Lorenz voulut reprendre le calcul d'un bulletin météo interrompu prématurément. Sans reprendre tous ses calculs depuis le début, il introduit son dernier listage en tronquant les nombres à 3 décimales : 0,506 (127), supposant que la différence – un pour un millier – sera sans conséquence. Lorsqu'il revient, une heure plus tard, le graphique, censé reproduire exactement le précédent, suit une évolution de plus en plus divergente jusqu'à la disparition de toute ressemblance. Ainsi, un petit changement initial avait entraîné un énorme changement final.

Le chaos impose donc une limite fondamentale à notre aptitude à prévoir la météo. Cela ne veut pas dire qu'il faut cesser d'écouter le bulletin météorologique. Les prévisions à court terme, sur un ou deux jours, et sur une superficie restreinte comme celle de l'Algérie sont assez fiables ; en revanche, au-delà de 6 ou 7 jours, les prévisions deviennent spéculatives, voire carrément fausses. Cette limite de la connaissance est incontournable. Même si on couvrait la terre de stations météo se touchant les unes les autres, il y aurait toujours de petites fluctuations dans l'atmosphère, si minuscules qu'elles ne pourraient être détectées, pour s'amplifier et modifier le climat de la planète entière.

C'est pourquoi le chaos a souvent été explicité par ce qu'on appelle l'effet papillon : le battement d'aile d'un papillon aujourd'hui à Pékin engendre dans l'air suffisamment de remous pour influer sur l'ordre des choses et provoquer une tempête le mois prochain à New-York.

L'effet papillon prit une désignation technique **:** la dépendance sensitive aux conditions initiales.

Ce que nous apprend le modèle de Lorenz, c'est qu'aucune incertitude initiale, aussi négligeable puisse-t-elle paraître, ne doit être négligée dans un système doté de sensibilité aux conditions initiales, vu ses conséquences à long terme. Cela revient aussi à dire que la prédiction à long terme n'a pas de sens, étant donné le très grand nombre de perturbations minimes mais incontrôlées présentes non seulement en météorologie, mais aussi dans beaucoup d'autres systèmes.

C'est ce que l'on appelle le " chaos ". Le chaos tel que le scientifique le comprend ne signifie pas " absence d'ordre " ; il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir à long terme. Parce que l'état final dépend de manière si sensible de l'état initial, qu'un petit rien peut tout venir modifier, nous sommes fondamentalement limités dans la prédiction de cet état final.

En somme, notre connaissance de l'état initial est toujours entachée d'une certaine imprécision. [1]

1.5. La différence entre le chaos et l'aléatoire

La différence entre le chaos et l'aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop important de paramètres en jeu dans sa description. Ce qui nous pousse à en donner une approche probabiliste qui peut être parfaitement satisfaisante, garde par définition une certaine marge d'aléatoire.

En ce qui concerne le chaos, il n'en est rien, les systèmes chaotiques se comportent, en effet, d'une manière qui peut sembler aléatoire. Mais ce comportement est en fait décrit de manière déterministe par des équations non-linéaires parfaitement déterministes, c'est-à-dire en particulier avec des outils mathématiques qui permettant une approche précise et certaine. Pour paraphraser une publicité célèbre, on pourrait écrire : "Ça ressemble à du hasard, ça a le goût du hasard,...mais ce n'est pas du hasard !". [4]

1.6. L'évolution vers le chaos

Il existe plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos. Nous allons en exposer brièvement deux. Ces évolutions surviennent par augmentation des contraintes appliquées au système (par exemple, les vitesses angulaires dans le cadre des pendules).

- **Par intermittences**

Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement périodique, c'est à dire une certaine "régularité", et il se déstabilise, brutalement, pour donner lieu à une sorte d'explosion chaotique. Il se stabilise de nouveau ensuite, pour donner lieu à une nouvelle "bouffée" plus tard.

On a constaté que la fréquence et la durée des phases chaotiques avaient tendance à s'accroître plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition. [4]

- **Par doublement de la période**

Par augmentation du paramètre de contrôle de l'expérience, la fréquence du régime périodique double, puis est multipliée par 4, par 8, par 16 … etc. Les doublements étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie. C'est à ce moment que le système devient chaotique. [4]

1.7. Les attracteurs

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évoluent un système, quelles que soient ses conditions initiales.

Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases.
Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques.

❖ Attracteurs réguliers

Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de deux sortes :

- **un point fixe :** la trajectoire du pendule dissipatif simple (dans l'espace des phases représentant son altitude et sa vitesse), par exemple, tend vers l'origine du repère, quelles que soient la position et la vitesse initiales.
- **un cycle limite** : la trajectoire du pendule idéal dans ce même espace des phases, par exemple.

Pour tous les attracteurs réguliers, c'est à dire pour tous les systèmes non-chaotiques, des trajectoires qui partent de "points" proches l'un de l'autre dans l'espace de phase [1] restent indéfiniment voisines. On sait donc prévoir l'évolution de ces systèmes, à partir d'une situation connue. [4]

❖ Les attracteurs étranges

Les attracteurs étranges sont caractéristiques de l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace des phases (et appartenant au bassin d'attraction de l'attracteur) donnent des trajectoires qui tendent à former l'attracteur étrange.

[1] Il s'agit d'un espace de 2 ou 3 dimensions dans lequel chaque coordonnée est une variable d'état du système considéré.

A grande échelle, un attracteur étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent (puisque, par définition deux point ne peuvent avoir la même évolution), mais comme l'attracteur a des dimensions finies, l'attracteur doit se replier sur lui-même. Le processus d'étirement-repliement se répète à l'infini et fait apparaître un nombre infini de "plis" imbriqués les uns dans les autres qui ne se recoupent jamais.

Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques.

On obtient ainsi des attracteurs différents (en fonction des systèmes étudiés), qui présentent des formes diverses et surprenantes. [4]

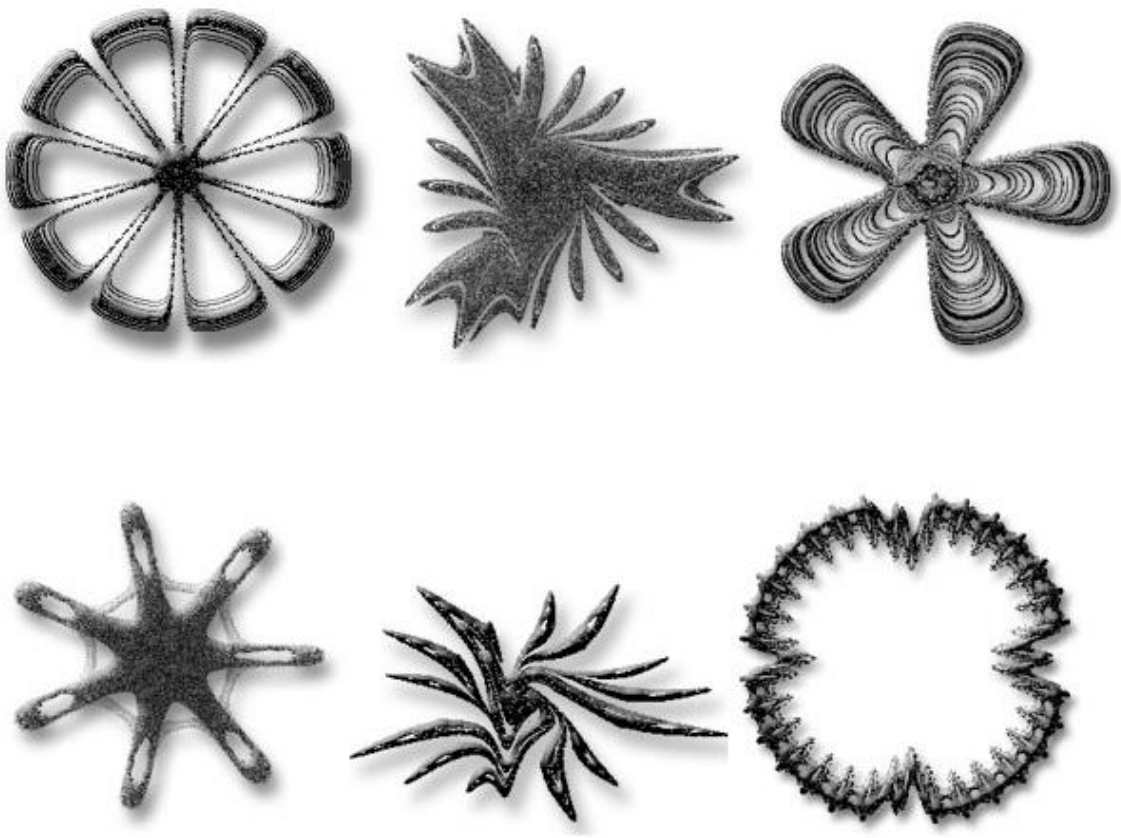


Fig.01.1. Attracteurs étranges.

1.8. Quelques exemples de récurrences chaotiques

Le chaos peut surgir simplement en réitérant des fonctions mathématiques. Plusieurs fonctions simples existent dans la littérature.

1.8.1. La récurrence logistique

Une récurrence logistique est un exemple simple de suite dont la récurrence n'est pas linéaire. Souvent citée comme exemple de la complexité pouvant surgir de simple relation non linéaire, cette récurrence fut popularisée par le biologiste Robert May en 1976. [5]

Sa relation de récurrence est :

$$X_{n+1} = \mu X_n (1 - X_n) \qquad (01.1)$$

Elle conduit, suivant les valeurs de μ, à une suite convergente, une suite soumise à oscillations ou une suite chaotique.

Elle est la solution en temps discret du modèle de Verhulst [5]. Le terme « logistique » provient de l'ouvrage de Pierre François Verhulst qui appelle courbe logistique la solution en temps continu de son modèle. Il écrit en 1845 dans son ouvrage consacré à ce phénomène : « *Nous donnerons le terme de logistique à cette courbe* ». L'auteur n'explique pas son choix mais « logistique » a même racine que logarithme et *logistikos* signifie « calcul » en grec.

Comportement selon μ :

Dans le modèle logistique, la variable notée ici x_n désigne l'effectif de la population d'une espèce. En faisant varier le paramètre μ, plusieurs comportements différents sont observés :

- Si $0 \leq \mu \leq 1$, l'espèce finira par mourir, quelle que soit la population de départ.
- Si $1 \leq \mu \leq 3$, la population se stabilisera sur la valeur $\frac{\mu - 1}{\mu}$ quelle que soit la population initiale.
- Si $3 < \mu \leq 1 + \sqrt{6}$ (approximativement 3,45), la population oscillera entre deux valeurs. Ces deux valeurs sont indépendantes de la population initiale.
- Si $3{,}45 < \mu < 3{,}54$ (approximativement), la population oscillera entre quatre valeurs, là encore sont indépendantes de la population initiale.
- Si μ est légèrement plus grand que 3,54, la population oscillera entre huit valeurs, puis 16, 32, etc.

- Vers μ = 3,57, le chaos s'installe. Aucune oscillation n'est encore visible et de légères variations de la population initiale conduisent à des résultats radicalement différents.
- La plupart des valeurs au-delà de 3,57 présentent un caractère chaotique, mais il existe quelques valeurs isolées de μ avec un comportement qui ne l'est pas. Celles-ci s'appellent parfois les iles de la stabilité. Par exemple autour de la valeur 3,82, un petit intervalle de valeurs de μ présente une oscillation entre trois valeurs et pour μ légèrement plus grand, entre six valeurs, puis douze, etc. ces comportements sont encore indépendants de la valeur initiale.
- Au-delà d*e* μ = 4, la population quitte l'intervalle [0;1] et diverge presque pour toutes les valeurs initiales.

Un diagramme de bifurcation permet de résumer tout cela :

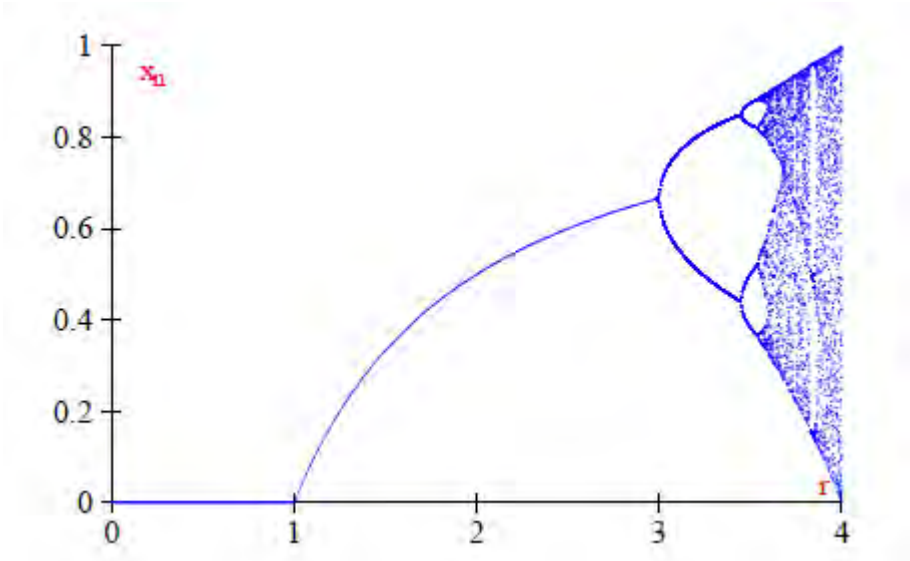


Fig.01. 2. Diagramme de bifurcation de la récurrence logistique dont l'axe horizontal porte les valeurs du paramètre μ (noté r), tandis que l'axe vertical montre les valeurs limites possibles.

1.8.2. La récurrence sine

La récurrence sine d'une (01) dimension a pour représentation d'état :

$$X_{n+1} = \lambda \sin(\pi X_n) \qquad (01.2)$$

Avec λ = 1 le comportement chaotique est généré par une manière très similaire à la fonction logistique. Comme la récurrence logistique, la carte sine est quadratique au voisinage de x = 0,5. Elles ont une distribution probabiliste et une évolution vers le chaos par doublement de période presque identique. Les fenêtres se produisent périodiquement dans le même ordre. Elle a le même nombre de

Feigenbaum que la carte logistique. Malgré les similitudes, il existe quelques différences, l'exposant de Lyapounov[2] est d'environ cinquante pour cent plus petit. Les bifurcations par doublement de période survenir plus tôt, et les fenêtres périodiques sont plus larges par rapport à la carte logistique. [6]

1.8.3. La récurrence standard: [7]

L'origine de l'utilisation et de la bonne reconnaissance de la carte standard réfère au domaine de la physique des particules. Le problème est examiné par Fermi avec une balle qui rebondit entre un mur fixe et un autre oscillant (puisqu'il est analogue au mécanisme d'accélération des rayons cosmique où les particules sont accélérés par une collision). Pour chaque impact de la balle sur le mur la phase de l'oscillation est choisie au hasard.

Ce problème de l'accélération des particules peut-être représenté par une simple fonction à 2 dimensions connue sous le nom de carte standard (également connu sous le nom carte de Chirikov-Taylor ou carte standard de Chirikov). Il est défini par:

$$X_{n+1} = X_n + K \sin Y_n$$
$$Y_{n+1} = Y_n + X_{n+1} \qquad (01.3)$$

Où X_n et Y_n sont prises modulo 2π.

Cette carte décrit également le mouvement d'un système mécanique simple, appelé rotateur forcé (kicked rotator). Il se compose d'un bâton qui est libre de la force gravitationnelle, et qui tourne dans un plan sans frottement autour d'un axe situé dans l'un de ses extrémités, et est périodiquement frappé. Les variables Xn et Yn, représentent respectivement, la position et le moment angulaire du bâton après le énième coup. La constante K mesure l'intensité des coups.

Pour K = 0, la carte n'est pas linéaire et seules les orbites périodiques et quasi-périodiques existent. Lorsqu'elles sont tracées dans l'espace des phases, les orbites périodiques apparaissent comme des courbes fermées, et les orbites quasi-périodiques comme des petites courbes fermées dont leurs centres se situent dans une autre courbe fermée plus grande. Ces types d'orbites sont observés suivant les conditions initiales utilisées. La non-linéarité de la carte est augmentée lorsque k augmente. La fig.01.3 représente une collection d'orbites différentes de la carte standard pour des valeurs diverses de k.

[2] Mesure le taux moyen de divergence de deux trajectoires issues de conditions initiales très proches

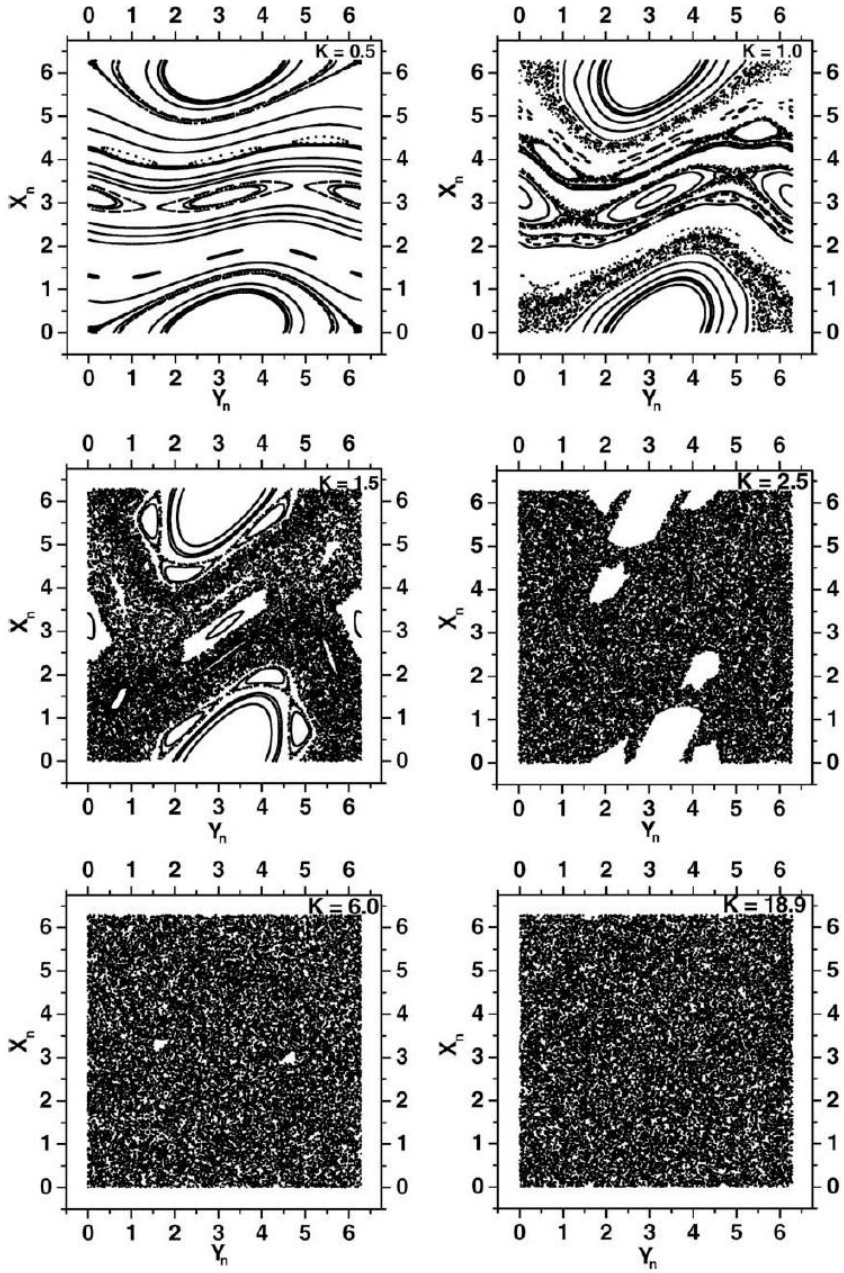


Fig.01.3. L'espace de phase de la carte standard pour K = 0.5, 1.0, 1.5, 2.5, 6.0 and 18.9.

1.9. Conclusion

Dans le présent chapitre, quelques rappels sur les systèmes chaotiques ont été effectués. Nous allons montrer leur utilisation à des fins de chiffrement de données. En effet, les systèmes chaotiques possèdent des propriétés proches de celles requises en cryptographie usuelle.

Le prochain chapitre introduit la notion de la cryptographie et présente les différents schémas de chiffrement basés sur l'utilisation des systèmes dynamiques chaotiques

Chapitre 02

Le chiffrement classique et le chiffrement basé sur le chaos

2.1. Introduction

Pendant longtemps, le chaos a été considéré comme indésirable par la communauté scientifique. Cependant, dans les années 90, des scientifiques ont réalisé que le chaos pouvait être contrôlé et ont commencé à chercher ses applications possibles. Les signaux issus des systèmes chaotiques sont imprédictibles à long terme, peuvent présenter des propriétés proches de l'aléatoire (auto-corrélation réduite), bien qu'issus de systèmes déterministes. Ces caractéristiques sont liées aux propriétés requises par les schémas de chiffrement, telles que la confusion et la diffusion de Shannon [8]. En 1990, Pecora et Carroll [9] ont montré que les systèmes chaotiques peuvent être synchronisés. Une des applications du chaos qui a alors intéressé les chercheurs est l'utilisation de systèmes chaotiques à des fins de chiffrement. De nombreux schémas de chiffrement basés sur le chaos ont été proposés dans la littérature.

En cryptographie usuelle, et parmi une grande variété de mécanismes de chiffrement, on distingue le chiffrement à clé publique et le chiffrement a clé secrète. Dans la section (2.2), une vue historique de la cryptographie est donnée. Ensuite dans la section (2.3), les deux principaux algorithmes de la cryptographie standard (chiffrement a clé publique et chiffrement a clé secrète) sont présentés. La Section (2.4) est consacrée aux différents schémas de chiffrement par le chaos rencontrés dans la littérature.

2.2. Introduction générale à la cryptographie

2.2.1. Un peu d'histoire

La fonction première de la cryptographie est de cacher le sens d'un message à ceux qui ne sont pas autorisés à le connaître. La cryptographie existe depuis que les hommes ont appris à communiquer entre eux. Vers 600 ans avant J.-C., Nabuchodonosor, roi de Babylone, écrivait le message qu'il souhaitait transmettre à ses généraux, sur le crâne préalablement rasé de ses esclaves. Il attendait que leurs cheveux repoussent avant de les envoyer chez ses généraux, qui rasaient de nouveau les cheveux des messagers pour lire le texte. Dans l'Antiquité, les Grecs employaient, en temps de guerre, un dispositif appelé une scytale. Ce dispositif consistait en une bande étroite de parchemin sur laquelle ils écrivaient après l'avoir enroulée en spirales autour d'un cylindre de bois. Une fois la bande déroulée, le texte ne pouvait être lu que par une personne possédant un cylindre de même diamètre sur lequel elle pouvait enrouler la bande.

Une méthode plus sûre qui se rapproche davantage des systèmes cryptographiques est le code de César (50 ans avant J.-C.). Pour masquer ses messages, Jules César utilisait une substitution, c'est-à-dire qu'il remplaçait chaque

lettre du message par une autre lettre de l'alphabet, décalée d'une quantité fixe de la lettre d'origine. Ce code était peu sûr car l'alphabet comprenant 26 lettres. Mais, la faible alphabétisation de la population le rendait assez efficace. De par sa simplicité de mise en œuvre, il a même été réutilisé par l'armée russe pendant la première guerre mondiale. Les systèmes cryptographiques qui suivirent gardèrent ce principe de substitution.

Plus tard, en 1467, Leone Battista Alberti proposa un procédé de substitution poly-alphabétique. Son principe était de remplacer chaque lettre du message par une lettre d'un autre alphabet et de changer plusieurs fois d'alphabet au cours du procédé. Vers 1500, l'abbé Jean Trithème imagina un dispositif consistant à remplacer une lettre du message par un groupe de mots. Ces groupes de mots étaient choisis de telle manière qu'un texte latin cohérent, une prière ou une glorification religieuse résultaient de la succession de ces groupes de mots.

L'inconvénient majeur de ces procédés cryptographiques fondés sur la substitution était le problème de la fréquence d'apparition des lettres. Par exemple, dans la langue française, la lettre "e" a une plus grande fréquence d'apparition dans les mots que la lettre *"z"*. Cette fréquence d'apparition est conservée dans le texte codé, pouvant ainsi conduire à son décodage. Pour renforcer la sécurité, les algorithmes basés sur la substitution ont été développés et améliorés. Ainsi, en 1586, le diplomate français Biaise de Vigenère proposa une technique plus élaborée, basée sur une substitution poly-alphabétique. Il utilisa une clé littérale, ou mot de passe, dont chaque lettre indiquait le décalage alphabétique à appliquer sur les lettres du message. L'inconvénient de ce procédé résidait dans l'échange de la clé qui n'était pas sécurisé et qui pouvait conduire à l'interception de la clé.

En 1918, Arthur Scherbius fit breveter sa machine à crypter, appelée Enigma. Son principe fut que chaque lettre du message était remplacée par une autre, la règle de substitution changeant d'une lettre à une autre. Ce procédé permettait d'évincer le problème de la fréquence d'apparition des lettres ainsi que celui de l'échange de la clé. Cette machine fut utilisée pendant la seconde guerre mondiale.

L'ingénieur américain Philip Johnston eut l'idée d'utiliser la langue navajo comme procédé cryptographique. La méconnaissance quasi totale de cette langue ainsi que sa construction grammaticale très particulière, la rendant impénétrable aux étrangers, décidèrent de son utilisation, lors de la campagne du Pacifique pendant la seconde guerre mondiale.

Le développement des ordinateurs, (les techniques de communication et la mondialisation des échanges (Internet, commerce électronique, ...) sont confrontés à de nouveaux problèmes de sécurité de l'information. De ce fait, la cryptographie n'a plus seulement la vocation de préserver la confidentialité des données, mais elle a

aussi pour rôle de préserver le contenu des messages de toute modification non souhaitée, de s'assurer de l'identité de l'émetteur et du destinataire afin d'éviter toute usurpation d'identité, les systèmes cryptographiques existant jusqu'alors doivent être perfectionnés pour faire face à ces nouveaux problèmes.

Dans les années 70, Horst Feistel a mené à IBM, un projet de recherche sur le chiffrement, qui inspira plus tard le schéma de chiffrement symétrique DES. En 1976, Whitfield Diffie et Martin Hellmann proposent la cryptographie à clé publique. Ce schéma permet de pallier le problème de l'échange de clé, rencontré dans la substitution poly-alphabétique de Vigenère. Le chiffrement du message est fondé sur des problèmes mathématiques difficiles à résoudre.

Un autre procédé célèbre est la cryptographie symétrique, dont quelques exemples sont le schéma de Vigenère et, beaucoup plus récemment, l'algorithme DES. Dans ce cas, les clés pour coder et décoder le message sont les mêmes. L'émetteur et le destinataire doivent alors s'accorder sur une clé qui doit être gardée secrète. Le chiffrement est fondé sur une combinaison complexe de substitutions. Les deux algorithmes principaux, le chiffrement à clé publique et le chiffrement symétrique, sont toujours d'actualité. [10]

2.2.2. Définitions

La cryptographie est l'étude de techniques mathématiques liées à la sécurité de l'information. Par sécurité de l'information, on entend la confidentialité des données, l'intégrité des données, l'authentification des données et des communicants, et la non répudiation des données. La confidentialité consiste à garder des données secrètes pour tous ceux qui ne sont pas autorisés à les connaître. L'intégrité des données a pour but de préserver les données de toute altération non autorisée. L'authentification des données consiste à faire le lien entre les données et leur expéditeur. L'authentification des entités consiste à s'assurer de leur identité. La non répudiation consiste à éviter que, par la suite, les communicants nient leurs actions : l'émetteur nie avoir envoyé un message et le récepteur nie avoir reçu un message.

La cryptographie consiste notamment en l'élaboration de schémas de chiffrement/déchiffrement ou crypto-systèmes et pratiquée par des cryptographes. Le chiffrement (”encryption”, en anglais) est l'opération qui consiste à transformer un message afin d'en cacher le sens à tous ceux qui ne sont pas autorisés à le connaître. Le déchiffrement (“decryption”, en anglais) est l'opération inverse du chiffrement. Il a pour but de récupérer l'information masquée. Un crypto-systeme est l'ensemble des deux méthodes de chiffrement et de déchiffrement. En cryptographie, l'information à masquer est également appelée message ou texte clair (“plaintext”, en anglais). Le résultat du chiffrement d'un texte clair est appelé texte chiffré

("ciphertext", en anglais). Le texte chiffré est le résultat d'une transformation dépendant du message et d'une clé. Les différents processus de la cryptographie sont illustrés par la figure suivante :

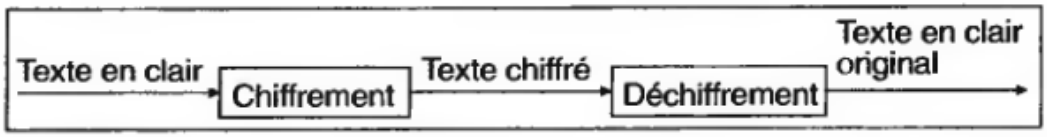


Fig.02.1. Chiffrement et déchiffrement

Le texte en clair est note *M.* Ce peut être une suite de bits, un fichier de texte, un enregistrement de voix numérisé, ou une image numérique. Du point de vue de l'ordinateur, *M* n'est rien d'autre que de l'information binaire. Le texte en clair peut être transmis ou stocké. Dans tous les cas, *M* est le message à chiffrer. Le texte chiffré est noté *C,* C'est aussi de l'information binaire, parfois de la même taille que *M* et parfois plus grande.

La fonction de chiffrement, notée *E*, transforme *M* en *C.* Ce qui en notation mathématique s'écrit:

$$E(M) = C. \qquad (02.1)$$

La fonction inverse, notée *D,* de déchiffrement transforme *C* en *M:*

$$D(C) = M. \qquad (02.2)$$

Comme le but de toutes ces opérations n'est rien d'autre que de retrouver le message en clair à partir de la version chiffrée de ce même message, l'identité suivante doit être vérifiée:

$$D(E(M)) = M. \qquad (02.3)$$

Parmi une grande variété de mécanismes de chiffrement, les deux algorithmes principaux en cryptographie standard sont le chiffrement à clé publique (antisymétrique) et le chiffrement à clé secrète (symétrique), présentés dans la section suivante. [10,11]

2.3. Chiffrement en cryptographie standard

2.3.1. Chiffrement à clef publique

Le chiffrement à clé publique, ou chiffrement asymétrique, a été proposé par Diffie et Hellman, en 1976. Dans un tel schéma, la clé de chiffrement est différente de celle de déchiffrement. N'importe qui peut utiliser la clé de chiffrement, ou clé publique, pour chiffrer un message, mais seul celui qui possède la clé de déchiffrement, ou clé privée, peut déchiffrer le message chiffré résultant.

De plus, la clé de déchiffrement K^d ne peut pas être calculée (du moins dans un temps raisonnable) à partir de la clé de chiffrement K^e. Ce type de schéma repose directement sur l'existence de fonctions à sens unique. Une fonction est dite à sens unique quand il est facile de calculer K^e en connaissant K^d mais très difficile de calculer K^d connaissant K^e. Parfois, des fonctions à sens unique qui possèdent en plus une trappe sont utilisées. Une fonction à sens unique est dite à trappes quand il est très difficile de calculer K^d à partir de K^e, sauf si on connaît une information supplémentaire.

Lorsque Alice l'émetteur et Bob le destinataire, veulent communiquer de façon sécurisée, Bob choisit une paire de clés de chiffrement et de déchiffrement (K^e, K^d). Il envoie la clé publique K^e à Alice, par l'intermédiaire d'un canal qui n'est pas forcément sécurisé. Alice transforme le message M en texte chiffré C = E (K^e, M), où E représente une fonction de chiffrement, et envoie ce texte chiffré C à Bob. De son côté, Bob reçoit le texte chiffré C et calcule M = D (K^d, C) où D est une fonction de déchiffrement et K^d est la clé privée connue uniquement de Bob. Ainsi, Bob récupère le message initial M.

Un exemple de chiffrement à clé publique est le schéma RSA, proposé par Rivest, Shamir et Adleman, en 1978. Ce schéma est encore très largement utilisé (sites web commerciaux, par exemple). Il repose sur la difficulté de factoriser des grands nombres et s'appuie donc sur la théorie des nombres.

La génération des clés publique et privée peut être résumée par les étapes suivantes :

- Bob choisit deux grands nombres premiers (de longueur 1024 ou 2048 bits, en général) p et q et calcule n = pq.
- Bob choisit aussi, de façon aléatoire, un entier $K^e < n$ qui est premier avec (p − 1) (q − 1).

- Il calcule K^d tel que $K^e K^d = 1 \bmod (p - 1)(q - 1)$.
  - Bob publie la clé publique, formée de (K^e, n).
  - Pour envoyer un message à Bob, Alice calcule $C = M^{K^e}$ et envoie C à Bob, et pour déchiffrer C, Bob calcule $M = C^{K^d} \bmod n$.

Dans ce schéma, la fonction de chiffrement est une fonction à sens unique et possède une trappe. En effet, toute personne connaissant la clé publique (K^e, n) et la factorisation de n peut calculer K^d. [10]

2.3.2. Chiffrement à clef secrète

Par opposition au chiffrement à clé publique, le chiffrement à clef secrète est aussi appelé chiffrement symétrique. La clé de chiffrement peut être calculée à partir de la clé de déchiffrement et vice versa. En général, les clés de chiffrement et de déchiffrement sont identiques. L'émetteur et le destinataire doivent se mettre d'accord préalablement sur une clé qui doit être gardée secrète, car la sécurité d'un tel algorithme repose sur cette clé.

Le chiffrement à clé publique et le chiffrement symétrique présentent chacun des avantages. Par exemple, le temps de chiffrement/déchiffrement du chiffrement à clé publique est supérieur à celui du chiffrement symétrique. Un des problèmes principaux du chiffrement symétrique est l'échange préalable de la clé secrète. Le chiffrement à clé publique peut être préféré pour générer de petites séquences comme des signatures ou des clés secrètes pour le chiffrement symétrique. Le chiffrement symétrique peut être préféré pour chiffrer des grandes quantités de données.

Les schémas de chiffrement symétrique peuvent être classés en deux catégories, le chiffrement par blocs et le chiffrement par flot.

Les schémas de chiffrement par flot et appelé aussi chiffrement en continu, traitent l'information bit à bit, et sont très rapides. Ils sont parfaitement adaptés à des moyens de calcul et de mémoire (cryptographie en temps réel) comme la cryptographie militaire, ou la cryptographie entre le téléphone portable GSM et son réseau.

Leur principe est d'effectuer un chiffrement de Vernam en utilisant une clé pseudo-aléatoire, c'est à dire une clé qui ne soit pas choisie aléatoirement parmi tous les mots binaires de longueur n. Cette clé (qu'on appellera *suite pseudo-aléatoire*) est générée par différents procédés à partir d'une clé secrète d'une longueur juste suffisante pour résister aux attaques exhaustives.

Dans un schéma de chiffrement par blocs, le message est divisé en blocs de bits, de longueur fixe. Chaque bloc est chiffré l'un après l'autre. Le chiffrement peut être effectué par substitutions (les bits d'un bloc sont substitués par d'autres bits) et par transpositions (les bits d'un bloc sont permutés entre eux). La substitution permet d'ajouter de la confusion, c'est-à-dire de rendre la relation entre le message et le texte chiffré aussi complexe que possible. La transposition permet d'ajouter de la diffusion, c'est-à-dire de réarranger les bits du message afin d'éviter que toute redondance dans le message ne se retrouve dans le texte chiffré.

On distingue le chiffrement par blocs itératifs. Une fonction constituée de combinaisons complexes de substitutions et/ou de transpositions, appelée fonction de tour ou fonction de ronde, est appliquée itérativement. Une itération est appelée un tour ou une ronde. Chaque ronde prend en entrée la sortie de la ronde précédente et chiffre cette entrée à l'aide de la fonction de ronde et d'une sous-clé de ronde générée à partir de la clé secrète *K*. La fonction de chiffrement n'est pas la fonction de ronde, mais elle est constituée par l'ensemble de toutes les rondes.

Un exemple de chiffrement par blocs itératifs est le célèbre schéma DES (Data Encryption Standard), adopté par le gouvernement américain, en 1977, comme algorithme de chiffrement standard officiel. Dans ce schéma, le texte clair est divisé en blocs de longueur 64 bits. La clé a également une longueur de 64 bits. Le chiffrement d'un bloc s'effectue avec 16 rondes. La clé secrète *K* est dérivée de 16 "sous-clés" une pour chaque ronde. Chaque entrée de ronde est partagée en une partie gauche *L* et une partie droite *R*, de même longueur. Pour $i = 0,\ldots, 15$, les quantités R_{i+1} et L_{i+1} sont calculées :

$$\begin{cases} \boldsymbol{R}_{i+1} = \boldsymbol{L}_i \oplus f\left(\boldsymbol{R}_i, \boldsymbol{K}_i\right) \\ \boldsymbol{L}_{i+1} = \boldsymbol{R}_i \end{cases} \qquad (02.4)$$

Où f est la fonction de ronde.

Pour renforcer la sécurité, il existe des variantes du DES qui consistent à utiliser une clé *K* de longueur plus importante et à répéter plusieurs fois l'algorithme sur chaque bloc, comme le triple-DES. Les longueurs des clés ne permettent pas toujours de résister à des attaques de plus en plus performantes grâce au progrès des ordinateurs. Pour pallier ce problème, le schéma DES est amélioré et devient le schéma AES (Advanced Encryption Standard), en 1997. [10,12]

2.4. Chiffrement basé sur le chaos [10]

Le principe des schémas de chiffrement basé sur le chaos consiste à mélanger l'information m_k avec une séquence chaotique issue d'un émetteur, décrit généralement par une représentation d'état avec le vecteur d'état x_k. Seule la sortie y_k de l'émetteur est transmise au récepteur. Le récepteur a pour rôle d'extraire l'information originale du signal reçu y_k. La récupération de l'information est généralement basée sur la synchronisation des états x_k de l'émetteur et des états x'_k du récepteur, c'est-à-dire :

$$\lim_{k\to\infty} \| x_k - x'_k \| = 0 \qquad (02.5)$$

Ou

$$\exists k_f, \quad \| x_k - x'_k \| = 0, \forall k > k_f \qquad (02.6)$$

Différentes techniques d'injection de l'information dans un système chaotique ont été proposées dans la littérature, telles que le masquage additif, la modulation chaotique, la modulation paramétrique. Dans cette section, ces différentes techniques sont présentées.

2.4.1. Masquage chaotique

Le principe de ce schéma consiste à effectuer une simple addition entre le signal de sortie de l'émetteur et l'information m_k .L'émetteur (générateur de chaos) et le récepteur ont pour représentation d'état, respectivement:

$$\begin{cases} x_{k+1} = f(x_k) \\ y_k = x_{k+1} + m_k \end{cases} \qquad \begin{cases} x'_{k+1} = f'(x'_k) \\ y'_k = x'_{k+1} \end{cases} \qquad (02.7)$$

Où x_k (resp. x'_k) est le vecteur d'état de l'émetteur (resp. du récepteur), y_k (resp. y'_k) la sortie de l'émetteur (resp. du récepteur), m_k l'information à masquer. La figure suivante illustre ce mode de masquage.

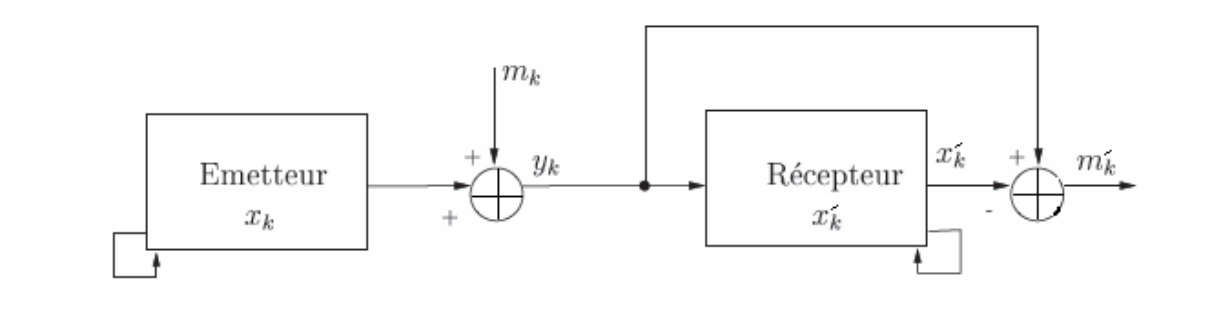


Fig.02.2. Masquage additif

La reconstruction de l'information nécessite la synchronisation de l'émetteur et du récepteur. L'information est alors récupérée en soustrayant la sortie du récepteur avec celle de l'émetteur :

$$m_k = y_k - x'_k \qquad (02.8)$$

2.4.2. Modulation chaotique

La modulation chaotique, est aussi connue sous le nom de "chaos shift-keying" ou "chaotic switching", en anglais.

Côté émetteur, à chaque symbole $m_k = m_i$ de l'information, appartenant à un ensemble fini $\{m_1, ... m_N\}$, correspond un signal y_k issu d'un système chaotique décrit par:

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_k = x_{k+1} \end{cases} \qquad (02.9)$$

où $i \in \{1, ..., N\}$, x_k est le vecteur d'état, y_k la sortie. Le cas le plus simple correspond à une information binaire. Dans ce cas, seulement deux systèmes émetteur, avec $i = \{1,2\}$, sont nécessaires, l'un correspondant à $m_1 = 0$ et l'autre à $m_2 = 1$.

La figure suivante illustre la modulation chaotique:

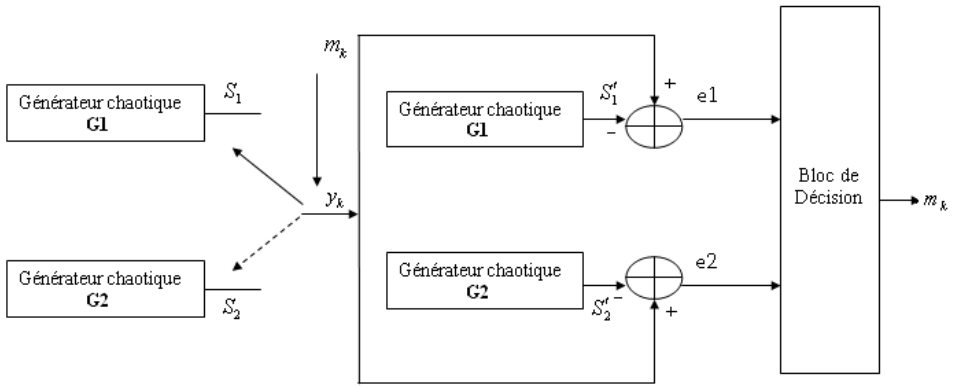


Fig.02.3. Modulation chaotique

Le rôle du récepteur est de détecter quel émetteur a produit la sortie y_k. Pour cela, le récepteur est composé d'autant de systèmes que l'émetteur, décrits par:

$$\begin{cases} x'_{k+1} = f'_i(x'_k) \\ y'_k = x'_{k+1} \end{cases}, \quad i = 1,\ldots,N \qquad (02.10)$$

2.4.3. Modulation paramétrique

La modulation paramétrique consiste à moduler un ou plusieurs paramètres du générateur de chaos par l'information m_k. Il en résulte un "mélange" entre le ou les paramètres du générateur de chaos et l'information.

Le cas le plus simple correspond à une information binaire m_k, où un "1" est codé en transmettant un signal chaotique et un "0" est codé en transmettant un autre signal chaotique, mais peut être étendu à un cas plus général. La figure suivante illustre ce type de modulation:

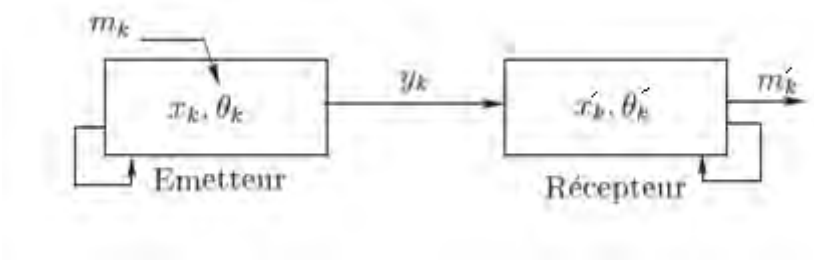


Fig.02.4. Modulation paramétrique

Le système émetteur peut être décrit par la représentation d'état suivante :

$$\begin{cases} x_{k+1} = f(x_k, \theta_k) \\ y_k = x_{k+1} \end{cases} \qquad (02.11)$$

ou x_k est le vecteur d'état, y_k la sortie, θ_k le vecteur des paramètres modulés. Le paramètre θ_k varie dans le temps car il est modulé par l'information m_k **.**

2.5. Quelques développements concernant la cryptographie basée-chaos

Dans [13], Fridrich a suggéré qu'une technique de chiffrement basée-chaos devrait comporter des itérations de deux processus : la confusion et la diffusion, dans son algorithme, la confusion est réalisée en permutant tous les pixels à l'aide d'une carte chaotique 2D Baker. Et la diffusion est faite en altérant les valeurs des pixels séquentiellement et la modification apportée à un pixel particulier dépend de l'effet accumulé de toutes les valeurs des pixels précédents. Cette architecture de confusion-diffusion a formé plus tard, la structure de base pour plusieurs techniques de chiffrement d'images basées- chaos.

Dans [14], Chen et al ont employé une version *3D* de la carte Arnolad's Cat pour la substitution, la carte logistique pour la diffusion et le système chaotique de Chen comme un générateur des clefs. L'algorithme de chiffrement est illustré dans la figure.02.5.

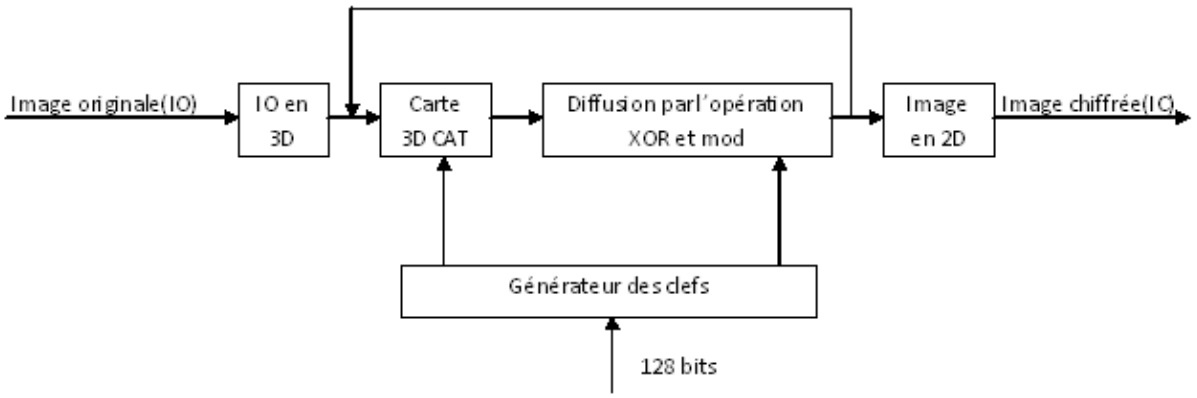


Fig.02.5. l'algorithme de chiffrement de Chen et al

Après la conversion de l'image originale en 3D, la carte 3D Arnolad's Cat definée comme suit :

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \\ Z_{n+1} \end{bmatrix} = A \begin{bmatrix} X_n \\ Y_n \\ Z_n \end{bmatrix} \mod N \qquad (02.13)$$

Où :

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} \qquad (02.14)$$

est employée pour créer la confusion. Ensuite, la formule ci-après est utilisée pour créer la diffusion.

$$c(k) = \Phi(k) \oplus \{[i(k) + \Phi(k)] \mod N\} \oplus c(k-1) \qquad (02.15)$$

Où :

$\Phi(k)$ est généré en utilisant la carte logistique, $i(k)$ représente la valeur du pixel en cours et $c(k)$ est la nouvelle valeur du pixel en cours.

Dans [15] la même idée est utilisée par Mao et al sauf qu'ils ont employé la carte 3D Baker à l'étape de substitution au lieu de la carte 3D Cat.

Après, Lian et al [16] ont prouvé qu'il existe quelques clefs faibles (problème de sécurité) dans les techniques de chiffrement utilisant les cartes chaotiques Baker et Cat, et que l'espace de clef de la carte chaotique standard est assez grand que ces deux dernières cartes. Ils ont utilisé la carte standard pour la substitution et la fonction suivante pour la diffusion :

$$C_i = v_i \oplus q\left[f\left(c_{i-1}\right), L\right] \qquad (02.16)$$

Avec : $$q\left[f\left(c_{i-1}\right), L\right] = 2^L \times f\left(c_{i-1}\right) \qquad (02.17)$$

Où :

V_i représente la valeur du pixel de l'image permutée, C_i désigne la valeur du pixel de l'image diffusée et la fonction f représente la carte logistique.

Ils ont également recommandé au moins quatre rondes de la substitution et de la diffusion.

L'algorithme de Lian et al est bien illustré par la figure.02.6.

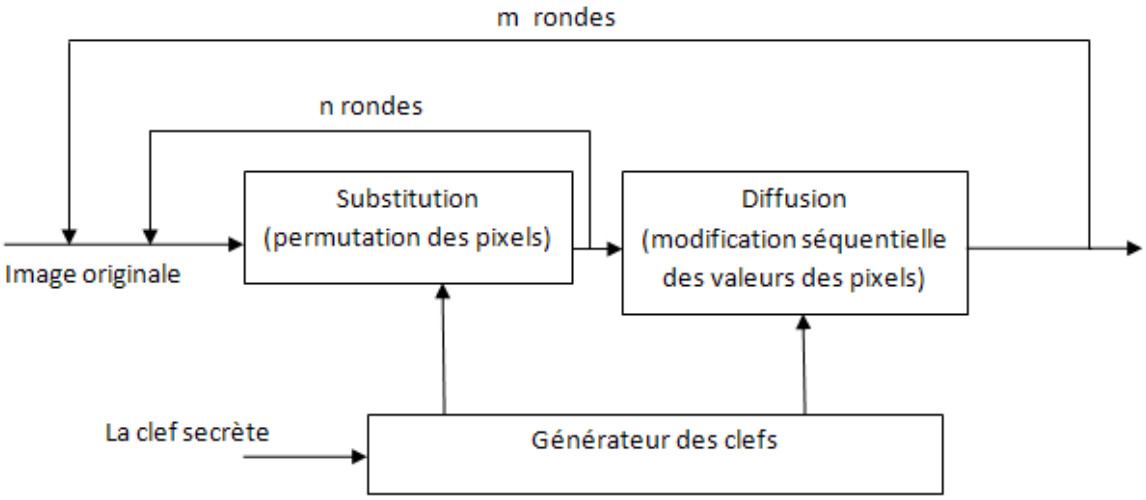


Fig.02.6. l'algorithme de chiffrement de Lian et al

Derrière l'architecture de confusion-diffusion plusieurs autres techniques de chiffrement ont été proposées, V. Patidar et al [17] ont proposé un nouvel algorithme de chiffrement en utilisant la carte chaotique standard et la carte logistique avec une clef secrète de 157 bits pour chiffrer des images couleurs. La condition initiale, le paramètre système de la carte standard et le nombre d'itération constituent ensemble la clef secrète. La première ronde de confusion est effectuée par l'intermédiaire des XORing keys calculé à partir de la clef secrète. Ensuite, dans les deux rondes de diffusion les propriétés des pixels horizontalement et verticalement adjacents sont mélangées respectivement. Dans la quatrième ronde une confusion robuste et efficace est réalisée à l'aide de la carte standard et logistique.

Cet algorithme est bien détaillé dans la figure.02.7.

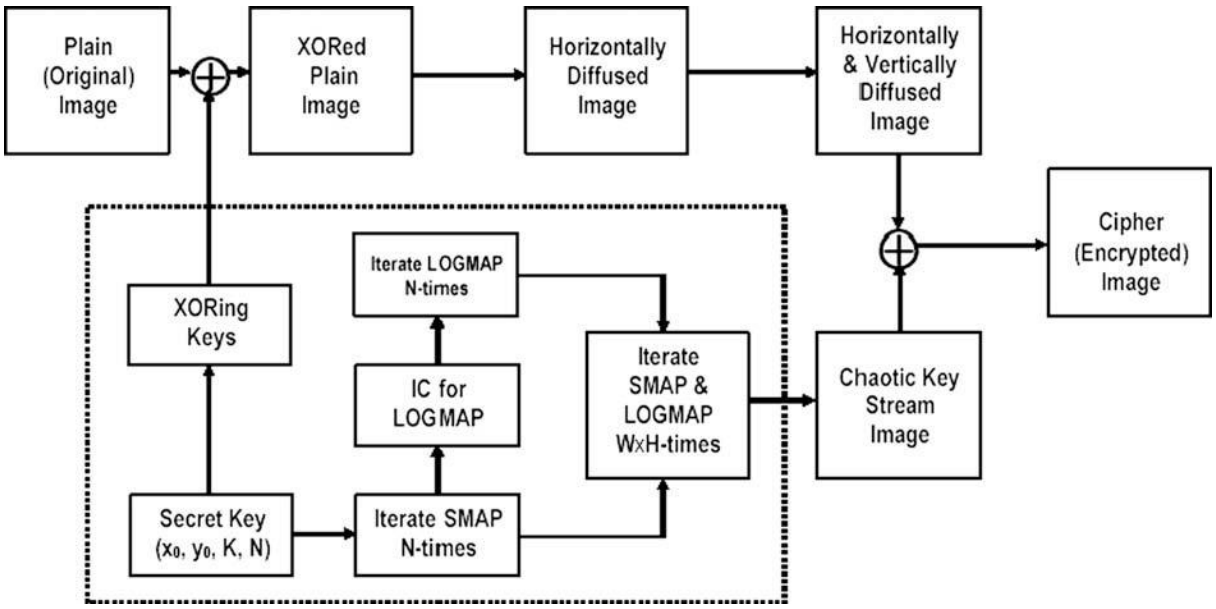


Fig.02.7. l'algorithme de chiffrement de Patidar et al

Lorsqu'un crypto-système est synthétisé, il faut s'assurer qu'il est effectivement robuste face à des attaques pirates. Cette étape de validation est appelée la cryptanalyse. Elle consiste à tester les crypto-systèmes afin de déceler leurs éventuelles faiblesses.

2.6. Cryptanalyse [10, 11]

Alice et Bob essaient de communiquer de façon sécurisée, un adversaire, Charlie, tente de faire échouer la communication secrète entre Alice et Bob. Il peut, par exemple, intercepter le signal transitant sur le canal dans le but de récupérer le texte clair, il peut modifier le signal transitant sur le canal, ou encore il peut se faire passer pour l'une des entités Alice ou Bob. Toutes ces tentatives sont des attaques sur le crypto-système.

La cryptanalyse est l'étude des probabilités de succès des attaques possibles sur les crypto-systèmes afin de déceler leurs éventuelles faiblesses Un des principaux objectifs de la cryptanalyse est de tester si un adversaire peut déchiffrer le texte clair ou récupérer la clé secrète. Pour cela, le cryptanalyste se met à la place de l'adversaire.

La cryptographie et la cryptanalyse sont deux domaines d'études évoluant constamment et en parallèle. En effet, de nouveaux crypto-systèmes, toujours plus complexes, sont développés pour remplacer ceux qui ont été "cassés" par la cryptanalyse et de nouvelles techniques de cryptanalyse sont inventées pour tester

ces nouveaux crypto-systèmes. Le problème de la cryptographie est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire pour "casser" un crypto-système soit supérieure à sa durée de validité. La tendance actuelle est de chercher à prouver la sécurité d'un système sur la base d'hypothèses, sur la puissance de calcul requise ou sur la quantité de texte.

La réussite pratique d'une attaque dépend d'un certain nombre d'éléments, comme les connaissances nécessaires a priori, l'effort demandé (complexité, temps de calcul), la quantité et la qualité des informations pouvant être déduites de l'attaque (déchiffrement de la clé secrète, algorithme de chiffrement découvert sans connaître la clé secrète, informations sur le texte clair, ...).

La complexité de l'attaque se caractérise par le temps en nombre d'opérations effectuées (addition, XOR, ...), par la mémoire nécessaire et par la quantité de données (texte clair et texte chiffré) requises.

A travers les années, de nombreuses attaques possibles contre les crypto-systèmes ont été identifiées, de telle sorte qu'il est difficile d'en établir une liste exhaustive. En revanche, on distingue deux classes d'attaques : les attaques actives et les attaques passives.

Dans les attaques actives, l'adversaire agit sur l'information. Il altère l'intégrité des données, l'authentification et la confidentialité. Il peut chercher à altérer la transmission du message sur le canal, par exemple, en modifiant le message (suppression, ajout, modification des séquences du message), en retardant (ou empêchant) sa transmission, en répétant son envoi.

Dans les attaques passives, l'adversaire observe des informations qui transitent sur le canal sans les modifier. Il cherche à récupérer des informations sur le crypto-système sans l'altérer, telles que le message, la clé secrète, ... Dans ce cas, l'adversaire touche à la confidentialité des données.

La cryptanalyse des schémas de cryptage peut être effectuée sous un certain nombre d'hypothèses. Une hypothèse fondamentale, connue sous le nom de principe de Kerckhoff est que l'adversaire connaît complètement l'algorithme de cryptage, à l'exception de la clé secrète qui est inconnue. Dans ce cas, la sécurité du crypto-système repose entièrement sur la clé secrète. Cette hypothèse signifie que la sécurité d'un schéma de cryptage ne doit pas reposer sur la confidentialité du schéma, c'est-à-dire la fonction de chiffrement employée, mais sur la confidentialité de la clé.

L'objectif commun de toutes les attaques est de systématiquement retrouver le texte clair à partir de texte chiffré ou de déduire la clé secrète. Ces attaques sont rappelées ci-dessous.

2.6.1. Les différentes classes d'attaques [10, 11]

On distingue, les différents types d'attaques en fonction des données supposées connues par les attaquants**:**

- **L'attaque à texte chiffré seulement (Ciphertext only attack) :** L'attaquant ou (l'adversaire) a connaissance du texte chiffré de plusieurs messages ; alors il tente de déduire la clé secrète ou le texte clair en observant seulement le texte chiffré.

- **L'attaque à texte en clair connu (known plaintext attack) :** Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages mais aussi aux textes en clairs correspondants. La tâche est de retrouver la ou les clef(s) utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clef.

- **L'attaque à texte en clair choisi (chosen plaintext attack) :** Non seulement le cryptanalyste a accès aux textes chiffrés et aux textes en clair mais de plus il peut choisir les textes en clair à chiffrer. Cette attaque est plus efficace que l'attaque à texte en clair connu car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clef. La tâche consiste à retrouver la ou les clefs utilisées pour chiffrer ces messages ou un algorithme qui permette de déchiffrer n'importe quel nouveau message chiffré avec la même clef.

- **L'attaque adaptative à texte en clair choisi (adaptive chosen plaintext attack) :** C'est un cas particulier de l'attaque à texte en clair choisi. Non seulement le cryptanalyste peut choisir les textes en clair mais il peut également adapter ses choix en fonction des textes chiffrés précédents. Dans une attaque à texte en clair choisi, le cryptanalyste est juste autorisé à choisir un grand bloc de texte en clair au départ tandis que dans une attaque à texte en clair adaptative, il choisit un bloc initial plus petit et ensuite il peut choisir un autre bloc en fonction du résultat pour le premier et ainsi de suite (le choix du texte clair peut dépendre du texte chiffré reçu précédemment).
- **L'attaque à texte chiffré choisi (chosen ciphertext attack) :** Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique, sa tâche est de retrouver la clef.

- **L'attaque adaptative à texte chiffré choisi (adaptive chosen ciphertext attack) :** Cette attaque est une attaque à texte chiffré choisi où le choix du texte chiffré peut dépendre du texte en clair reçu précédemment.
- **L'attaque exhaustive ou attaque par force brute (brute force attack) :** L'attaquant essaie toutes les combinaisons possibles des clés jusqu'à l'obtention d'un texte clair. Cette attaque est la plus coûteuse en temps de calcul et en mémoire à cause de la recherche exhaustive.

2.7. Conclusion

Les besoins de sécurité de la vie réelle restent toujours en augmentation. Pour cette raison plusieurs personnes ont développé des systèmes cryptographiques pour réaliser ces besoins.

Dans notre travail on essaie de proposer un cryptosysteme basé sur le chaos qui chiffre et déchiffre des images satellitaires sur chaque bande (images en niveaux de gris). Et avant d'aller plus loin on doit d'abord donner une petite introduction concernant ce type d'images, a cet effet le prochain chapitre aborde ce sujet.

Chapitre 03

Les images satellitaires

3.1. Introduction

La télédétection ou encore l'observation de la terre est la technique qui, par l'acquisition d'images, permet d'obtenir de l'information sur la surface de la Terre sans contact direct avec celle-ci. La télédétection englobe tout le processus qui consiste à capter et à enregistrer l'énergie d'un rayonnement électromagnétique émis ou réfléchi, à traiter et à analyser l'information, pour ensuite mettre en application cette information.

Dans la plupart des cas, la télédétection implique une interaction entre l'énergie incidente et les cibles. Le processus de la télédétection au moyen de systèmes imageurs comporte les sept étapes que nous élaborons ci-après :

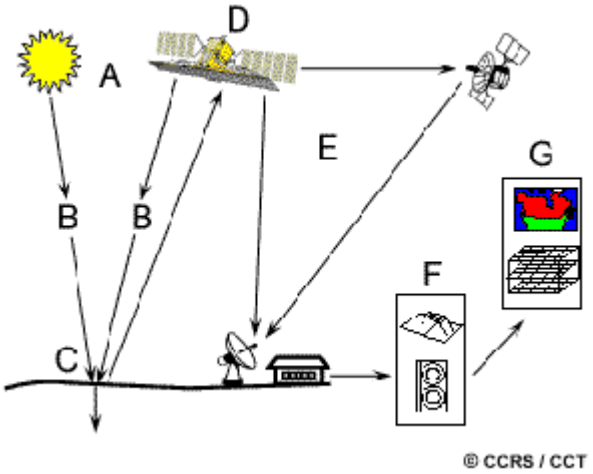


Fig.03.1. le processus de la télédétection.

1. Source d'énergie ou d'illumination (A)

À l'origine de tout processus de télédétection se trouve nécessairement une source d'énergie pour illuminer la cible.

2. Rayonnement et atmosphère (B)

Durant son parcours entre la source d'énergie et la cible, le rayonnement interagit avec l'atmosphère. Une seconde interaction se produit lors du trajet entre la cible et le capteur.

3. Interaction avec la cible (C)

Une fois parvenue à la cible, l'énergie interagit avec la surface de celle-ci. La nature de cette interaction dépend des caractéristiques du rayonnement et des propriétés de la surface.

4. Enregistrement de l'énergie par le capteur (D)

Une fois l'énergie diffusée ou émise par la cible, elle doit être captée à distance (par un capteur qui n'est pas en contact avec la cible) pour être enfin enregistrée.

5. Transmission, réception et traitement (E)

L'énergie enregistrée par le capteur est transmise, souvent par des moyens électroniques, à une station de réception où l'information est transformée en images (numériques).

6. Interprétation et analyse (F)

Une interprétation visuelle et/ou numérique de l'image traitée est ensuite nécessaire pour extraire l'information que l'on désire obtenir sur la cible.

7. Application (G)

La dernière étape du processus consiste à utiliser l'information extraite de l'image pour mieux comprendre la cible, pour nous en faire découvrir de nouveaux aspects ou pour aider à résoudre un problème particulier.

3.2. Vue historique

En 1859 Gaspard Tournachon a pris une photographie d'un petit village près de Paris à partir d'un ballon. Par cette image l'ère de l'observation de la terre et de la télédétection avait commencé. Pendant la guerre civile dans les Etats-Unis, la photographie aérienne à partir des ballons a joué un rôle important pour indiquer les positions de la défense en Virginie. Comme d'autres développements scientifiques et techniques, la guerre civile aux Etats-Unis a accéléré le développement de la photographie et l'utilisation de cette technologie en vols.

La deuxième période des développements rapides de l'observation de la terre a eu lieu en Europe et pas aux Etats-Unis. C'était pendant la Première Guerre Mondiale que des avions ont été utilisés à grande échelle pour la photographie. Les avions sont des plates-formes plus fiables et plus stables pour les observations de la terre que les ballons. Dans la période entre les deux guerres mondiales l'utilisation civile des photos aériennes a été commencée. Les champs d'application des photos aéroportées ont inclus à cette période la géologie, l'agriculture et la cartographie. Ces développements mènent à l'amélioration des appareils-photos et aux équipements d'interprétation. Les développements les plus importants de la photographie aérienne et de l'interprétation des photos ont eu lieu pendant la deuxième guerre mondiale. Pendant cette période autres systèmes d'imageries tels que la photographie en infrarouge, la détection thermique et le radar sont développés. La photographie en infrarouge et l'infrarouge thermique sont très efficaces dans la séparation de la vraie végétation du camouflage. Le premier radar aéroporté de

l'imagerie n'a pas été utilisé pour des buts civils mais a prouvé sa fiabilité pour le bombardement de nuit et a été développé en Grande-Bretagne en 1941.

Après les guerres dans les années 50 les systèmes de télédétection ont continué d'évoluer à partir des systèmes développés pour les efforts de la guerre.

Au début des années 60 les États-Unis ont commencé à placer des télédétecteurs dans l'espace pour l'observation de la météo et plus tard pour des observations de la terre. TIROS (Television Infrared Observation Satellite) était le premier satellite météorologique. Une longue série de satellites météorologiques a suivi celui-ci. 1960 était également le commencement d'un projet militaire de reconnaissance d'image appelé Corona. En 1970 le programme TIROS a été renommé NOAA (National Oceanic and Atmospheric Administration). Jusqu'à aujourd'hui le NOAA AVHRR (Very High Resolution Radiometer) collecte des informations sur la météo en longueur d'ondes visibles, proche infrarouges et thermiques. NOAA-17 a été lancé le 24 juin 2002. Les années 50 et les années 60 étaient également importantes pour le développement organisationnel de la télédétection. Des divers organismes civils et des universités sont devenus fortement intéressés par ces nouvelles technologies. Et comme conséquence plusieurs organismes professionnels et journaux de télédétection sont apparus tels que IEEE Transactions on Geoscience and Remote Sensing, International Journal of Remote Sensing, Remote Sensing of Environment and Photogrammetric Engineering.

Au début des années 70 le premier satellite spécifiquement conçu pour rassembler des données de la surface terrestre et ses ressources a été développé et lancé : ERTS-1 Earth Resources Technology Satellite-One. Plus tard, en 1975, ce programme a été renommé Landsat. Ce premier satellite de ressources terrestres était en fait un satellite de météo modifié (Nimbus) portant deux types de détecteurs (MSS, RBV).

Landsat 2 et 3 ont été lancés en 1975 et 1978, respectivement, et ont porté la même charge utile que le premier satellite de cette série. La charge utile a été changée en 1982 avec Landsat 4, un détecteur plus avancée techniquement (TM) a remplacé le RBV. Une conception améliorée du TM (ETM+) a été montée sur Landsat 7 et lancée en 1999.

Diverses autres missions d'observation de la terre suivent le programme de Landsat sont menées par d'autres pays. En 1978 le gouvernement Français a décidé de développer son propre programme d'observation de la terre. Ce programme a eu comme conséquence le lancement du premier satellite SPOT en 1986. Avec la conception originale de SPOT (trois bandes spectrales) un nouveau détecteur appelée Végétation a été ajoutée au SPOT-4 en 1998. D'autres missions d'observation de la terre sont le programme indien de télédétection (IRS) commencé en 1988, les séries russes Resurs lancées la première fois en 1985 et les ADEOS japonais mis en orbite en

1996. L'agence spatiale européenne (ESA) a lancé son premier satellite de télédétection, ERS-1, en 1991 et ERS-2 en 1995. En mars 2002, l'ESA a lancé Envisat-1 un satellite d'observation de la terre avec une charge utile impressionnante de 13 instruments.

Un développement récent important est le lancement des systèmes d'observation de la terre à haute résolution tels que IKONOS et QuickBird. Ces systèmes ont des systèmes multi spectraux avec une résolution spatiale de 4 mètres ou plus. IKONOS a également un mode panchromatique (0.45- 0.90 μm) avec une résolution spatiale de 1 m. Avec IKONOS, QuickBird et les systèmes semblables, la télédétection spatiale approche la qualité de le photographie aéroportée. [18]

3.3. Satellites et capteurs pour la télédétection

Des images prises à distance de la terre sont capturées par des satellites ou par des avions pour être utilisés dans les domaines agricole, hydrologique, géologique, militaires et beaucoup d'autres applications. Parmi ces systèmes de satellite il existe NOAA AVHRR, le module de balayage multi spectral (MSS) et TM (thematique mapper) de LANDSAT, SPOT (satellite pour l'observation de la terre), et le RADAR (Radio Detection and Ranging).

3.3.1. NOAA AVHRR

Les satellites NOAA (National Oceanic and Atmospheric Administration) ont été conçus par la NASA pour fournir à United States National Weather Service des images fréquentes et à petite échelle de la surface de la Terre et de la couverture des nuages. Ces satellites, en orbite polaire héliosynchrone (830 à 870 km au-dessus de la Terre), font partie de la série Advanced TIROS (datant du début des années 1960). Ils complètent l'information fournie par les satellites géostationnaires (GOES). Les deux satellites, dont chacun produit une couverture totale de la Terre, travaillent conjointement pour assurer que les données de toutes les régions de la Terre soient mises à jour au moins toutes les six heures. Un satellite croise l'équateur du nord au sud, tôt le matin, et l'autre le croise dans l'après-midi.

À bord des satellites NOAA se trouve le capteur primaire AVHRR (Advanced Very High Resolution Radiometer). Celui-ci est utilisé pour la météorologie et pour l'observation à petite échelle de la surface de la Terre. Le capteur AVHRR capte le rayonnement électromagnétique du visible, proche IR, du moyen IR et de l'IR thermique. La fauchée au sol mesure 3000 km. Le tableau suivant décrit les bandes AVHRR, leurs longueurs d'onde, leurs résolutions spatiales (au nadir) et leurs applications générales. [19]

Tableau.03.1. bandes de NOAA AVHRR.

bande	Domaine spectrale (μm)	Résolution spatiale	Application
1	0,58 – 0,68 (rouge)	1,1 km	Surveillance des nuages, de la neige et de la glace
2	0,725 – 1,1 (PIR)	1,1 km	Surveillance de l'eau, de la végétation et de l'agricole
3	3,55 – 3,93 (MIR)	1,1 km	Température de la surface des océans, volcans, feux de forets
4	10,3 – 11,3 (IR thermique)	1,1 km	Température de la surface des océans, humidité du sol
5	11,5 – 12,5 (IR thermique)	1,1 km	Température de la surface des océans, humidité du sol

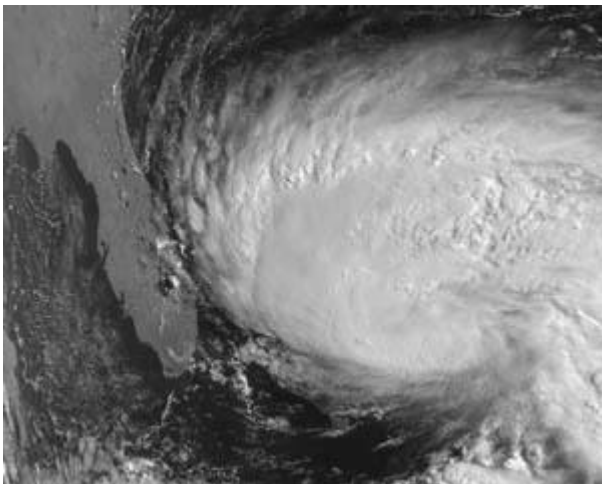


Fig.03.2.Image capturée par NOAA AVHRR

3.3.2. LandSat

Bien que plusieurs satellites météorologiques (comme celui décrit dans la section précédente) soient également utilisés pour la surveillance de la surface de la Terre, ceux-ci n'ont pas été conçus pour la cartographie détaillée de la surface terrestre. Suite aux succès éclatants des premières images des satellites météorologiques dans les années 60, et par les images acquises lors des missions spatiales habitées, le premier satellite l'observation Landsat-1 a été lancé par la NASA en 1972. Connu à l'origine sous l'acronyme ERTS-1 (Earth Resources Technology Satellite), Landsat avait été conçu pour tester la faisabilité d'une plate-forme multispectrale d'observation de la Terre non habitée. Depuis, le programme Landsat a permis l'acquisition de données sur tous les coins de la planète. En 1985, le

programme a été commercialisé pour fournir des données aux divers utilisateurs civils.

Parmi les facteurs qui ont contribué au succès de Landsat, il faut mentionner une combinaison de capteurs avec des domaines spectraux façonnés pour l'observation de la Terre, une résolution spatiale fonctionnelle et une bonne couverture du globe (fauchée et répétitivité). La longévité du programme a permis d'accumuler des archives de données volumineuses sur les ressources terrestres, ce qui facilite la surveillance à long terme ainsi que le maintien des données historiques et de la recherche. Tous les satellites Landsat ont été placés en orbite héliosynchrone polaire. Les trois premiers satellites (Landsat-1 à Landsat-3) se situaient à une altitude de 900 km avec une répétitivité de 18 jours, tandis que les derniers orbitent à une altitude approximative de 700 km avec une répétitivité de 16 jours. Tous les satellites Landsat croisent l'équateur le matin pour profiter des conditions d'illumination optimales.

Les satellites de la série Landsat portent plusieurs capteurs comme les systèmes de caméras RBV (Return Beam Vidicon), le système MSS (Multi Spectral Scanner), et plus tard, le TM (Thematic Mapper). Chacun de ces capteurs a une fauchée de 185 km.

Le MSS capte le rayonnement électromagnétique de la surface de la Terre provenant de quatre bandes spectrales. Chaque bande possède une résolution spatiale de 60 sur 80 mètres, et une résolution radiométrique de 6 bits, ou de 64 valeurs numériques. Le MSS capte le rayonnement avec un balayeur mécanique qui utilise un miroir oscillant. Six lignes de balayage peuvent être recueillies simultanément à chaque balayage. [19]

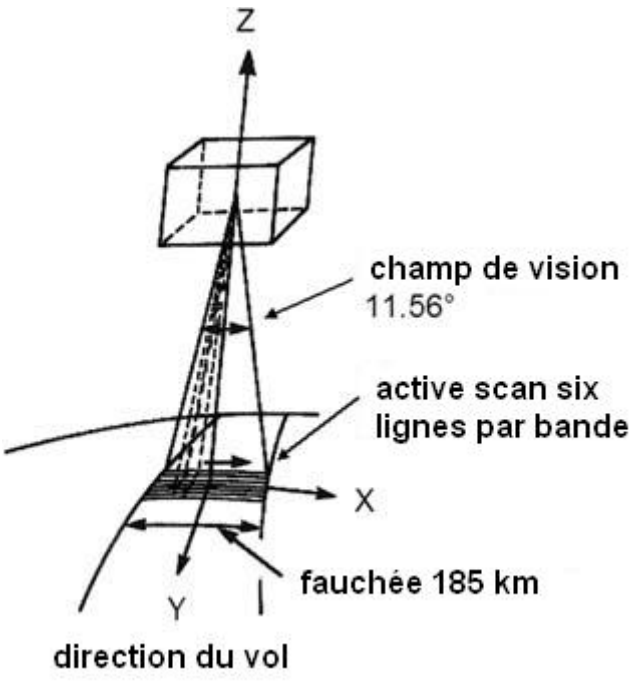
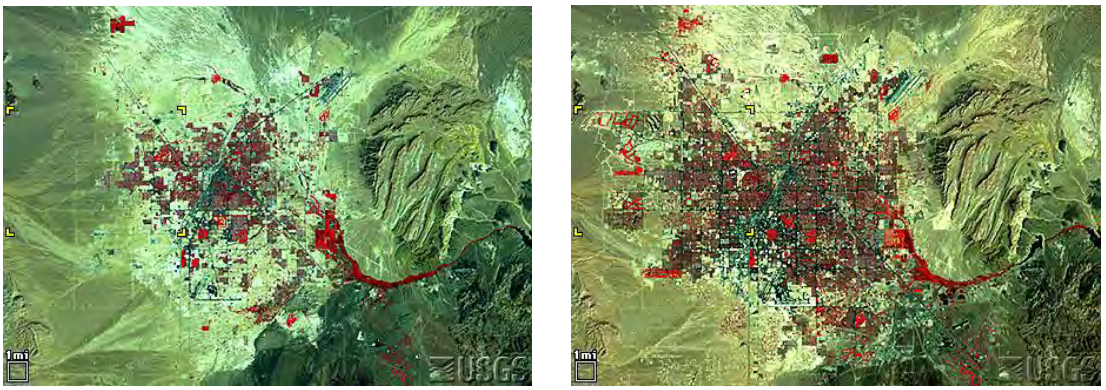


Fig.03.3. Landsat Multispectral Scanner (MSS)

Le tableau suivant décrit les domaines spectraux des bandes MSS.

Tableau.03.2. Bandes MSS.

bandes		Longueurs d'ondes (µm)
Landsat 1, 2, 3	**Landsat 4, 5**	
MSS 4	MSS 1	0,5 – 0,6 (vert)
MSS 5	MSS 2	0,6 – 0,7 (rouge)
MSS 6	MSS 3	0,7 – 0,8 (PIR)
MSS 7	MSS 4	0,8 – 1,1 (PIR)



(a) (b)

Fig.03.4. Images de Las Vegas, Nevada captées par Landsat MSS (a) Image de Landsat 1 MSS captée en 13 Septembre 1972 sur les bandes 4,2 et 1, (b) Image de Landsat 5 MSS captée en 10 Septembre 1992 sur les bandes 4,2 et 1.

Le capteur TM porté par Landsat 4 lancé le 16 juillet 1982 apporte plusieurs améliorations : une meilleure résolution spatiale et radiométrique, des bandes spectrales plus étroites, sept bandes spectrales par rapport à quatre pour le MSS, et une augmentation du nombre de détecteurs par bandes (seize pour les bandes non thermiques par rapport à six pour MSS). Seize lignes de balayage sont captées simultanément pour chaque bande spectrale non thermique (quatre pour les bandes thermiques). Les seize lignes sont captées simultanément à l'aide d'un miroir oscillant qui balaie à l'aller de l'ouest vers l'est et au retour de l'est vers l'ouest. La limite de résolution spatiale du TM est de 30 m pour toutes les bandes, sauf l'infrarouge thermique qui est de 120 m. Toutes les bandes sont enregistrées sur une étendue de 256 valeurs numériques (8 octets). Le tableau suivant décrit la résolution spectrale des bandes individuelles TM et leurs applications. [19]

Tableau.03.3. Bandes TM.

Bandes	Domaine spectral (μm)	application
TM 1	0,45 – 0,52 (bleu)	Discrimination entre le sol et la végétation, identification des traits culturels et urbains
TM 2	0,52 – 0,60 (vert)	Cartographie de la végétation verte, identification des traits culturels et urbains
TM 3	0,63 – 0,69 (rouge)	Discrimination entre les espèces de plantes a feuilles et sans feuilles (absorption de chlorophylle), identification des traits culturels et urbains
TM 4	0,76 – 090 (PIR)	Identification des types de végétation, et de plante, délimitation des étendues d'eau, humidité dans le sol
TM 5	1,55 – 1,75 (MIR)	Sensible à l'humidité dans le sol et les plantes, la discrimination entre la neige et les nuages
TM 6	10,4-12.5 (IR thermique)	Cartographie thermique, discrimination de la végétation, et de l'humidité dans le sol
TM 7	2,08 – 2,35	Discrimination entre les minéraux et les types de roches

Les données des capteurs TM et MSS sont utilisées pour plusieurs applications comme la gestion des ressources, la cartographie, la surveillance de l'environnement etc.

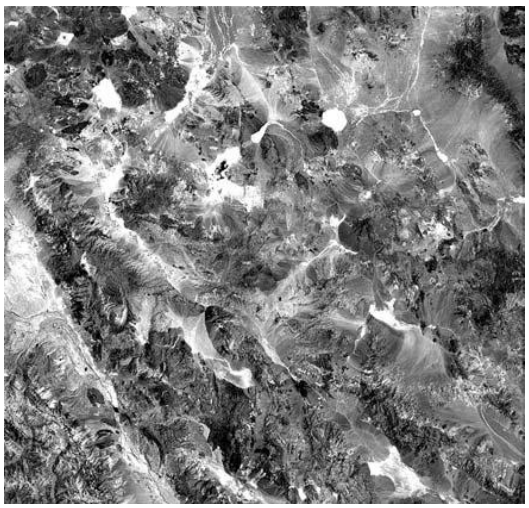


Fig.03.5. Image de Gold field Nevada captée par Landsat ETM+

3.3.3. SPOT

Le système SPOT (Système pour l'observation de la Terre) est une série de satellites d'observation de la Terre qui ont été conçus et lancés par le Centre National d'Études Spatiales (CNES) de la France, avec l'aide de la Belgique et de la Suède.

SPOT-1 a été lancé en 1986, et a été suivi d'autres satellites lancés tous les trois ou quatre ans. Tous les satellites sont en orbite héliosynchrone polaire à une altitude de 830 km, ce qui produit une répétitivité de 26 jours. Ils croisent l'équateur vers 10h30 heure solaire locale. Conçu dans le but d'acquérir des données de télédétection à des fins commerciales, SPOT a été le premier satellite à utiliser la technologie du balayage à barrettes ou balayage longitudinal.

Tous les satellites SPOT ont deux balayeurs multi-bandes HRV (haute résolution visible) à barrettes, qui peuvent être opérés indépendamment ou simultanément. Chaque HRV peut capter en mode panchromatique (une seule bande) et offre une excellente limite de résolution spatiale de 10 m. Ils peuvent aussi capter en mode multi-bande (trois bandes) qui offre une résolution spatiale de 20 m. Chaque balayeur à barrettes est composé de quatre rangs linéaires de détecteurs : un de 6 000 éléments pour l'enregistrement en mode panchromatique, et un de 3 000 éléments pour chacune des trois bandes multi-spectrales. La fauchée pour les deux modes est de 60 km à partir du nadir. Le tableau suivant décrit les caractéristiques spectrales des deux modes. [19]

Tableau.03.4. Caractéristiques spectrale des deux modes du SPOT.

Mode/ Bande	Domaine spectral (µm)
Panchromatique	0,51 – 0,73 (bleu-vert-rouge)
Multi-spectral	
Bande 1	0,50 – 0,59 (vert)
Bande 2	0,61 – 0,68 (rouge)
Bande 3	0,79 – 0,89 (PIR)

Fig.03.6. Image captée par SPOT HRV.

3.3.4. IRS

La série des satellites IRS (Indian Remote Sensing satellite) combine les caractéristiques des capteurs de Landsat MSS et TM et du capteur HRV de SPOT. Le troisième satellite de la série, IRS-1C, lancé en décembre 1995, a trois capteurs : une caméra de haute résolution panchromatique à une bande (PAN), le capteur à quatre bandes LISS-III (Linear Imaging Selfscanning Sensor) de résolution moyenne, et le capteur à deux bandes WiFS (Wide Field of View) de faible résolution. Le tableau suivant décrit les caractéristiques de chaque capteur.

Tableau.03.5. Capteurs de IRS.

capteur	Domaine spectrale (μm)	Résolution spatiale	Largeur de la fauchée	Répétitivité
PAN	0,5 – 0,75	5,8 m	70 km	24 jours
LISS-II				
Vert	0,52 – 0,59	23 m	142 km	24 jours
Rouge	0,62 – 0,68	23 m	142 km	24 jours
PIR	0,77 – 0,86	23 m	142 km	24 jours
MIR	1,55 – 1,70	70 m	148 km	24 jours
WIFS				
Rouge	0,62 - 068	188 m	774 km	5 jours
PIR	0,77 – 0,86	188 m	774 km	5 jours

Les données à haute résolution sont utiles pour les applications comme la planification urbaine et la cartographie. Les quatre bandes multi-spectrales LISS-III ressemblent aux bandes 1 à 4 du capteur TM de Landsat. Celles-ci sont utiles pour la discrimination de la végétation, la cartographie terrestre, et pour la gestion des ressources naturelles. Le capteur WiFS est semblable aux bandes AVHRR de NOAA. La résolution spatiale de ce capteur ainsi que son recouvrement sont utilisés pour la surveillance de la végétation à l'échelle régionale. [19]

3.3.5. Nimbus CZCS

Le satellite Nimbus-7, lancé en 1978, portait le CZCS (Coastal Zone Colour Scanner), le premier capteur spécifiquement conçu pour la surveillance des océans et des étendues d'eau. Le principal objectif de ce capteur était d'observer la couleur et la température de l'océan, particulièrement dans les régions côtières. La résolution spatiale et spectrale permettait de détecter les polluants dans les couches supérieures de l'océan et de déterminer la nature des matériaux en suspension dans la colonne d'eau. Le satellite Nimbus-7 a été placé en orbite héliosynchrone polaire à une altitude de 955 km. Les heures de passage à l'équateur étaient fixées à midi heure locale pour les passes ascendantes, et à minuit heure locale pour les passes descendantes. Le cycle de répétition du satellite permettait une couverture complète

de la Terre tous les six jours. Le capteur CZCS avait six bandes spectrales dans les parties visible, proche infrarouge, et infrarouge thermique du spectre, chacune recueillant des données à une résolution spatiale de 825 m au nadir, sur une largeur de fauchée de 1566 km. Le tableau suivant décrit les longueurs d'onde de chaque bande et le paramètre primaire mesuré par chacune.

Tableau.03.6. Bandes spectrales CZCS.

bandes	Domaines spectral (μm)	Paramètre primaire mesuré
1	0,43 – 0,45	Absorption de chlorophylle
2	0,51 – 0,53	Absorption de chlorophylle
3	0,54 – 0,56	Gelbstoffe (substance jaune)
4	0,66 – 0,68	Concentration de chlorophylle
5	0,70 – 0,80	Végétation de surface
6	10,5 – 12,50	Température de surface

Les quatre premières bandes du capteur CZCS sont très étroites. Elles ont été optimisées pour permettre la discrimination détaillée des différences de réflectance de l'eau causées par les particules en suspension dans l'eau. En plus de détecter la végétation à la surface de l'eau, la bande 5 était utilisée pour différencier l'eau de la terre. [19]

3.3.6. RADAR

Le RADAR (Radio Detection and Ranging) est un système actif qui fournit sa propre source d'énergie électromagnétique. Les détecteurs, qu'ils soient aéroportés ou spatioportés, émettent de la radiation micro-onde dans une série d'impulsions à partir d'une antenne qui est positionnée vers la surface. Lorsque l'énergie atteint la cible, une portion de l'énergie est réfléchie vers le détecteur. La dispersion de la radiation micro-onde est alors détectée et mesurée. Le temps requis par l'énergie pour se rendre à la cible et retourner au détecteur détermine la distance de la cible. En enregistrant le délai et l'amplitude de l'énergie réfléchie par toutes les cibles lors du passage du système, nous pouvons produire une image à deux dimensions de la surface.

Puisque le RADAR a sa propre source d'énergie, nous pouvons obtenir des images le jour ou la nuit. Puisque l'énergie micro-onde peut également pénétrer à travers les nuages et la pluie, le RADAR est considéré comme un détecteur toutes saisons. [19]

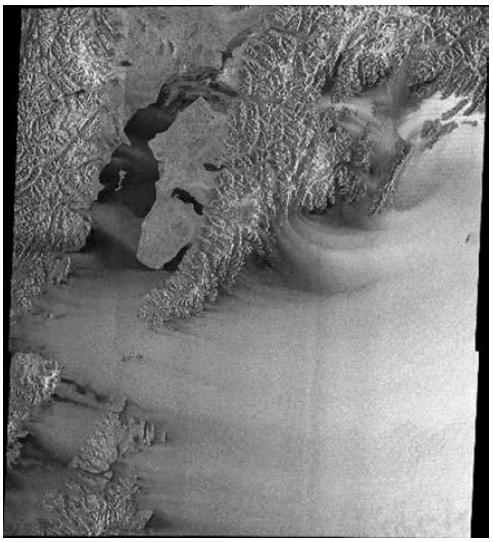


Fig.03.7. Image de sud d'Alaska captée en 1996 par RADARSAT

3.3.7. Caméras vidéo

Les caméras vidéo sont un moyen utile et peu coûteux pour acquérir des données et des images avec annotation verbale. Par contre, la résolution spatiale est plus grossière que pour la photographie et les images numériques. La gestion de désastres naturels (feux, inondations), l'évaluation des moissons et des maladies, le contrôle de danger environnemental et la surveillance policière sont tous des exemples d'applications. Les caméras utilisées pour l'enregistrement vidéo mesurent la radiation dans les plages du visible, du proche infrarouge et parfois dans la portion de l'infrarouge moyen du spectre électromagnétique. Les données de l'image sont enregistrées sur bande magnétique et peuvent être immédiatement visualisées.[19]

3.4. Propriétés des données numériques de télédétection

3.4.1. Données Digitales

Les images numériques sont des tableaux des nombres c-à-d représentées logiquement par des matrices. Les valeurs des nombres stockés dans les éléments du tableau se situent dans une gamme spécifique, généralement limitée à l'intervalle 0-255. La valeur 0 indique le manque de la couleur associée (rouge, vert ou bleu), et la valeur 255 est le niveau le plus lumineux auquel cette couleur est affichée.

La figure.03.8 montre une image numérique d'un œil humain, avec une section d'un tableau des nombres (valeurs des pixels) correspondant à la partie de l'image décrite par le rectangle blanc. L'image de la figure.03.8 est une image en niveaux de gris, et ainsi seulement un tableau de nombres est exigé pour les valeurs des pixels,

qui peuvent prendre l'un de 256 niveaux lumineux s'étendant de 0 (noir) à 255 (blanc). Une image en niveau de gris a seulement un composant - les niveaux du gris - tandis qu'une image couleur a trois composantes.

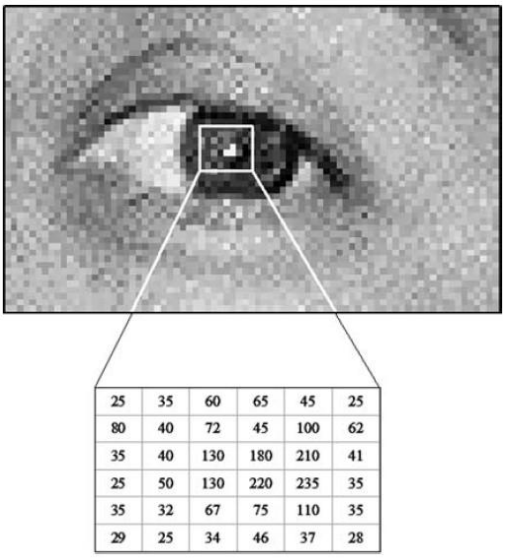


Fig.03.8. Image d'un œil humain montrant la correspondance entre les niveaux de gris et la représentation numérique.

Comme déjà noté, une image couleur est produite en employant trois tableaux numériques, tenant les valeurs des pixels et qui représentent les niveaux des trois couleurs primaires de la lumière (la figure.03.9). Les niveaux 0,… 255 représentent la gamme de chaque couleur primaire de 0 (noir) à 255 (intensité maximale de rouge, de vert, ou de bleu). Les différentes combinaisons de RG et de B produisent les couleurs du spectre, comme démontré par l'expérience célèbre de monsieur Isaac Newton. Les couleurs primaires de la lumière sont additives par exemple le rouge + le vert = le jaune.

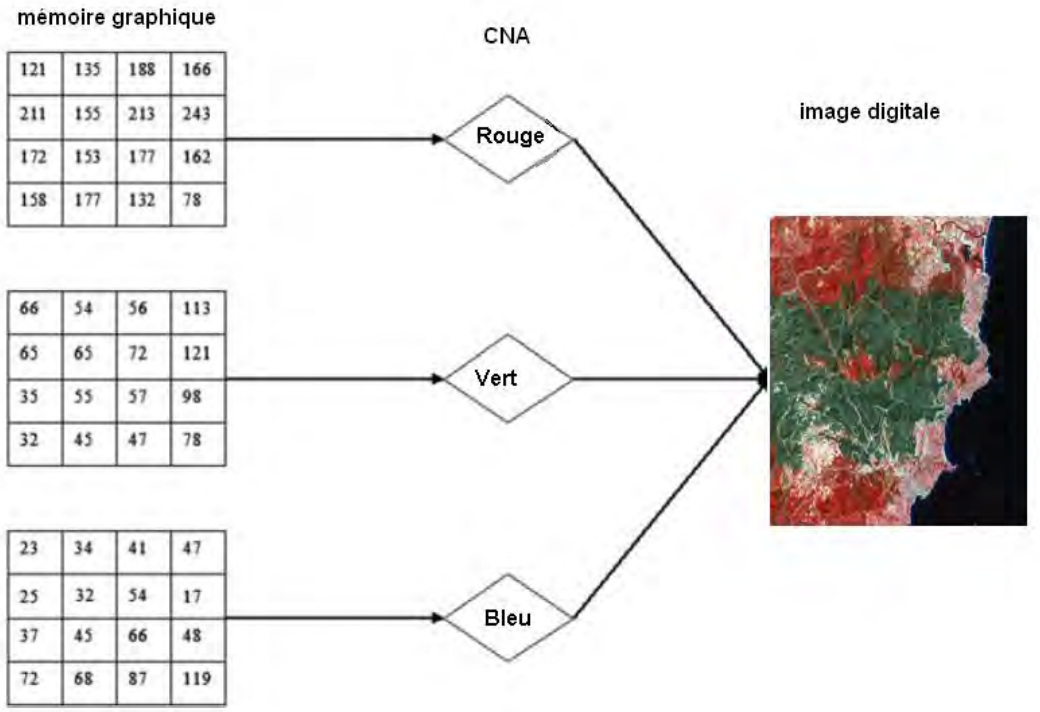


Fig.03.9. Image couleur générée en utilisant trois tableaux d'intensité de couleur

En revanche, les couleurs utilisées dans l'impression sont soustractives, c'est pourquoi une imprimante à jet d'encre emploie l'encre cyan, magenta et jaune. Le tableau.03.7 énumère quelques exemples de couleurs produites en ajoutant différentes proportions de R, G et de B. Noter que les combinaisons de RGB dans lesquelles les niveaux du rouge, du vert et du bleu sont égaux produits des nuances de gris.

Tableau.03.7. Les différentes combinaisons générées par les couleurs primaires de la lumière.

Intensité rouge	Intensité verte	Intensité bleue	Nom du couleur
255	255	0	jaune
0	255	255	cyan
255	0	255	magenta
127	0	0	Mid-rouge
127	127	127	Mid-gris
0	0	0	noir
255	255	255	blanc
241	0	171	violet
255	155	50	orange

Toutes les images de télédétection n'ont pas des valeurs de pixels qui se situent dans la gamme 0-255. Par exemple, les données d'AVHRR utilisent une gamme de 0-1023 (10 bits). Les pixels d'IKONOS se situent dans la gamme 0-2047 (11 bits), et les bandes thermiques des images d'ASTER sont mesurées sur une échelle de 0-4095 (12 bits). [20]

Les valeurs stockées dans les cellules des tableaux sont représentées électroniquement par une série de chiffres binaires (base deux). Dans la base deux les numéros décimaux 0, 1, 2, 3 sont écrits en tant que 0, 1, 10, 11. Si huit éléments binaires sont employés pour enregistrer la valeur de chaque pixel, alors 0 et 255 sont représentés par 00000000 et 11111111. Ainsi, huit éléments binaires (bits) sont nécessaires pour représenter les 256 nombres dans la gamme 0-255. Puisque huit bits sont nécessaires pour représenter la gamme de chacune des trois couleurs primaires, l'image résultante appelée une image du `24-bits'. Il existe d'autre représentation des données des pixels. Par exemple, une image de simple-bande de 10 bits par pixel fournit 1024 niveaux de gris.

La plupart des moniteurs d'ordinateur exigent un signal d'entrée analogique, ainsi les valeurs numériques (discrètes) tenues dans la mémoire graphique sont converties en forme analogique, par un convertisseur numérique-analogique (CNA) comme illustré dans la fig.03.9.

Il est important de mentionner que le nombre de bits par pixel dans la mémoire graphique est fixé à huit bits par le matériel. Cependant, il existe des images de télédétection ont une représentation des valeurs des pixels sur 10 bits, 12 bits, 16 bits. Et donc l'apparence de ces images sur moniteur est fortement affectée par le choix de la méthode de mapping (transformation) des valeurs des pixels de l'image source à la forme de huit bits.

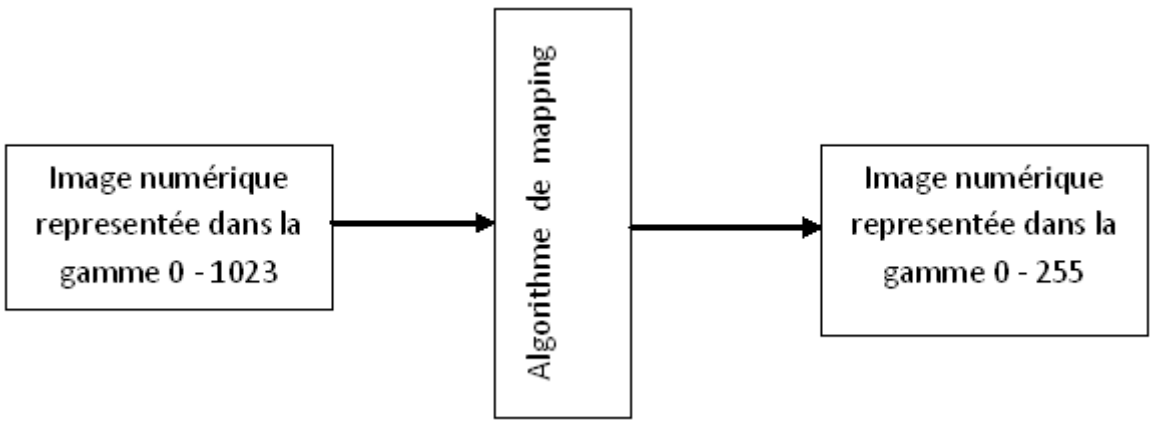


Fig.03.10. Méthodes de mapping

Il y a principalement deux méthodes de mapping employées pour transformer la structure de représentation des valeurs des pixels d'une image à la forme de huit bits. [20]

La première méthode prend la valeur numérique de chacune des trois couleurs, et effectue une mapping entre l'entrée et la sortie, utilisant la formule suivante :

$$\text{sortie} = \frac{(\text{entrée} - \text{entrée}_{\min})}{\text{entrée}_{\max} - \text{entrée}_{\min}} \times 255 \qquad (03.1)$$

Où la sortie est une valeur entre 0 et 255, l'entrée$_{max}$ et l'entrée$_{min}$ sont les valeurs maximale et minimale des pixels de l'image source respectivement, et l'entrée est la valeur du pixel de l'image à convertir. Par exemple, si les valeurs minimale et maximale des pixels de l'image source sont 139 et 2409 respectivement, alors la valeur placée dans la mémoire graphique quand l'entrée égale 1500 est 152. Cette méthode peut provoquer un manque du contraste. Par exemple, 99% des valeurs de pixel dans une image source peut se situer dans la gamme 1290-1879, et a les valeurs minimale et maximale 5 et 2009 respectivement. La valeur 1290 est transformée à la valeur 164 utilisant l'équation (1), alors que la valeur 1879 devient 238 (utilisant toujours l'équation (1)). Par conséquent, 99% des pixels de l'image source sont mappés dans l'intervalle 164-238 de la gamme 0-255, ainsi l'image résultante présente un manque de contraste et une grande partie de la gamme 0-255 est restée inutilisée. Cependant, cette transformation est réversible.

La deuxième méthode employée pour transformer la structure de représentation des valeurs des pixels de l'image source à la forme de huit bits s'appelle l'Égalisation. Les valeurs des pixels de l'image source sont groupées en 256 classes. Les 256 classes ont des fréquences égales plutôt que des intervalles (gamme) égaux (la figure.03.11). Par rapport à l'approche précédente, l'égalisation produit généralement une image de grand contraste. Cependant, plusieurs valeurs d'entrée peuvent être mappées à la même valeur, ainsi la transformation n'est pas réversible.

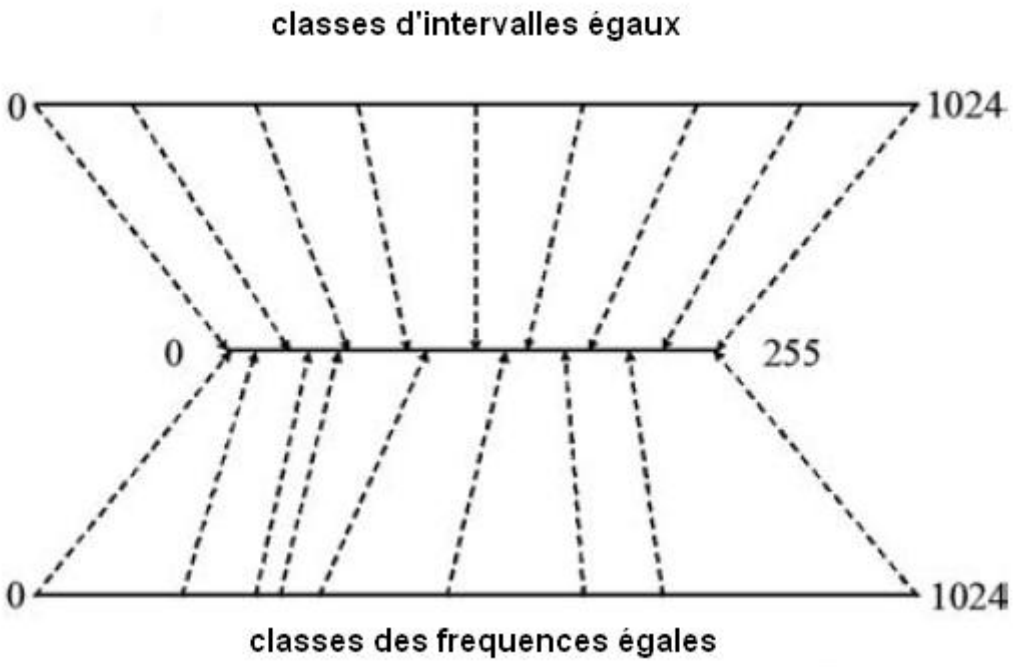


Fig.03.11. Les deux méthodes de mapping.

3.4.2. Les différents types d'images

D'une façon générale, trois types d'images peuvent être stockés dans la mémoire graphique et affichés sur écran. Ces types sont : les images couleurs, les images en niveau de gris (greyscale images) et les images classifiées (labelled images). Les images couleur peuvent être l'un des trois types. Le premier type appelé image des couleurs vraies (des couleurs naturelles), se compose de trois composants représentant les couleurs du monde réel (la bande rouge visible, verte visible et bleue visible (par exemple, les bandes 3, 2 et 1 de Landsat ETM+) Les images des couleurs vraies sont les mêmes que les images couleurs ordinaires des photographies. Si les trois bandes choisies pour l'affichage ne représentent pas le rouge, le vert et le bleu réel alors le résultat est une image fausse-couleur. Par exemple Les bandes 4, 3 et 1 de Landsat ETM+. Ainsi L'image vue sur l'écran montrerait des variations de la réflectivité proche infra-rouge (bande 4) comme nuances du rouge, et les variations de rouge (bande 3) comme nuances du vert. Le troisième type d'image de couleur est désigné sous le nom d'une image pseudo-couleur, parce qu'il est basé sur des données qui occupent un tableau dans la mémoire graphique, au lieu de trois tableaux. Ceci implique que les valeurs des pixels dans une image pseudo-couleur s'étendent de 0 à 255. Ces 256 niveaux sont associés aux couleurs RGB par l'intermédiaire d'un tableau de couleurs (palette) (look up table « LUT »). Par exemple, le niveau 0 peut être mappé à 255, 0 et 0, respectivement, tandis que le niveau 1 représente le niveau 255, 255 et 0, et ainsi de suite. Dans cette représentation, la valeur du pixel de l'image est envoyée à chacun des trois convertisseurs numérique-analogique en passant par le LUT. Beaucoup de formats de fichier d'image tels que le BMP et le TIF spécifient que, pour une image de 256 niveaux, un tableau de 256 × 3 est spécifié et stocké avec l'image (dans l'entête), c.-à-d. 256 niveaux × rouge, vert et bleu. La distinction entre l'image couleurs vraies, fausse-couleur et pseudo-couleur est montrée dans la figure.03.12.

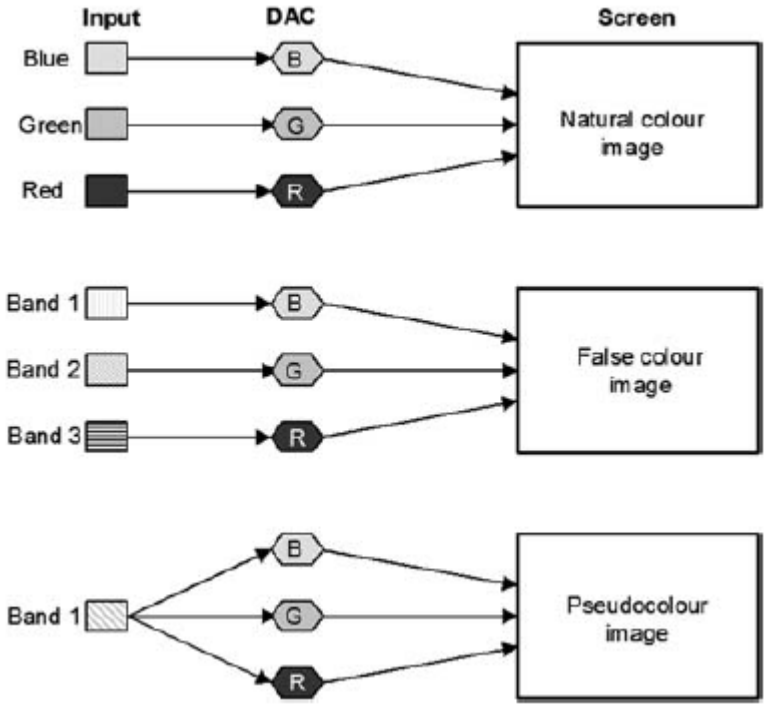


Figure.03.12. Les différents types de l'image couleur

Le deuxième type d'image qui peut être stocké dans la mémoire graphiques et affiché sur écran est appelé une image en niveau de gris. Comme l'image pseudo-couleur, l'image en niveau de gris a seulement une entrée unique (représentant un canal simple). À la différence de l'image pseudo-couleur, pour laquelle les trois CNA produisent des niveaux indépendants du rouge, vert et de bleu, les CNA pour l'image en niveau de gris produisent exactement le même niveau de rouge, vert et de bleu. Rappelons que des valeurs d'intensité égale du rouge, vert et bleu forment en ensemble des nuances de gris. Ainsi, un pixel en niveau de gris d'une valeur 127 est représenté dans le mode RGB par le triple {127, 127, 127}.

Le troisième type d'image est l'image classifiée (labelled image) qui se compose des pixels dont les valeurs représentent une étiquette qui indique une propriété d'une certaine espèce. L'étiquette elle-même n'a aucune signification numérique. Il existe plusieurs méthodes de classifications pour ce type d'image, Ces méthodes permettent d'affecter chaque pixel à une catégorie spécifique, tel que : un type particulier des roches. Ces catégories sont décrites par des étiquettes comme `1', `2', ou `3', etc. qui indiquent par exemple l'eau, forêts ou sol. Pour afficher une telle image à l'écran, l'image classifiée est placée d'abord dans la mémoire et les trois CNAs (Rouge, vert et Bleu) sont programmés pour attribuer des valeurs de RGB aux différents pixels (juste comme dans le cas de l'image pseudo-couleur). Par exemple, les valeurs générées par les trois CNAs pour l'étiquette 'l' (l'eau) pourraient être {0, 0, 255} ce qui signifié : aucun rouge, aucun vert et bleu maximale. Et alors tous les pixels de l'eau apparaîtront dans le bleu le plus lumineux. [20]

3.4.3. Formats de données

Un problème que la race humaine n'arrive pas à résoudre est celui de la standardisation. Par exemple, des conducteurs de voiture au royaume-unis, en l'Irlande, en l'Afrique du Sud et au Japon gardent le côté gauche de l'autoroute, alors que les conducteurs du reste du monde gardent le côté droit. L'électricité est fournée à 240 volts au Royaume-Unis, et à 110 volts aux Etats-Unis, alors que les gallons des États-Unis et les gallons Britanniques ne sont pas les même et le reste du monde emploie des litres. Le même problème est constaté pour les données de télédétection où les fournisseurs de ces données fournissent leurs produits dans différents formats. Un format de données décrit la manière dans laquelle les données sont écrites sur un support de stockage. L'ensemble des données peut être stocké dans un format comme :

(i) Un fichier contenant l'ensemble de descriptions numériques et textuelles des données telles que le nombre de lignes de balayage et le nombre de pixel par ligne, la latitude et la longitude etc. cette description est appelée métadonnées. (figure.03.13)

(ii) Un deuxième fichier contenant les valeurs de pixel de l'image.

```
REQ ID =000101072000000000   LOC =196/000FF          ACQUISITION DATE =20010603
SATELLITE =LANDSAT7   SENSOR =ETM+        SENSOR MODE =NORMAL LOOK ANGLE =  0.00
                        LOCATION =                    ACQUISITION DATE =
SATELLITE =           SENSOR =            SENSOR MODE =       LOOK ANGLE =
                        LOCATION =                    ACQUISITION DATE =
SATELLITE =           SENSOR =            SENSOR MODE =       LOOK ANGLE =
                        LOCATION =                    ACQUISITION DATE =
SATELLITE =           SENSOR =            SENSOR MODE =       LOOK ANGLE =
VOLUME #/# IN SET =01/01 PIXELS PER LINE =7368  LINES PER BAND =7036 /7036
START LINE # =      BLOCKING FACTOR =   REC SIZE  =51841248  PIXEL SIZE = 30.00
OUTPUT BITS PER PIXEL =8  ACQUIRED BITS PER PIXEL =8
BANDS PRESENT =123457
FILENAME =L71196000_00020010603_B10.FSTFILENAME =L71196000_00020010603_B20.FST
FILENAME =L71196000_00020010603_B30.FSTFILENAME =L71196000_00020010603_B40.FST
FILENAME =L71196000_00020010603_B50.FSTFILENAME =L72196000_00020010603_B70.FST
```

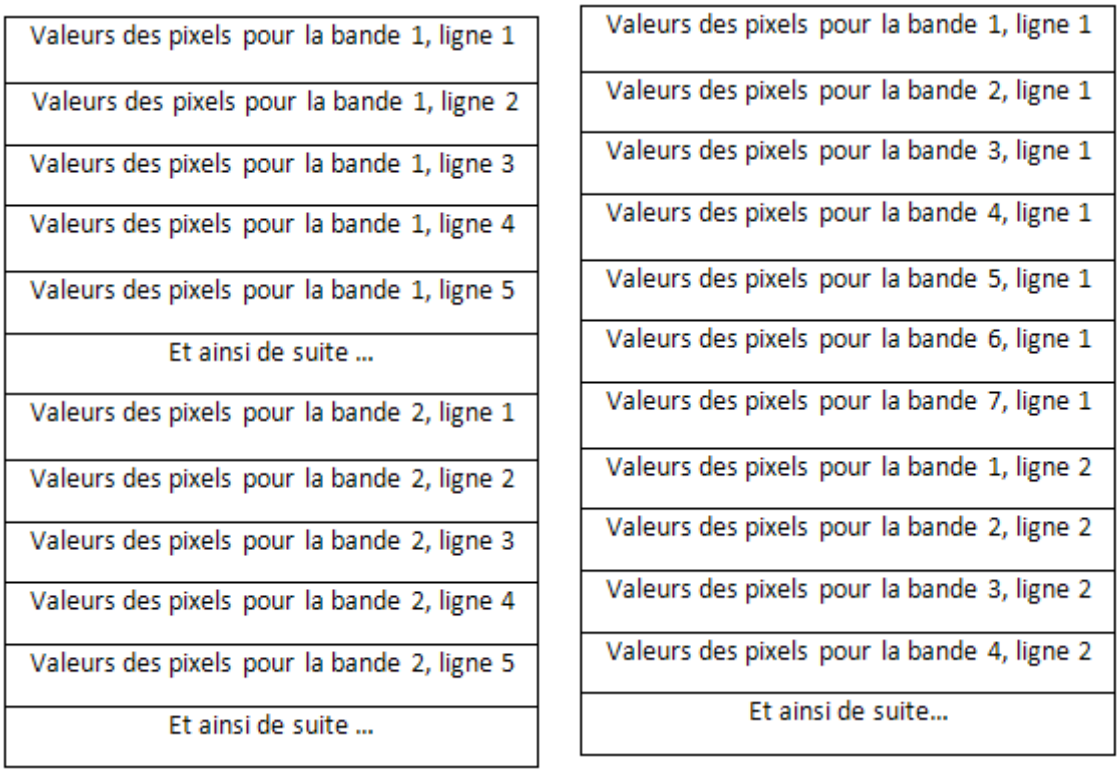
Fig.03.13. Une partie d'un fichier de métadonnées.

Il existe deux structures d'arrangement des valeurs des pixels pour le deuxième fichier, dans la première structure les valeurs de pixels sont arrangées bande par bande. Pour chaque bande, les valeurs des pixels pour la première ligne de balayage sont écrites dans l'ordre de gauche à droite comme premier groupe, tandis que le deuxième groupe contenant les valeurs des pixels pour la ligne de balayage 2, et ainsi de suite (la figure.03.14 (a)).

Dans la deuxième structure les valeurs des pixels sont arrangées ligne par ligne. c-à-d si le nombre de bandes est égale à sept alors le fichier tient la ligne de

balayage 1 pour chacune des sept bandes, suivie de la ligne de balayage 2 pour chacune des sept bandes, et ainsi de suite (la figure.03.14 (b)).

Le premier format (le fichier de métadonnées + le deuxième fichier utilisant la première structure) est appelé format BSQ (Band SeQuential). Tandis que le deuxième format (le fichier de métadonnées + le deuxième fichier utilisant la deuxième structure) est appelé format BIL (Band Interleaved by Line).



(a) (b)

Fig.03.14. Format des données, (a) le format BSQ, (b) le format BIL.

Un certain nombre des formats génériques et propriétaire sont en existence. Un format générique est un format qui n'est pas limité à un produit particulier, alors qu'un format propriétaire est possédé par une compagnie ou une organisation spécifique. Par exemple, le satellite SPOT fournit des données dans un format propriétaire appelé `CAP'. Des données de Landsat-7 ETM+ peuvent être obtenues en format ` GeoTIFF' (générique), HDF (propriétaire) ou Fast (propriétaire).

Le format dans lequel les données de télédétection sont fournies peut être considéré comme externe dans le sens que les données livrées par une compagnie particulière aux différents clients ont le même format. Les producteurs des logiciels de traitement d'images définissent également leurs propres formats de données (formats internes) Par exemple, le système de traitement d'images ENVI, lancé sur le marché par Research Systems Inc., exige deux fichiers par image. Le premier représente un fichier de métadonnées avec l'extension .hdr, alors que les données d'image sont contenues dans un fichier simple dans le format BSQ avec l'extension

.bsq ou dans le format BIL avec l'extension .bil. Le logiciel d'ENVI lit les données d'image dans un format externe, tel que la CAP ou GeoTIFF et les convertit au format interne d'ENVI. [20]

3.5. Conclusion

Dans ce chapitre nous avons présenté quelques notions importantes concernant les images satellitaires notamment : les différents types d'images satellitaires, la structure de représentation des pixels et les différents formats des données images.

Dans le prochain chapitre nous suggérons une méthode de chiffrement/déchiffrement pour ce type d'image basée sur les systèmes chaotiques. Nous présentons aussi une analyse de la sécurité de l'algorithme de chiffrement et une évaluation de sa performance.

Chapitre 04

Un crypto-système pour les images satellitaires

4.1. Introduction

Avec le développement rapide des technologies et des applications spatiales, plusieurs images satellitaires sont prises. Certaines images doivent être chiffrées avant de les transmettre au sol. Nous proposons dans ce travail une méthode de chiffrement/ déchiffrement de trois rondes (deux rondes de diffusion et une ronde de confusion) au lieu de quatre rondes (deux rondes de confusion et deux rondes de diffusion) tel que supposé dans [17].

Dans la première et la deuxième ronde de diffusion les propriétés des pixels horizontalement adjacents sont mélangées et décalées circulairement à droite et à gauche respectivement. Dans la troisième ronde une confusion robuste et efficace est réalisée à l'aide d'une image clef chaotique (ICC) qui est générée en premier lieu par deux cartes d'une seule dimension (logistique, sine) et en deuxième lieu par une carte 2D (carte standard) et une carte 1D (logistique). Selon les résultats obtenus (sécurité et analyse de performances) nous choisirons la meilleure combinaison de production de l'image clef chaotique. L'algorithme de chiffrement et de déchiffrement seront donnés en détail dans la section 4.2 et 4.3 respectivement. Et dans la section 4.4 nous analysons la sécurité de l'algorithme de chiffrement et nous évaluons sa performance.

4.2. L'algorithme de chiffrement

Dans cette section, on donne l'architecture détaillée du mécanisme de confusion-diffusion adoptée pour le chiffrement dans notre algorithme.

4.2.1. La lecture de l'image originale (IO)

Dans notre travail on chiffre des images satellitaires sur chaque canal. Ce qui implique que les images traitées sont des images en niveau de gris (grayscale) dont les valeurs de leurs pixels varient dans la plage 0..255. Alors :

IO = $Bande_{i,j}$ où $1 \leq i \leq H$ et $1 \leq j \leq L$, H et L sont respectivement la hauteur et la largeur de l'image satellitaire en pixels.

Bande: représente le canal de l'image originale.

4.2.2. La clef sécrète

La clef secrète dans la technique proposée du chiffrement est un ensemble de trois nombres de virgule flottante et d'un nombre entier (X_0, Y_0, K, N), où X_0, $Y_0 \in (0,2\pi)$, K peut avoir n'importe quelle valeur réelle supérieure ou égale à 18.0 et N peut prendre n'importe quelle valeur entière.

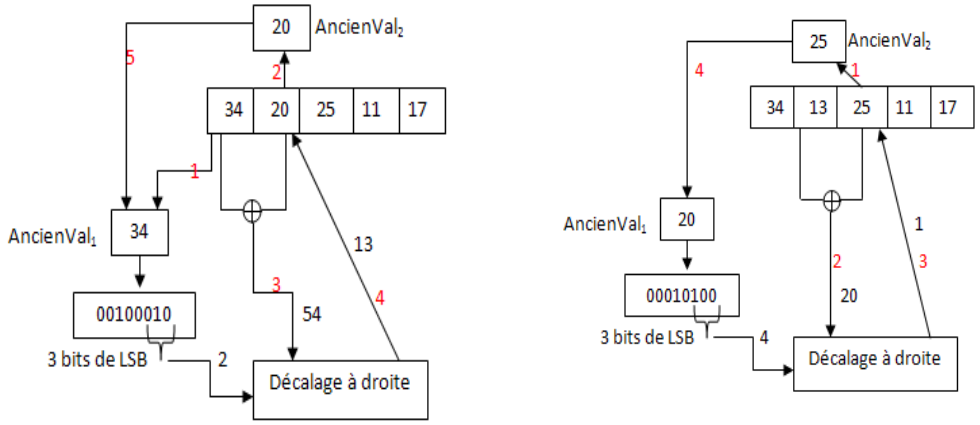
4.2.3. Diffusion

Dans la cryptographie, la diffusion désigne le processus de réarrangement des bits dans le message de sorte que la redondance dans le texte clair soit repartie dans tout le texte chiffré [21]. En particulier dans les images où la redondance est importante, le processus de la diffusion est nécessaire pour développer une technique de chiffrement sûre. Dans le chiffrement des images, le processus de diffusion change les propriétés statistiques de l'image source en distribuant l'influence de chaque bit sur la totalité de l'image chiffrée. Ceci enlève la possibilité d'attaques différentielles en comparant les paires de l'image originale et chiffrée. Dans notre algorithme de chiffrement, on emploie deux types de diffusion : une diffusion horizontale droite (DOD) et une diffusion horizontale gauche (DOG).

(i) Dans le processus de la DOD, les propriétés des pixels horizontalement adjacents sont mélangées et décalées circulairement à droite par la valeur originale des trois bits de poids faible du premier pixel de la paire courante. Ainsi, le premier pixel reste inchangé, le deuxième pixel est modifié en appliquant un $OU_{exclusif}$ entre le premier et le deuxième pixel et le résultat est décalé circulairement à droite par la valeur des trois bits de poids faible du premier pixel et le troisième est modifié en appliquant toujours un $OU_{exclusif}$ entre le pixel lui-même et le dernier pixel modifié. Ensuite, le pixel est décalé circulairement à droite par la valeur originale des trois bits de poids faible du deuxième pixel. Et le processus se répète de la même manière jusqu'au dernier pixel de l'image. Le DOD peut être récapitulé mathématiquement de la façon suivante :

$AncienneVal_1 \leftarrow Bande_{1,1}$
Pour i allant de 1 à H
  Pour j allant de 1 a L-1
  début
    $AncienneVal2 \leftarrow Bande_{i,j+1}$
    $Bande_{i,j+1} \leftarrow Bande_{i,j+1} \oplus Bande_{i,j}$
    $Bande_{i,j+1} \leftarrow DecCircDroite\ [Bande_{i,j+1}, LSB_3(AncienneVal_1)]$
    $AncienneVal_1 \leftarrow AncienneVal_2$
  fin
  Si i < Hauteur alors
  début
    $AncienneVal_2 \leftarrow Bande_{i+1,1}$
    $Bande_{i+1,1} \leftarrow Bande_{i+1,1} \oplus Bande_{i,L}$
    $Bande_{i+1,1} \leftarrow DecCircDroite\ [Bande_{i+1,1}, LSB_3(AncienneVal1)]$
    $AncienneVal_1 \leftarrow AncienneVal_2$
  fin.

Le diagramme illustrant le processus de la DOD est montré dans la figure Fig.04.1.



(a) (b)

Fig.04.1. le processus de la DOD : (a) la première itération, (b) la deuxième itération. Les nombre en rouge représentent l'ordre d'exécution.

(ii) Le DOG est le même que *DOD* sauf que la direction est de droite à gauche et le décalage circulaire à droite est fait par la valeur courante (modifiée) des trois bits de poids faible du deuxième pixel de la paire courante. Ainsi, contrairement au *DOD* le dernier pixel reste inchangé. Le *DOG* peut être récapitulé mathématiquement de la façon suivante :

AncienneVal$_1$ ← Bande$_{H,L}$
Pour i allant de H à 1
  Pour j allant de L à 2
  début
    AncienneVal$_2$ ← Bande$_{i,j-1}$
    Bande$_{i,j-1}$ ← Bande$_{i,j-1}$ ⊕ Bande$_{i,j}$
    Bande$_{i,j-1}$ ← DecCircDroite [Bande$_{i,j-1}$, LSB$_3$ (AncienneVal$_1$)]
    AncienneVal$_1$ ← AncienneVal$_2$
  fin
  Si i > 1 alors
  début
    AncienneVal$_2$ ← Bande$_{i-1,L}$
    Bande$_{i-1,L}$ ← Bande$_{i-1,L}$ ⊕ Bande$_{i,j}$
    Bande$_{i-1,L}$ ← DecCircDroite [Bande$_{i-1,L}$, LSB$_3$ (AncienneVal$_1$)]
    AncienneVal$_1$ ← AncienneVal$_2$
  fin.

4.2.4. Confusion

Dans la cryptographie la confusion est attendue pour faire une relation très complexe entre la clef secrète et le texte chiffré [21], pour atteindre cet objectif avec la satisfaction des performances de sécurité, plusieurs tests (combinaisons) ont effectués permettant de choisir la combinaison la plus efficace et la plus robuste pour générer l'image clef chaotique. Chaque combinaison (test) est constituée de deux étapes où la première étape est une étape préparatrice de la deuxième étape:

4.2.4.1. La première combinaison

Pour générer l'image clef chaotique nous avons besoin de trois cartes chaotiques, deux cartes d'une dimension (carte logistique, carte sine) et une autre carte de deux dimensions (carte standard).

Les deux cartes (logistique et sine) sont utilisées pour produire les pixels de l'image clef chaotique, une carte à chaque fois (à chaque itération. Tandis que la carte standard est utilisée pour modifier les conditions initiales des deux cartes précédentes à chaque ligne de pixels.

Remarque

- ✓ On choisit la première dimension de la carte standard pour changer les conditions initiales de la carte logistique et la deuxième dimension pour changer les conditions initiales de la carte sine. La somme des deux dimensions est employée pour déterminer la carte à utiliser.
- ✓ Ce choix est fait d'une manière aléatoire.

❖ **Etape 01**

On réitère d'abord la carte standard N-fois et en utilisant X_0, Y_0, K comme conditions initiales et paramètre système respectivement. Le résultat (X_N, Y_N) est stocké pour une utilisation ultérieure (comme des conditions initiales).

Ce résultat est également employé pour calculer les conditions initiales pour la carte logistique selon la manière suivante:

$$Z \leftarrow (X_N+Y_N) \bmod 1 \qquad (04.1)$$

Ensuite, on réitère la carte logistique N-fois en utilisant comme paramètre système la valeur 4.0 (λ = 4.0 pour générer le comportement chaotique) et stocker le résultat pour une utilisation ultérieure.

❖ **Etape 02**

On génère Maintenant l'image clef chaotique de hauteur H et de largeur L comme suit :

```
Pour i allant de 1 à  H
debut
    Pour  j allant de 1 à L
    début

        X       ←    X + K * sin(Y) mod 2π
        Y       ←    Y + X  mod 2π
        Indice  ←    (X+Y) mod 2 // pour déterminer la carte à utiliser
        Si  indice = 0  alors   // la carte logistique est choisie
        début
            Z   ←  4 * Z *(1 - Z)  mod 1
            ICC(i,j) ← Z * 256
        fin
        Sinon       // la carte sine est choisie
        début
             Z'   ←  1 * sin(π * Z') mod 1
             ICC(i,j) ←  Z' * 256
         fin

      Fin
       Z ← Y mod 1  // changer la condition initiale de la carte logistique
       Z' ← X mod 1 // changer la condition initiale de la carte sine
Fin.
```

4.2.4.2. La deuxième combinaison

Dans la combinaison précédente on a utilisé une carte (carte logistique ou carte sine) pour générer un pixel à la fois (une carte à la fois). Dans cette combinaison la même procédure est répétée en utilisant les deux cartes simultanément. Ainsi, chaque carte produit 04 bits du pixel de l'image clef chaotique.

Le problème qui se pose est que : les quatre bits de poids fort de chaque pixel sont générés par qui ? Comme solution à ce problème on utilise la carte logistique pour générer les quatre bits de poids fort de chaque pixel de l'image clef chaotique dans la combinaison courante et l'autre carte (carte sine) dans la combinaison suivante.

❖ **Etape 01 :** identique à l'étape 01 de la première combinaison.

❖ **Etape 02 :** est détaillée par l'algorithme ci-dessous.

```
Pour i allant de 1 à  H
debut
    Pour  j allant de 1 à L
    début

        X  ←   X + K * sin(Y) mod 2π
        Y  ←   Y + X mod 2π

        Z  ←  4  *Z*(1 - Z) mod 1
        ICC_i,j  ←  Z * 256
        ICC_i,j  ←  ( 15   Et_logique  ICC_i,j )   // l'extraction des quatre bits générés par la carte
        DecalageGauche(ICC_i,j,4)        // logistique et les rendus au MSB

        Z'  ←  1 * sin(π*Z') mod 1
        temp_j  ←  Z' * 256
        temp  ←  ( 15   Et_logique  temp  )   // l'extraction des quatre bits générés par la carte sine
        ICC_i,j     ←  (temp  Ou_logique  ICC_i,j  )
    Fin
    Z  ← Y mod 1  // changer la condition initiale de la carte logistique
    Z' ← X mod 1  // changer la condition initiale de la carte sine
fin
```

4.2.4.3. La troisième combinaison

Elle est identique à la deuxième combinaison sauf que la génération des quatre bits de poids fort de chaque pixel de l'image clef chaotique est faite par la carte sine.

- **Etape 01 :** identique à l'étape 01 de la première combinaison.
- **Etape 02 :** donnée par l'algorithme ci-dessous.

```
Pour i allant de 1 à  H
debut
        Pour  j allant de 1 à L
        début

                X  ←   X + K * sin(Y) mod 2π
                Y  ←   Y + X mod 2π

                Z' = 1 * sin(π*Z') mod 1
                ICC_i,j ← Z' * 256
                ICC_i,j  ←  ( 15   Et_logique  ICC_i,j  )// l'extraction des quatre bits générés par la carte
                DecalageGauche(ICC_i,j,4)   // sine et les rendus au MSB
```

```
            Z = 4 *Z*(1 - Z) mod 1
            temp ← Z * 256
            temp ← ( 15  Et_logique  temp )   // l'extraction des quatre bits générés par la
                                              //  carte sine
            ICC_i,j ← (temp  Ou_logique  ICC_i,j )

      Fin
      Z ← Y mod 1 // changer la condition initiale de la carte logistique
      Z' ← X mod 1  // changer la condition initiale de la carte sine
fin
```

4.2.4.4. Quatrième combinaison

Dans les deux combinaisons précédentes, chaque carte (sine, logistique) produit ***04 bits*** de chaque pixel de l'image clef chaotique, mais rien ne nous empêchons de rendre le nombre de bits (04) de chaque pixel de l'image clef chaotique généré par les deux cartes un nombre aléatoire (le nombre de bits généré par les deux cartes est différent). Cette philosophie est concrétisée par ce qui suit :

- **Etape 01 :** identique à l'étape 01 de la première combinaison.
- **Etape 02 :** donnée par l'algorithme ci-dessous.

```
Pour i allant de 1 à  H
debut
      Pour  j allant de 1 à L
      début

            X ←  (X + K * sin(Y)) mod 2π
            Y ←  (Y + X) mod 2π
            Distvar ← (X+Y) mod 2
            Si  distvar = 0   alors  // utiliser la carte logistique pour le MSB
                                     // distvar = distinction variable
            Debut
                  Nbrbits ←  (X+Y) mod 8  // determiner le nombre de bits généré par la
                  Nbrbits ←  nbrbits + 1   // la carte logistique.

                  Z = 4 *Z*(1 - Z) mod 1
                  ICC_i,j ← Z * 256
```

nbrdec ← 0
nbrdec ← comp(nbrdec)
DecalageDroite(nbrdec, 32-nbrbits)
$ICC_{i,j}$ ← (nbrdec $Et_{logique}$ $ICC_{i,j}$)
} l'extraction de nbrbits générés par la carte logistique et les rendus au MSB

DecalageGauche($ICC_{i,j}$, 8-nbrbits)

Z' = 1 * sin(π*Z') mod 1
temp ← Z' * 256
nbrdec ← 0
nbrdec ← comp(nbrdec)
DecalageDroite(nbrdec, 32-(8-nbrbits))
temp ← (nbrdec $Et_{logique}$ temp)
$ICC_{i,j}$ ← (temp $Ou_{logique}$ $ICC_{i,j}$)
} compléter les bits du pixel restés par la carte sine

Fin

Sinon // utiliser la carte sine pour MSB
Debut
Nbrbits ← (X+Y) mod 8
Nbrbits ← nbrbits + 1

Z' = 1 * sin (π*Z') mod 1

$ICC_{i,j}$ ← Z' * 256
nbrdec ← 0
nbrdec ← comp(nbrdec)
DecalageDroite(nbrdec, 32-nbrbits)
$ICC_{i,j}$ ← (nbrdec $Et_{logique}$ $ICC_{i,j}$)
DecalageGauche($ICC_{i,j}$, 8-nbrbits)

Z = 4 *Z*(1 - Z) mod 1
temp ← Z * 256
nbrdec ← 0
nbrdec ← comp(nbrdec)
DecalageDroite(nbrdec, 32-(8-nbrbits))
temp ← (nbrdec $Et_{logique}$ temp)
$ICC_{i,j}$ ← (temp $Ou_{logique}$ $ICC_{i,j}$)

```
            fin

        fin
        Z ← Y mod 1
        Z' ← X mod 1
fin
```

Dans les combinaisons précédentes nous avons utilisé des cartes d'une dimension pour générer les pixels de l'image clef chaotique. Dans les combinaisons qui suivent, nous allons essayer d'utiliser une carte d'une dimension (carte logistique) et une autre de deux dimensions (standard) pour observer l'effet de l'introduction d'une carte de ce genre dans la production des pixels dans l'espoir d'optimiser les résultats trouvés antérieurement.

4.2.4.5. Cinquième combinaison

Elle est identique à la première combinaison sauf que la carte sine est remplacée par la carte standard (deuxième dimension).

Remarque :

La carte standard a deux objectifs :

- ✓ Changer la condition initiale de la carte logistique (en utilisant la première dimension).
- ✓ Contribuer à la génération des pixels de l'image clef chaotique (en utilisant la deuxième dimension).

- ❖ **Etape 01 :** identique à l'étape 01 de la première combinaison.
- ❖ **Etape 02 :** est détaillée par l'algorithme ci-dessous.

```
Pour i allant de 1 à H
debut
    Pour j allant de 1 à L
    début

        X ← (X + K * sin(Y)) mod 2π
        Y ← (Y + X) mod 2π
        Indice ← (X+Y) mod 2
        Si indice = 0 alors
        debut
            Z = 4 *Z*(1 - Z) mod 1
            ICC_{i,j} ← Z * 256
        fin
```

```
            Sinon
            debut
                Z'← (Y mod 2π)
                ICC_{i,j} ← Z' * 256
            fin
        fin
        Z ← X mod 1
    fin
```

4.2.4.6. Sixième combinaison

Elle est similaire à la deuxième combinaison sauf que la génération des 04 bits de poids faible de chaque pixel de l'image clef chaotique est effectuée par la carte standard (deuxième dimension).

- **Etape 01 :** similaire à l'étape 01 de la première combinaison.
- **Etape 02 :** donnée par l'algorithme ci-dessous.

```
Pour i allant de 1 à H
debut
    Pour j allant de 1 à L
    début

        X ← (X + K * sin(Y)) mod 2π
        Y ← (Y + X) mod 2π


        Z = 4 *Z*(1 - Z) mod 1
        ICC_{i, j} ← Z * 256
        ICC_{i,j} ← ( 15 Et_logique ICC_{i, j} )
        DecalageGauche(ICC_{i, j},4)

        Z'← (Y mod 2π)
        temp ← Z' * 256
        temp ← ( 15 Et_logique temp )
        ICC_{i, j} ← (temp Ou_logique ICC_{i, j} )
    Fin
    Z ← X mod 1
fin
```

4.2.4.7. Septième combinaison

Elle est similaire à la troisième combinaison sauf que la génération des 04 bits de poids fort de chaque pixel de l'image clef chaotique est faite par la carte standard.

- **Etape 01 :** identique à l'étape 01 de la première combinaison.
- **Etape 02 :** est détaillée par l'algorithme ci-dessous.

```
Pour i allant de 1 à H
debut
    Pour j allant de 1 à L
        début

            X ← (X + K * sin(Y)) mod 2π
            Y ← (Y + X) mod 2π

            Z' ← (Y mod 2π)
            ICC_{i,j} ← Z' * 256
            ICC_{i,j} ← ( 15 Et_logique ICC_{i,j} )
            DecalageGauche(ICC_{i,j},4)


            Z = 4 *Z*(1 - Z) mod 1
            temp ← Z * 256
            temp ← ( 15 Et_logique temp )
            ICC_{i,j} ← (temp Ou_logique ICC_{i,j} )
        Fin
        Z ← X mod 1
fin
```

4.2.4.8. Huitième combinaison

Elle est identique à la quatrième combinaison sauf que la génération des bits est faite par la carte standard et la carte logistique au lieu de la carte sine et logistique.

- **Etape 01 :** identique à l'étape 01 de la première combinaison.
- **Etape 02 :** est détaillée par l'algorithme ci-dessous.

```
Pour i allant de 1 à H
debut
    Pour j allant de 1 à L
    début
```

```
X ← X + K sin(Y) mod 2π
Y ← Y + X mod 2π
Distvar ← (X+Y) mod 2

Si distvar = 0 alors // utiliser la carte logistique pour MSB
Debut
    Nbrbits ← (X+Y) mod 8
    Nbrbits ← nbrbits + 1

    Z = 4*Z*(1 - Z) mod 1
    ICC_i,j ← Z * 256
    nbrdec ← 0
    nbrdec ← comp(nbrdec)
    DecalageDroite(nbrdec, 32-nbrbits)
    ICC_i,j ← (nbrdec Et_logique ICC_i,j )
    DecalageGauche(ICC_i,j , 8-nbrbits )

    Z' = Y mod 2π
    temp ← Z' * 256
    nbrdec ← 0
    nbrdec ← comp(nbrdec)
    DecalageDroite(nbrdec, 32-(8-nbrbits))
    temp ← (nbrdec Et_logique temp )
    ICC_i,j ← (temp Ou_logique ICC_i,j )

Fin
Sinon // utiliser la carte standard pour MSB
Debut
    Nbrbits ← (X+Y) mod 8
    Nbrbits ← nbrbits + 1

    Z' = Y mod 2π
    ICC_i,j ← Z' * 256
    nbrdec ← 0
    nbrdec ← comp(nbrdec)
    DecalageDroite(nbrdec, 32-nbrbits)
    ICC_i,j ← (nbrdec Et_logique ICC_i,j )
    DecalageGauche(ICC_i,j , 8-nbrbits )

    Z = 4 *Z*(1 - Z) mod 1
    temp ← Z * 256
```

```
                    nbrdec  ← 0
                    nbrdec  ← comp(nbrdec)
                    DecalageDroite(nbrdec, 32-(8-nbrbits))
                    temp  ← (nbrdec  Et_logique  temp  )
                    ICC_i,j  ← (temp  Ou_logique  ICC_i,j  )

                Fin
            fin
                Z  ← X mod 1
        Fin
```

4.2.5. Confusion à l'aide de l'image clef chaotique

Elle est effectuée simplement par un $OU_{exclusif}$ entre l'image obtenue après l'opération de diffusion (après *DOG*) et l'image clef chaotique générée précédemment c-à-d:

```
Pour i allant de 1 à  H
        Pour  j allant de 1 à L
                Bande_i,j ⟵  Bande_i,j  ⊕  ICC_i,j
```

Ainsi, l'image résultante est l'image cryptée (chiffrée), prête à la transmettre. Le diagramme complet de l'algorithme de chiffrement est montré dans la figure Fig.04.2.

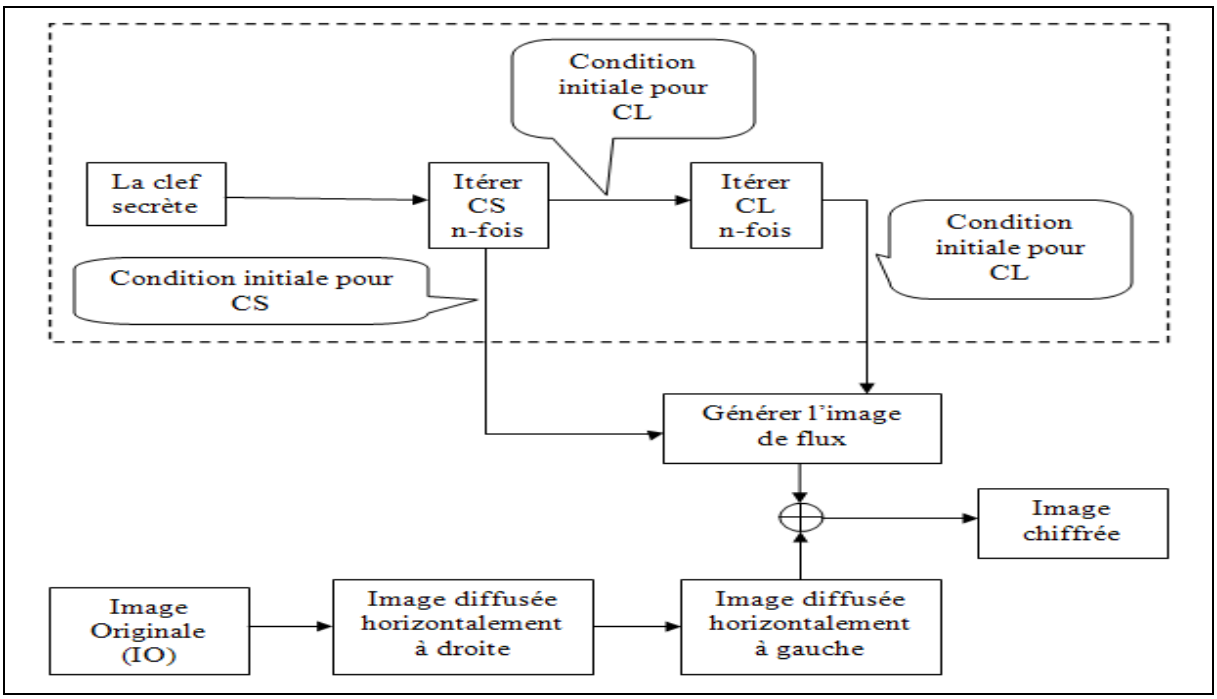


Fig.04.2. L'algorithme de chiffrement.

4.3. L'algorithme de déchiffrement

Dans cette section on donne la procédure de recouvrement de l'image cryptée par la procédure de chiffrement illustrée ci-dessus :

4.3.1. La lecture de l'image chiffrée

Puisque les images chiffrées ont les mêmes propriétés que les images originales (satellitaires), elles constituent des images en niveau de gris (grayscale) dont les valeurs de leurs pixels variées entre 0..255.

IC = $Bande_{i,j}$ où $1 \leq i \leq H$ et $1 \leq j \leq L$, H et L sont respectivement la hauteur et la largeur de l'image satellitaire en pixels.
Bande: représente le canal de l'image chiffrée.

4.3.2. Recouvrement de la confusion en utilisant l'image clef chaotique

On exécute d'abord la phase (04*)* de la procédure de chiffrement pour générer l'image clef chaotique suivant la combinaison choisie. Ensuite, on exécute la phase (05) (procédure de chiffrement) pour faire le recouvrement de la confusion.

4.3.3. Recouvrement de la diffusion

- On effectue d'abord le recouvrement de la diffusion horizontale gauche (*DOG*) suivant cette procédure :

```
AncienneVal1 ← Bande H, L
Pour i allant de H à 1
    Pour j allant de L à 2
        début
            AncienneVal2 ← Bande i, j-1
            Bande i, j-1 ← DecCircGauche[Bande i, j-1, LSB3 (AncienneVal1)]
            Bande i, j-1 ← Bande i, j-1 ⊕ Bande i, j
            AncienneVal1 ← AncienneVal2
        fin
    Si i > 1 alors
    Début
        AncienneVal2 ← Bande i-1,L
        Bande i-1, L ← DecCircGauche[Bande i-1,L , LSB3 (AncienneVal1)]
        Bande i-1, L ← Bande i-1, L ⊕ Bande i,j
        AncienneVal1 ← AncienneVal2
    fin.
```

- Ensuite, la procédure ci-dessous est exécutée pour recouvrir la diffusion horizontale droite:

```
AncienneVal1 ← Bande1, 1
Pour i allant de 1 à H
    Pour j allant de 1 a L -1
        début
            AncienneVal2 ← Bandei, j+1
            Bandei, j+1 ←DecCircGauche [Bandei, j+1, LSB3 (AncienneVal1)]
            Bandei, j+1 ← Bandei, j+1 ⊕ Bandei, j
            AncienneVal1 ← AncienneVal2
        fin
    Si i < Hauteur alors
    début
        AncienneVal2 ← Bandei+1, 1
        Bandei+1, 1 ←DecCircGauche[Bandei+1, 1, LSB3 (AncienneVal1)]
        Bandei+1, 1 ← Bandei+1, 1 ⊕ Bandei, L
        AncienneVal1 ← AncienneVal2
    fin.
```

Ainsi, on arrive à décrypter l'image chiffrée avec succès. Le diagramme complet de l'algorithme de déchiffrement est illustré dans la figure Fig.04.3 :

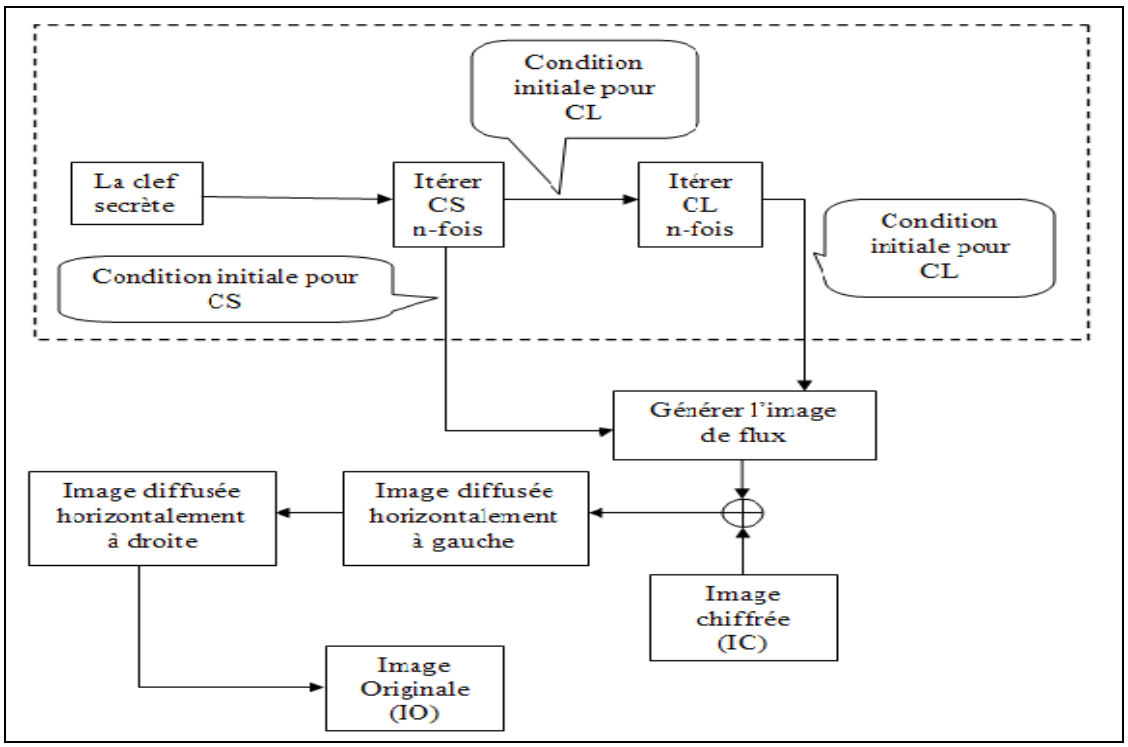


Fig.04.3. L'algorithme de déchiffrement.

4.4. Sécurité et l'analyse des performances

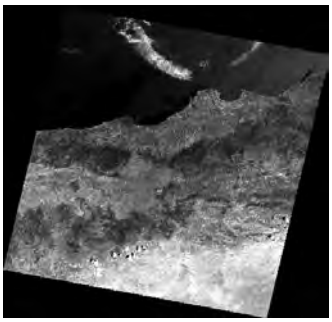
Un algorithme de chiffrement idéal est l'algorithme qui résiste à toutes sortes d'attaques telles que : attaque à texte chiffré seulement, attaque à texte clair connu, recherche exhaustive, etc. Nous discutons dans cette section, les résultats de la sécurité et l'analyse des performances effectués sur l'algorithme proposé de chiffrement d'images.

Plusieurs images dont les contenus sont significativement différents sont utilisées dans les différents tests. Une partie de résultats trouvés est montrée dans les annexes A et B respectivement.

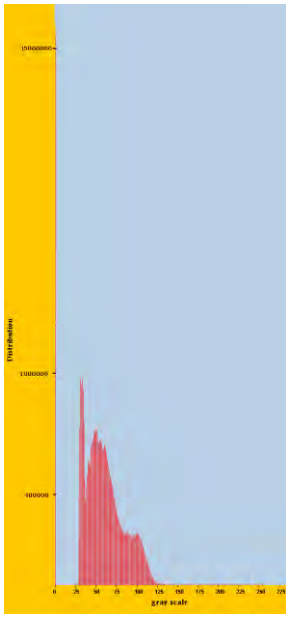
4.4.1. Analyse d'histogramme

Un histogramme d'images montre la manière de distribution des pixels dans une image en traçant le nombre de pixel correspondant à chaque intensité de couleur.

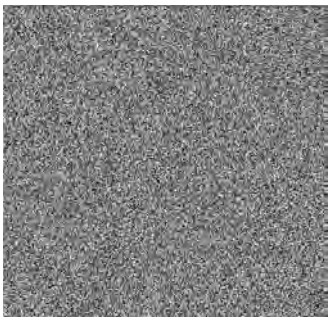
A titre d'exemple, l'image (a) de la figure 01 (image d'Alger capturée par le satellite Landsat 7 ETM+ en 03/06/2001 sur la Bande 2) de taille 7036 x 7368, et ses images chiffrées par l'algorithme de chiffrement proposé (huit images (pour chaque combinaison)) sont montrées avec leur histogrammes dans la fig.04.4.



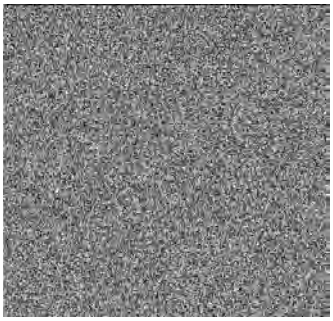
(a) IO (L71196000_00020010603_B20.FST)



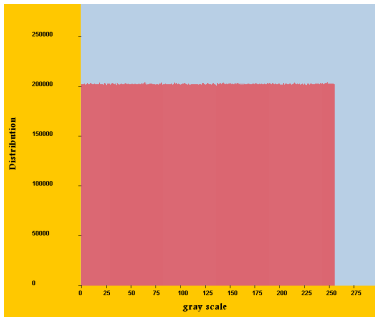
(a') Histogramme de IO



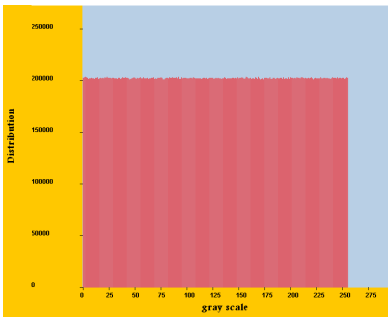
(b) IC (combinaison 01)



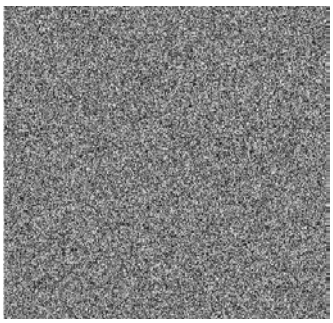
(c) IC (combinaison 02)



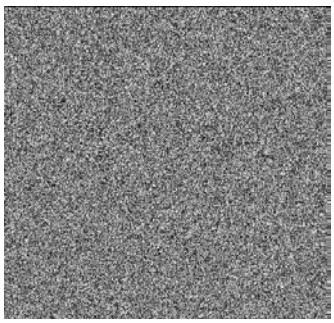
(b′) Histogramme de IC (combinaison 01)



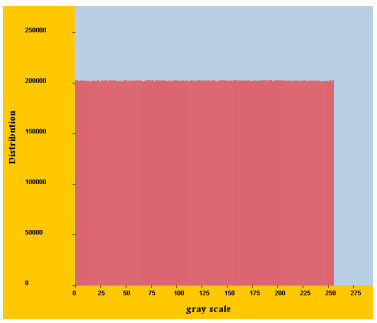
(c′) Histogramme de IC (combinaison 02)



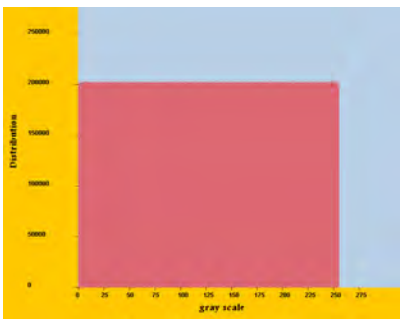
(d) IC (combinaison 03)



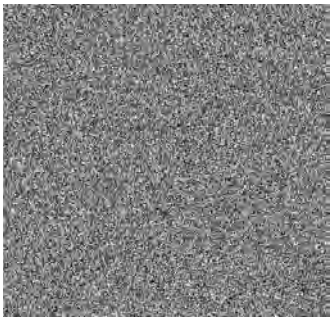
(e) IC (combinaison 04)



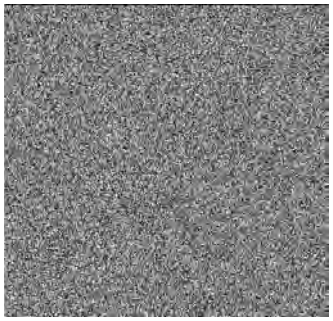
(d′) Histogramme de IC (combinaison 03)



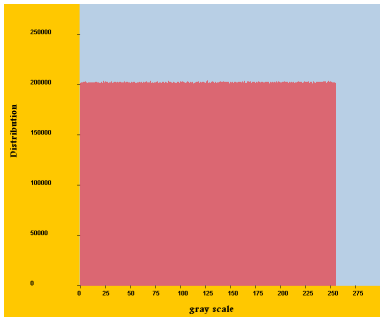
(e′) Histogramme de IC (combinaison 04)



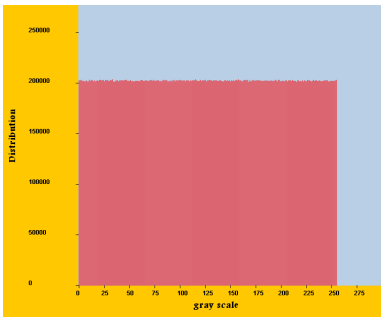
(f) IC (combinaison 05)



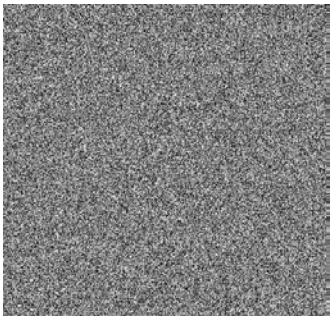
(g) IC (combinaison 06)



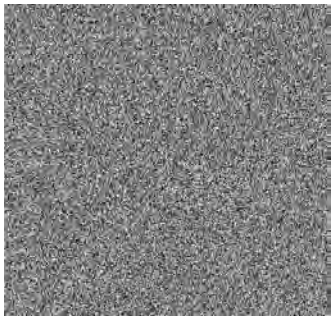
(f') Histogramme de IC (combinaison 05)



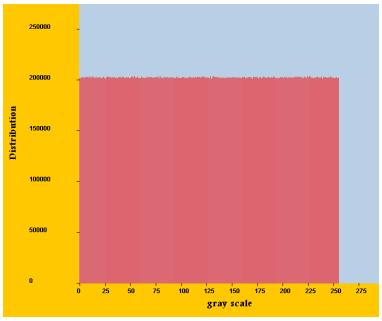
(g') Histogramme de IC (combinaison 06)



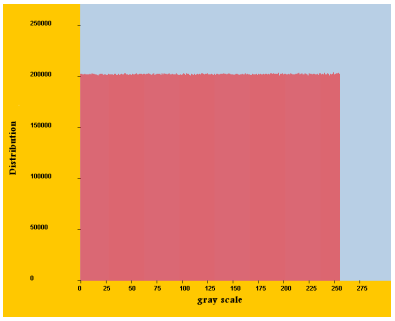
(h) IC (combinaison 07)



(i) IC (combinaison 08)



(h') Histogramme de IC (combinaison 07)



(i') Histogramme de IC (combinaison 08)

Fig.04.4. L'image originale et les images chiffrées avec leur histogrammes en utilisant la clef secrète X= 0.58265532842531, Y= 5.45962347821562, K= 19.52152431277649, N= 110.

On peut bien voir que les histogrammes des images chiffrées (pour chaque combinaison) sont à peu près uniformes. Ils sont très différents de celui de l'image originale. L'algorithme de chiffrement utilisé fait en sorte que la dépendance des propriétés statistiques de l'image chiffrée et de l'image originale soit quasi aléatoire. Ceci rend la cryptanalyse de plus en plus difficile.

4.4.2. Corrélation entre l'image originale et l'image chiffrée

En plus de l'analyse d'histogramme (qui est juste un test visuel), nous avons également calculé et analysé la corrélation entre les diverses paires de l'image originale (l'image fig.01. (a)) et ses images chiffrées (8 images). Les coefficients de corrélation sont calculés par la formule suivante :

$$Coeff_{OC} = \frac{\frac{1}{H \times W}\sum_{i}^{H}\sum_{j}^{W}\left(O_{i,j} - \overline{O}\right)\left(C_{i,j} - \overline{C}\right)}{\sqrt{\left(\frac{1}{H \times W}\sum_{i}^{H}\sum_{j}^{W}\left(O_{i,j} - \overline{O}\right)^2\right)\left(\frac{1}{H \times W}\sum_{i}^{H}\sum_{j}^{W}\left(C_{i,j} - \overline{C}\right)^2\right)}} \quad (04.2)$$

Avec $\overline{O} = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W} O_{i,j}$ **et** $\overline{C} = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W} C_{i,j}$

Ici, O représente le canal de l'image originale, C représente le canal de l'image chiffrée, $\overline{O}$ et $\overline{C}$ respectivement sont les valeurs moyennes des éléments des matrices O et C. H et L sont respectivement la hauteur et la largeur de l'image originale et chiffrée.

Les résultats de corrélation obtenus sont illustrés dans le tableau.01.

Tableau.04.1. Coefficients de corrélation entre l'image originale et ses images chiffrées.

Algorithme de chiffrement utilisant la combinaison :	**Corrélation entre l'image originale et son image chiffrée**
01	0,0001707
02	0.0001523
03	0,0001027
04	0,0003585
05	0,0001089
06	-0,0003209
07	0,0000657
08	-0,0003736

Il est clair que les coefficients de corrélation pour tous les cas de tests de l'image originale et ses images chiffrées sont très petits (ou pratiquement zéro). Par conséquence il n'y a pas de corrélation entre image originale et son image chiffrée (image de chaque combinaison) qui prend les caractéristiques d'une image aléatoire.

4.4.3. Analyse de la sensibilité à la clef secrète

La sensibilité à la clef secrète est une caractéristique essentielle pour un bon crypto-systeme qui garantit la sécurité de ce dernier contre toute attaque exhaustive. On effectue deux types de test pour observer la sensibilité à la clef secrète de notre algorithme de chiffrement :

1) **Test 01 :** l'image chiffrée produite par le système cryptographique devrait être très sensible à la clef secrète, c.-à-d., si on emploie deux clefs légèrement différentes pour chiffrer la même image les deux images produites (chiffrées) devraient être complètement indépendantes entre elles ou en d'autres termes elles devraient posséder une corrélation négligeable.
2) **Test 02 :** l'image décryptée ne peut pas être déchiffrée correctement malgré la présence d'une légère différence entre la clef de chiffrement et de déchiffrement.

- **Test 01**

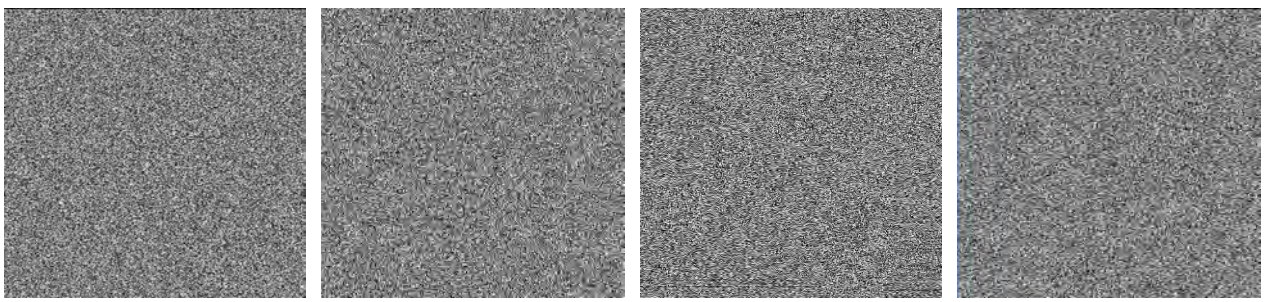
Dans la première étape, l'image de fig.1.(a) est chiffrée à l'aide de l'algorithme de chiffrement cité précédemment (utilisant à chaque fois une combinaison de confusion) avec la clef secrète (X= 0.58265532842531, Y= 5.45962347821562, K= 19.52152431277649, N= 110) les images résultantes sont montrées dans la figure 01.

Dans la deuxième étape et pour chaque combinaison de la confusion, la même image est chiffrée avec quatre clefs légèrement différentes :

- X_0= 0.58265532842530, Y_0= 5.45962347821562, K= 19.52152431277649, N= 110.
- X_0= 0.58265532842531, Y_0= 5.45962347821563, K= 19.52152431277649, N= 110.
- X_0= 0.58265532842531, Y_0= 5.45962347821562, K= 19.52152431277648, N= 110.
- X_0= 0.58265532842531, Y_0= 5.45962347821562, K= 19.52152431277649, N= 111.

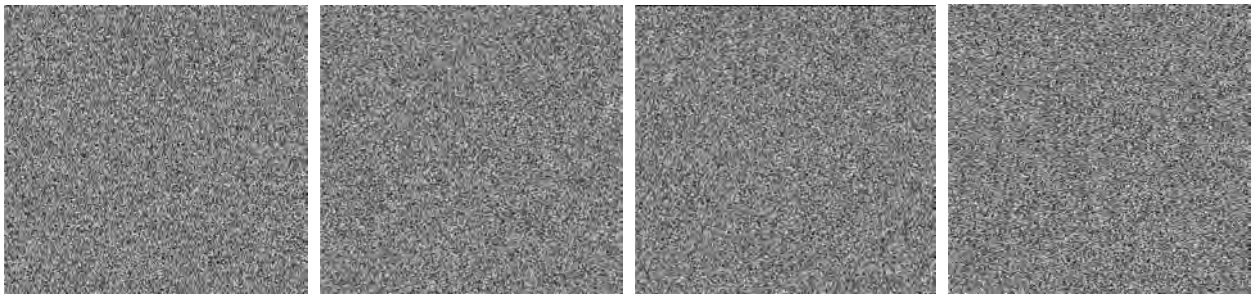
Dans chacune des clefs secrètes utilisées dans la deuxième étape au moins trois parties sont exactement les mêmes que celle utilisées dans la première étape.

Les images chiffrées produites dans la deuxième étape sont montrées dans la figure Fig.04.5.



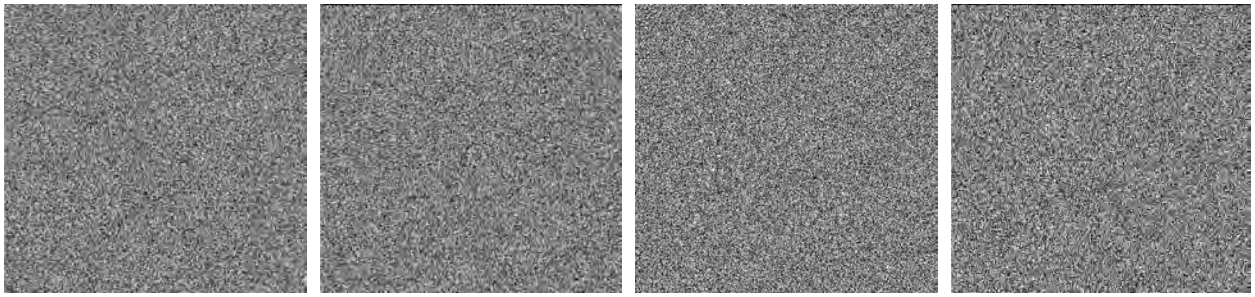
clef 01 **clef 02** **clef 03** **clef 04**

(a)



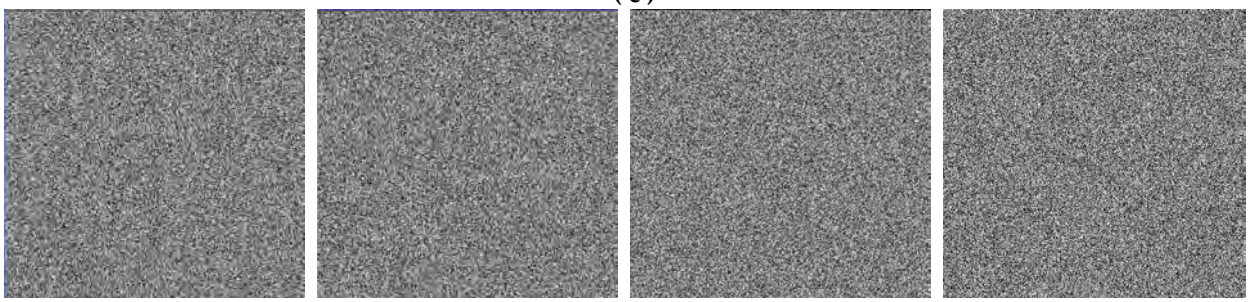
clef 01 clef 02 clef 03 clef 04

(b)



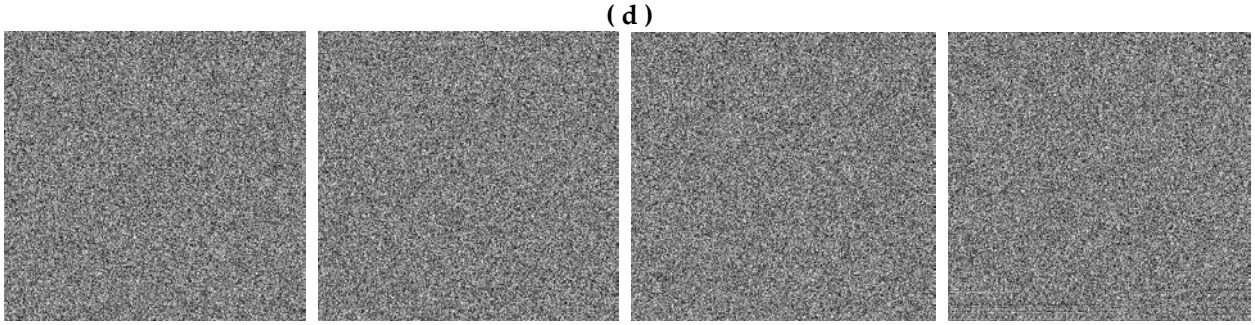
clef 01 clef 02 clef 03 clef 04

(c)



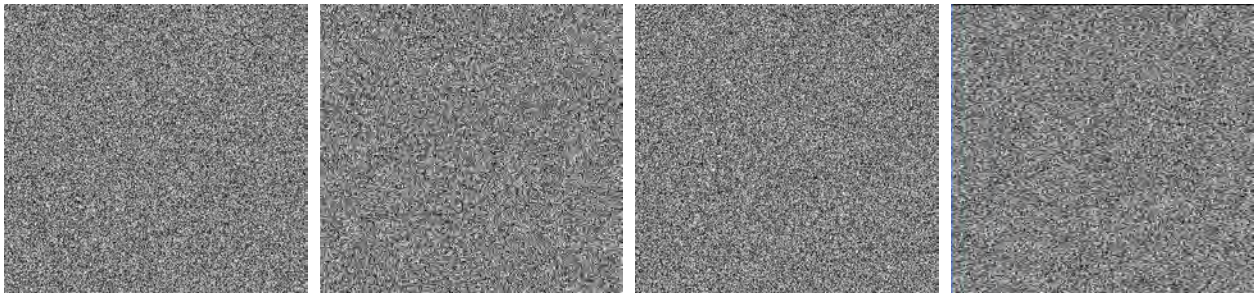
clef 01 clef 02 clef 03 clef 04

(d)



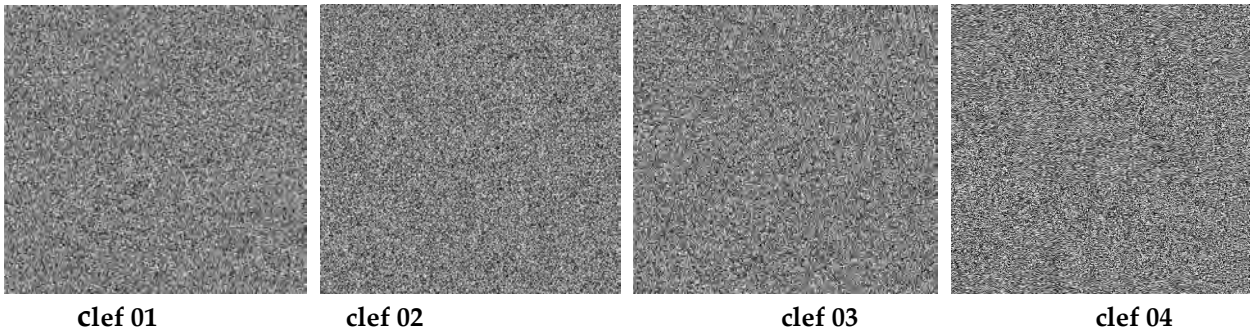
clef 01 clef 02 clef 03 clef 04

(e)



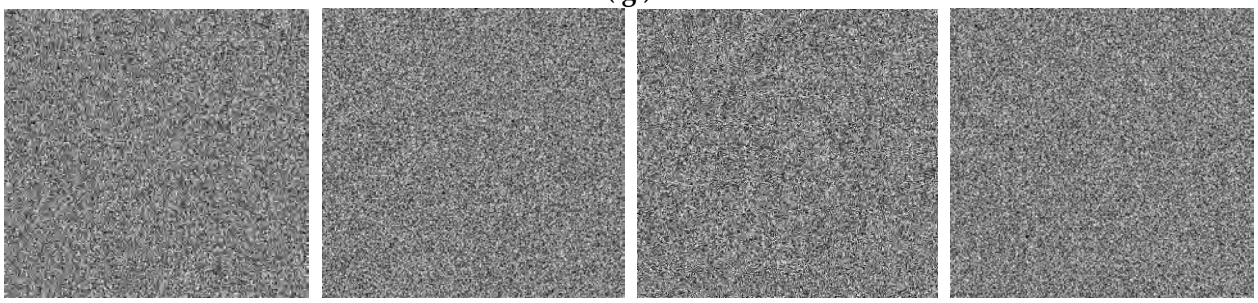
clef 01 clef 02 clef 03 clef 04

(f)



clef 01 **clef 02** **clef 03** **clef 04**

(g)



clef 01 **clef 02** **clef 03** **clef 04**

(h)

Fig.04.5. Les images résultantes du test 01: (a), (b), (c), (d), (e), (f), (g) et (h) représentent les images obtenues par l'algorithme de chiffrement utilisant les combinaisons 1, 2, 3, 4, 5, 6, 7 et 8 respectivement.

Ensuite les corrélations entre les images produites dans l'étape 01 et les images résultantes dans l'étape 02 sont calculées et les résultats trouvés sont montrés dans le tableau. 2.

Tableau.04.2. coefficients de corrélation obtenus après le Test 01

Algorithme de chiffrement utilisant la combinaison :	**Algorithme de chiffrement utilisant la clef :**	**Corrélation calculée**
Combinaison 01	Clef 01	0,0016360
	Clef 02	0,0015274
	Clef 03	-0,0016530
	Clef 04	0,0016376
Combinaison 02	Clef 01	-0,0001872
	Clef 02	-0,0002024
	Clef 03	0,0001607
	Clef 04	-0,0002865
Combinaison 03	Clef 01	0,0077156
	Clef 02	0,0075362
	Clef 03	0,0077905
	Clef 04	-0,0001710

Combinaison 04	Clef 01	0,0092270
	Clef 02	0,0090526
	Clef 03	0,0101999
	Clef 04	-0,0002107
Combinaison 05	Clef 01	0,0073033
	Clef 02	0,0077037
	Clef 03	0,0077516
	Clef 04	-0,0189042
Combinaison 06	Clef 01	0,0000423
	Clef 02	0,0000651
	Clef 03	-0,0000180
	Clef 04	-0,0001376
Combinaison 07	Clef 01	0,0005211
	Clef 02	0,0000541
	Clef 03	0,0002114
	Clef 04	0,0009572
Combinaison 08	Clef 01	0,0016135
	Clef 02	0,0012090
	Clef 03	0,0013144
	Clef 04	0,0023202

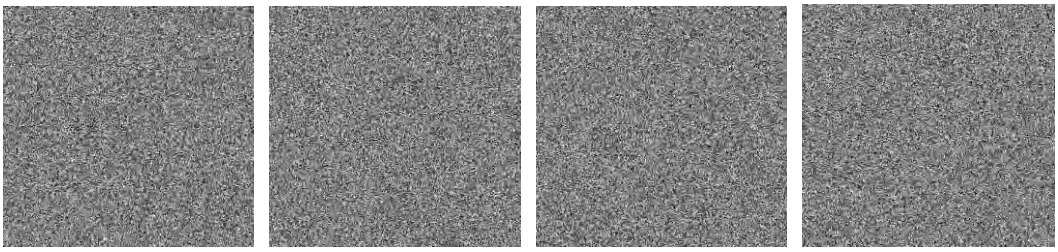
Il est claire qu'il ya une forte de-corrélation entre les pixels de l'image chiffrée en premier lieu et les images cryptées en deuxième lieu.

- **Test 02**

De même, l'image (a) de la figure 01 est chiffrée en utilisant l'algorithme de chiffrement cité précédemment avec la clef (**X= 0.58265532842531, Y= 5.45962347821562, K= 19.52152431277649, N= 110)** les images résultantes sont montrées dans la figure 01. Et on essaie par la suite de les décrypter en utilisant ces quatre clefs de déchiffrement :

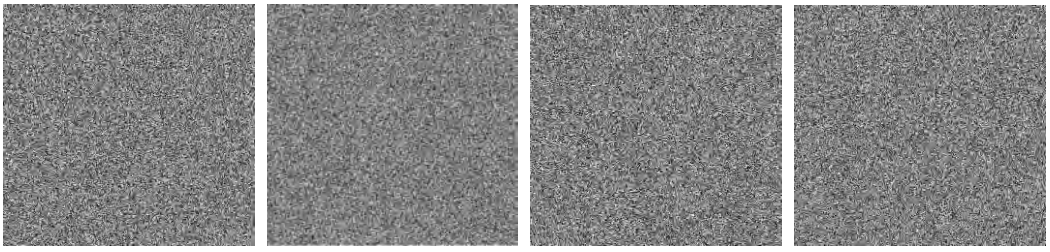
- X_0= 0.58265532842530, Y_0= 5.45962347821562, K= 19.52152431277649, N= 110.
- X_0= 0.58265532842531, Y_0= 5.45962347821563, K= 19.52152431277649, N= 110.
- X_0= 0.58265532842531, Y_0= 5.45962347821562, K= 19.52152431277648, N= 110.
- X_0= 0.58265532842531, Y_0= 5.45962347821562, K= 19.52152431277649, N= 111.

Ces clefs diffèrent légèrement de la clef employée pour le chiffrement. Les images résultantes sont montrées dans la figure Fig.04.6.



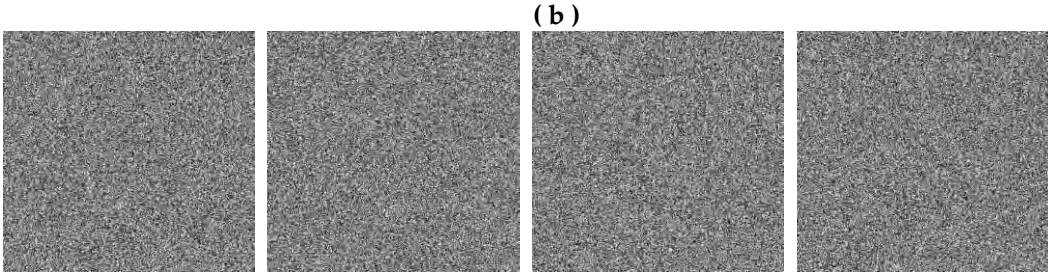
clef 01 clef 02 clef 03 clef 04

(a)



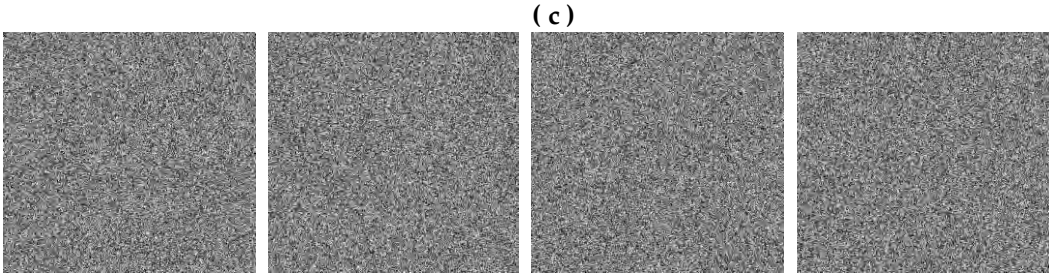
clef 01 clef 02 clef 03 clef 04

(b)



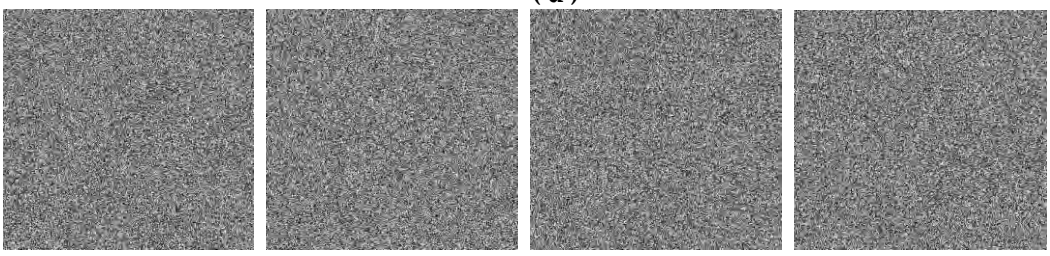
clef 01 clef 02 clef 03 clef 04

(c)



clef 01 clef 02 clef 03 clef 04

(d)



clef 01 clef 02 clef 03 clef 04

(e)

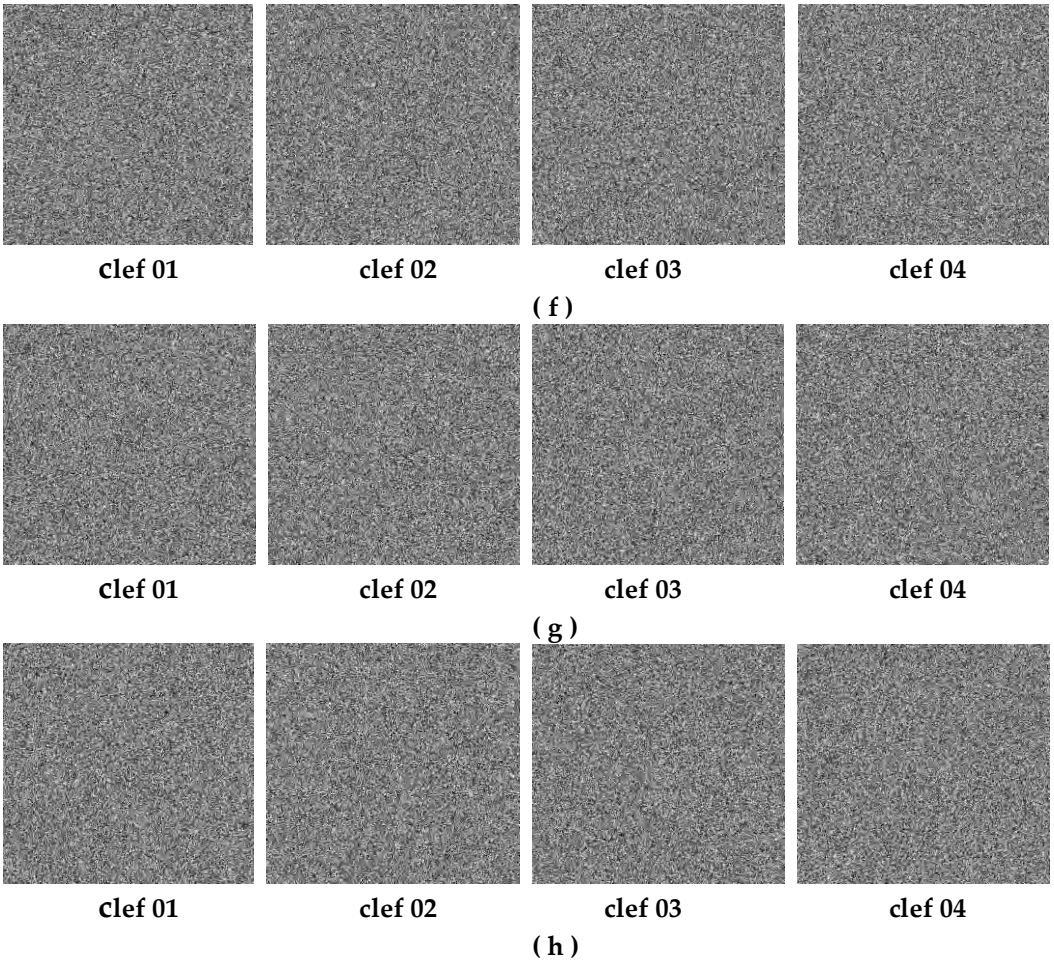


Fig.04.6. Les images résultantes du test 02: (a), (b), (c), (d), (e), (f), (g) et (h) représentent les images obtenues par l'algorithme de chiffrement utilisant les combinaisons 1, 2, 3, 4, 5, 6, 7 et 8 respectivement.

Ensuite les corrélations entre l'image originale et les images résultantes en deuxième lieu sont calculées et les résultats trouvés sont illustrés par le tableau. 3.

Tableau.04.3. coefficients de corrélation obtenu après le Test 02

Algorithme de chiffrement utilisant la combinaison :	**Algorithme de chiffrement utilisant la clef :**	**Corrélation calculée**
Combinaison 01	Clef 01	-0,0002319
	Clef 02	-0,0001880
	Clef 03	-0,0001766
	Clef 04	-0,0002185
Combinaison 02	Clef 01	-0,0000552
	Clef 02	0,0000638
	Clef 03	0,0001562
	Clef 04	-0,0000505

Combinaison 03	Clef 01	-0,0002389
	Clef 02	0,0000532
	Clef 03	0,0000227
	Clef 04	-0,0001314
Combinaison 04	Clef 01	0,0000474
	Clef 02	0,0003279
	Clef 03	0,0000806
	Clef 04	0,0000288
Combinaison 05	Clef 01	0,0000128
	Clef 02	0,0000355
	Clef 03	-0,0000423
	Clef 04	0,0000985
Combinaison 06	Clef 01	0,0001030
	Clef 02	-0,0001428
	Clef 03	0,0000891
	Clef 04	0,0002040
Combinaison 07	Clef 01	0,0000017
	Clef 02	0,0001564
	Clef 03	0,0000950
	Clef 04	0,0000339
Combinaison 08	Clef 01	0,0002334
	Clef 02	0,0002294
	Clef 03	0,0001798
	Clef 04	0,0002033

D'après le tableau précédent on obtient une forte dé-corrélation entre les pixels de l'image décryptée en premier lieu et les images déchiffrées en deuxième lieu. Ainsi, On peut bien constater que l'algorithme proposé est bien sensible à tout petit changement dans la clef secrète.

4.4.4. Corrélation entre les pixels adjacents

Pour une image ordinaire, chaque pixel est fortement corrélé avec ses pixels adjacents dans la direction horizontale ou verticale. Un algorithme de chiffrement idéal devrait produire des images chiffrées dont la corrélation entre les pixels adjacents est négligeable.

Pour tester la corrélation entre les pixels adjacents horizontalement ou verticalement de l'image (a) de la figure.01, on calcule les coefficients de corrélation à l'aide de la formule suivante :

$$Coeff_{X,Y} = \frac{\frac{1}{N}\sum_{i=1}^{N}\left(X_i - \bar{X}\right)\left(Y_i - \bar{Y}\right)}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}\left(X_i - \bar{X}\right)^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}\left(Y_i - \bar{Y}\right)^2\right)}} \qquad (04.3)$$

Avec $\bar{X} = \frac{1}{N}\sum_{i=1}^{N} X_i$ et $\bar{Y} = \frac{1}{N}\sum_{i=1}^{N} Y_i$

(X_i, Y_i) représente la i[ieme] paire des pixels horizontalement ou verticalement adjacents et N est le nombre total de ces paires des pixels (horizontalement ou verticalement adjacents). Pour une image de taille $L \times W$ pixels N = (L-1) H (pour les pixels horizontalement adjacents) et N = (H-1) L (pour les pixels verticalement adjacents).

Les résultats des coefficients de corrélation calculés (des pixels horizontalement et verticalement adjacents) de l'image ci-dessus et son image chiffrée sont montrés dans les tableaux 4 et 5 respectivement.

Tableau.04.4. Cœfficients de corrélation des pixels horizontalement et verticalement adjacents de l'image fig1.(a).

	Corrélation horizontale	**Corrélation verticale**
Image originale	0,9961243	0,9956713

Tableau.04.5. Cœfficients de corrélation des pixels horizontalement et verticalement adjacents des images cryptées.

Algorithme de chiffrement utilisant la combinaison de confusion numéro :	**Corrélation entre les pixels horizontalement adjacents**	**Corrélation entre les pixels verticalement adjacents**
01	0,0001298	-0,0001827
02	-0,0000494	-0,0000605
03	0,0002234	0,0000094
04	0,0019160	-0,0001335
05	-0,0006511	-0,0000458
06	0,0001687	-0,0000555
07	0,0000208	-0,0000069
08	-0,0000632	-0,0001919

Il est clair que la corrélation entre les pixels adjacents est très petite (pratiquement nulle) dans l'image chiffrée produite par la technique de chiffrement proposée.

4.4.5. Analyse différentielle

Par ce test, on démontre la sensibilité de l'image chiffrée par rapport à l'image initiale. Pour cela, on chiffre deux images (IC_1 et IC_2) qui diffèrent seulement par un pixel. Ensuite, Les deux paramètres NPCR (Number of Pixels Change Rate) et UACI (Unified Average Changing Intensity) sont calculés pour tester l'influence de changement d'un pixel sur l'image claire par l'algorithme proposé.

NPCR représente le taux des pixels changés lors du changement d'un seul pixel dans l'image originale. Il est défini par cette formule : [22]

$$NPCR = \frac{\sum_{i=1}^{H}\sum_{j=1}^{L} D_{i,j}}{H \times L} \qquad (04.4)$$

Avec :

$$\mathbf{D_{i,j}} = \begin{cases} \textbf{si } \mathbf{IC_1 \neq IC_2} \\ \textbf{0} \quad \textbf{sinon} \end{cases}$$

Où :

$NPCR_{espérée} = 99{,}6094\%.$

et l'UACI est la différence de l'intensité moyenne entre deux images chiffrées, il est défini comme suit : [21]

$$UACI = \frac{1}{H \times L}\sum_{i=1}^{H}\sum_{j=1}^{L}\frac{IC_{1_{i,j}} - IC_{2_{i,j}}}{2^8 - 1} \times 100\% \qquad (04.5)$$

Où La valeur espérée de UACI est :

$UACI_{espérée} = 33{,}4635\%.$

Le tableau. 6, résume les valeurs des différentes mesures obtenues après les tests qui ont été effectués sur l'images originale (figure 01. (a)) de taille 7036 x 7368 en niveau de gris et ses versions chiffrées (figure 01).

Tableau.04.6. NPCR et UACI.

Algorithme de chiffrement utilisant la combinaison :	**NPCR (%)**	**UACI (%)**
01	*99,5886730967*	*33,4771951068*
	99,5886730967	*33,4780958658*
	99,7065020502	*31,9323785233*
	99,5761232440	*38,4875575780*
	99,7621874380	*35,9391001102*

	99,7320164823	*40,6816900521*
	99,9514730040	*38,6792354560*
	99,9708475300	*36,0833083686*
	99,9109184200	*35,5793404884*
	100	*29,0880427133*
02	*99,6109545819*	*33,4619432045*
	99,6107964067	*33,4761176923*
	99,7196865322	*34,4242069094*
	99,5959125058	*38,4978007501*
	99,7765080809	*35,9037127552*
	99,7597472900	*31,7478972762*
	99,9603520300	*29,4694989800*
	99,9933122751	*33,7377438836*
	99,9197955265	*34,2978121560*
	100	*40,7939025356*
03	*99,6109545819*	*33,4636952502*
	99,6107964067	*33,4779083476*
	99,7196865322	*34,4290654525*
	99,5959125058	*38,4956481906*
	99,7765080809	*35,9007891302*
	99,7597472962	*31,7444955789*
	99,9603520347	*29,4708971783*
	99,9933122751	*33,7351508844*
	99,9197955265	*34,2965946079*
	100	*40,7950692347*
04	*99,6109545819*	*33,4664435501*
	99,6107964067	*33,4787120985*
	99,7196865322	*34,4281550812*
	99,5959125058	*38,4930016796*
	99,7765080809	*35,9032733508*
	99,7597472962	*31,7434300030*
	99,4697295261	*29,4697295261*
	99,9933122751	*33,7335501302*
	99,9197955265	*34,2968445413*
	100	*40,7968483918*
05	*99,5886730967*	*33,4759858948*
	99,4770525297	*33,4770525297*
	99,7065020502	*31,9253694932*
	99,5761232445	*38,4789443745*
	99,7621874380	*35,9321390396*
	99,7320164823	*40,6709940193*

	99,9514730046	*38,6673314064*
	99,9708475382	*36,0835948692*
	99,9109184254	*35,5724577564*
	100	*29,0893805835*
06	*99,5886730967*	*33,4753750102*
	99,5886730967	*33,4766152067*
	99,7065020502	*31,9143722998*
	99,5761232445	*38,4775132785*
	99,7621874380	*35,9228813951*
	99,7320164823	*40,6600059033*
	99,9514730046	*38,6569598484*
	99,9708475382	*36,0837983410*
	99,9109184254	*35,5659449018*
	100	*29,0868485246*
07	*99,5886730967*	*33,4700746355*
	99,5886730967	*33,4712994154*
	99,7065020502	*31,9139833143*
	99,5761232445	*38,4803878613*
	99,7621874380	*35,9255054998*
	99,7320164823	*40,6589835665*
	99,9595804483	*38,5852739608*
	99,9708475382	*36,0843455924*
	99,9109184254	*35,5674566211*
	100	*29,0882292859*
08	*99,5886730967*	*33,4745777043*
	99,5886730967	*33,4757340097*
	99,7065020502	*31,9169164621*
	99,5761232445	*38,4829192395*
	99,7621874380	*35,9293232486*
	99,7320164823	*40,6631853233*
	99,9514730046	*38,6624181714*
	99,9708475382	*36,0782088635*
	99,9109184254	*35,5722363111*
	100	*29,0863896122*

Il est très clair que les valeurs des NPCR et UACI pour tous les cas du test restent dans la gamme des valeurs espérées c-à-d : l'algorithme proposé montre une extrême sensitivité par rapport au texte clair. Par conséquence, l'algorithme résiste bien à l'attaque différentielle.

4.4.6. L'analyse de l'espace des clefs

L'espace des clefs est le nombre total des différentes clefs employées dans la procédure de chiffrement ou de déchiffrement. Comme il a été mentionné auparavant la clef de chiffrement dans la technique proposée est composée de quatre parties : trois nombres réels et un nombre entier (X_0, Y_0, K, N) où X_0, $Y_0 \in (0,2\pi)$, K peut prendre n'importe quelle valeur supérieur ou égale à 18.0 et N peut avoir n'importe quelle valeur entière.

Si on considère une précision de 10^{-14}, le nombre total des valeurs possibles de X_0 qui peuvent être utilisées dans la procédure de chiffrement ou de déchiffrement est 6.28×10^{14}. De même le nombre total des valeurs possibles de Y_0 qui peuvent être employées dans la procédure de chiffrement ou de déchiffrement est 6.28×10^{14}.

Dans la technique de chiffrement proposée, le variable K prend n'importe quelle valeur supérieure ou égale à 18.0. Par conséquence il y a un nombre infini des valeurs possibles de K qui peuvent être employées dans la clef secrète. Mais si on se limite à l'intervalle $(0,2\pi)$, K également peut avoir un nombre total de 6.28×10^{14} des valeurs possible.

Pour la dernière partie de la clef secrète qui peut prendre n'importe quelle valeur entière, le nombre total des valeurs possibles qui peuvent être employées est effectivement infini. Puisque la valeur de N affecte directement la vitesse d'exécution des procédures de chiffrement ou de déchiffrement (nombre d'itérations), on préfère garder la valeur de N entre 100,1100. Ce qui rend le nombre total des valeurs possibles prise par N égale à 10^3.

Ainsi, l'espace de la clef pour la technique de chiffrement ou de déchiffrement est $\approx (6.28)^3 \times 10^{45}$. Et ce nombre est représenté sur 157 bits, ce qui est suffisant pour résister à l'attaque exhaustive.

7] l'analyse de la vitesse d'exécution

Nous avons également analysé la vitesse d'exécution de l'algorithme de chiffrement et de déchiffrement implémenté en Java 6 en utilisant un ordinateur Intel Core 2 duo 2.2 Ghz CPU avec 1 Go de RAM sous Windows XP Professional **Edition**, les résultats trouvés sont illustrés par les tableaux 7 et 8 respectivement.

Tableau.04.7. les variations de temps d'exécution pour les différentes combinaisons de l'algorithme de chiffrement.

Algorithme de chiffrement utilisant la combinaison :	Temps d'exécution min(s)	Temps d'exécution max(s)	Temps d'exécution moyen(s)
01	13,593	13,641	13,617
02	17,672	17,719	17,695
03	18,375	18,406	18,390
04	16,750	16,796	16,773
05	10,687	10,735	10,711
06	10,250	10,281	10,265
07	10,422	10,460	10.441
08	11,672	11,720	11.696

Tableau.04.8. les variations de temps d'exécution pour les différentes combinaisons de l'algorithme de déchiffrement.

Algorithme de déchiffrement utilisant la combinaison	Temps d'exécution min(s)	Temps d'exécution max(s)	Temps d'exécution moyen(s)
01	13,718	13,740	13,729
02	17,730	17,770	17.750
03	18,484	18,515	18,499
04	16,797	16,844	16,820
05	10,781	10,830	10,805
06	10,325	10,360	10,342
07	10,515	10,563	10,539
08	11,765	11,797	11,781

4.4.8. Chiffrement d'une région

Dans plusieurs applications nous n'avons pas intérêt à crypter l'image entière, mais seulement une partie ou une région spécifique. Pour cela on essaye d'adapter notre application pour réaliser cet objectif. Le résultat trouvé est présenté dans la figure fig.04.7.

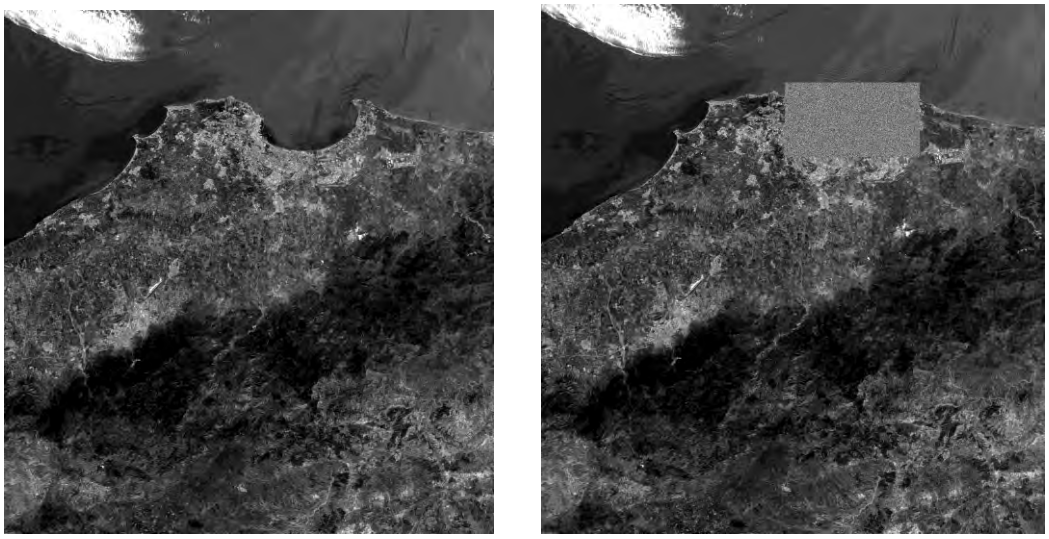


Fig.04.7. cryptage d'une region (combinaison 01).

Les coordonnées exactes de la region cryptée servent comme des clefs de dechiffrement en plus de la clé secrete. En effet, si on ne connait pas les coordonnées exactes de la region on ne peut jamais déchiffrer l'image.

5. Conclusion

Dans cette étude, nous avons développé un nouvel algorithme de chiffrement/déchiffrement basé surtout sur les deux cartes chaotiques standard et logistique. Les conditions initiales, le paramètre système de la carte standard et le nombre d'itérations constituent la clef secrète de cet algorithme qui utilise trois rondes (deux rondes de diffusion et une ronde de confusion) pour produire une image chiffrée.

L'ensemble des tests effectués montre la bonne robustesse des différentes combinaisons de l'algorithme de chiffrement aux différents types d'attaques. Puisque les différents tests donnent presque les mêmes résultats, nous nous limitons au test de temps d'exécution, ce qui nous permet de choisir la combinaison six (06) de la confusion de l'algorithme de chiffrement.

En général, la comparaison entre la vitesse d'exécution de algorithme de chiffrement proposé et ceux existant dans la littérature est fortement liée a la structure du CPU, la taille de la mémoire, le système d'exploitation, le langage de programmation et les options de compilation. En plus l'optimisation du code affecte également la vitesse d'exécution des cryptosystemes. Ainsi, il est inutile de comparer la vitesse d'exécution de deux algorithmes de chiffrement sans utiliser les mêmes environnements de développement et les mêmes techniques d'optimisation.

Pour se situer dans le monde de la cryptographie, nous avons procédé à une comparaison de la vitesse d'exécution entre l'algorithme proposé et celui proposé dans [17]. Nous avons utilisé une machine Intel Core 2 duo 2.2 GHz CPU avec 1 Go de RAM sous Windows XP Professional Edition et Java 2 comme un langage de programmation, et nous avons essayé d'optimiser au maximum les codes des deux algorithmes de chiffrement en utilisant quatre (04) images de taille différentes (10, 14, 20, 42 Mo). Les résultats de la comparaison sont montrés dans le tableau.04.9.

Tableau04.9. Résultats de comparaison entre l'algorithme proposé et celui de Patidar et al.

La taille de l'image (Mo)	**Temps d'exécution de l'algorithme proposé (utilisant la combinaison 06) (s)**	**Temps d'exécution de l 'algorithme de V. Patidar et al (s)**	**Le gain en temps (%)**
10	2,093	03,250	35.60
14	2,812	04,360	35,51
20	4,157	07,140	41,78
42	8,828	16,203	45,52

Ainsi, nous pouvons conclure que l'algorithme proposé est bien sécurisé et recommandé pour la transmission des images satellitaires confidentielles.

Conclusion générale

Conclusion générale :

La cryptographie reste encore le moyen le plus sérieux d'assurer la sécurité des correspondances. Étroitement liée à l'effort de guerre, elle n'a pas cessé de se développer depuis ses origines antiques.

Les Anciens avaient déjà perçu dans cette technique quelque peu ésotérique le meilleur moyen de garantir la confidentialité de leurs missives. Ils l'ont développée d'une façon simple mais efficace, l'adaptant aux divers besoins. Leurs innovations nous ont été transmises soit par le concepteur lui-même (César) soit par des historiens qui en admiraient l'ingéniosité. La qualité de ces méthodes a suscité l'intérêt des crypto-logues ultérieurs qui employèrent ces techniques en introduisant leurs propres inventions.

Cette spécialité confinée dans l'Antiquité aux univers de la guerre et de la diplomatie s'est peu à peu transformée en une partie d'une science de l'information née dans la seconde moitié du XIXe siècle : l'informatique. En effet, de nos jours, la cryptographie ne se limite plus aux documents graphiques mais elle se déploie sur d'autres supports d'information souvent électroniques.

La vocation de cette dissertation est de présenter une tentative d'amélioration d'une nouvelle technique cryptographique basée sur le chaos et qui repose sur l'architecture de confusion-diffusion.

Après une étude bibliographique des techniques de chiffrement/ déchiffrement basée sur les systèmes dynamiques chaotiques, nous avons mis au point une méthode de chiffrement/ déchiffrement basée sur le chaos et l'architecture de confusion-diffusion. Des nombreux tests sur des images ont permis d'évaluer les performances de cette technique.

Parmi les problèmes que nous avons rencontrés au cours de la réalisation de ce travail, la lecture et l'écriture des images de télédétection (les images satellitaires) qui reste le plus grand.

Après, une bonne recherche deux solutions se sont imposées. La première solution est l'utilisation d'un outil Java très avancé appelé JAI (Java Advanced Image Processing) mais il reste très compliqué et il y a un risque de prendre beaucoup de temps pour le maîtriser. La deuxième solution est l'utilisation de l'outil imageIO que nous connaissons déjà.

Apres, une série de tests, les résultats obtenus nous ont rendu pessimiste, ce qui nous a obligé à faire une autre recherche dont le but est toujours : trouver une solution optimale pour la lecture et l'écriture des images de télédétection.

Ceci nous a poussé à utiliser les outils de base du traitement des fichiers (l'outil IO « méthode de bas niveau ») mais la simulation donne toujours des résultats décourageants, et une autre recherche est lancée. Cette fois-ci nous avons trouvé un nouvel outil (toujours pour le traitement des fichiers) appelé NIO (New In/Out). Heureusement, avec NIO nous somme arrivés à résoudre ce grand problème.

Le travail réalisé dans ce mémoire ne constitue pas une fin en soi, mais s'ouvre vers des contributions futures. Quelques idées sont listées ci-dessous.

L'emploi des autres cartes chaotiques à la différence de la carte logistique et sine sera très intéressant.

L'introduction du calcul parallèle dans notre méthode de chiffrement peut-mieux contribuer à l'optimisation de la vitesse de l'opération de chiffrement et de déchiffrement. Ce qui nous permet de l'utiliser pour les communications en temps réel et pourquoi pas de l'adopter pour chiffrer des signaux vidéos.

Bibliographie

[1] James Gleick La théorie du chaos vers une nouvelle science Champs Flammarion 1991.

[2] N. Mansouri cours de La Cryptographie Chaotique dans les communications école doctorale des technologies et des applications spatiales université de constantine.

[3] Tien-Yien Li & James A. Yorke ; Period three implies chaos, American Mathematical Monthly **82** (1975), 985-992.

[4] http://www.juliensalort.org.

[5] Alain Hillion - Les théories mathématiques des populations (1986), P.U.F., coll.

[6] Julien Clinton Sprott Chaos and Time-series Analysis Oxford University Press, 2003 .

[7] V. Patidar, N. K. Preek, K.K. Sud a new substitution-diffusion based image cipher using chaotic standard and logistic maps.

[8] C.E. Shanon, Communication theory of secrecy systems, *Bell. Syst. Tech. J*, pp. 656–715, 1949.

[9] L. M. Pecora, T. L. Carrol synchronization in chaotic system Phys Rev Lett 64 :821-824.

[10] Floriane Anstett Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et crypt- analyse Centre de Recherche en Automatique de Nancy (CRAN) Thèse juillet 2005.

[11] Bruce Schneier traduction de L. Viennot cryptographie appliquée : protocoles, algorithmes et codes sources en C deuxième édition Vuibert informatique.

[12] Christine Bachoc Cours de cryptographie symétrique Master CSI Université Bordeaux I Ann´ee 2004-2005.

[13] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int JBifurc Chaos 1998; 8(6): 1259–84.

[14] Chen G, Mao Y, Chui CK. A symmetric image encryption based on 3D chaotic cat maps. Chaos Solitons and Fractals 2004; 21: 749–61.

Bibliographie

[15] Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic Baker maps. Int J Bifurc Chaos 2004; 14(10): 3613–24.

[16] Lian S, Sun J, Wang Z. A block cipher based on a suitable use of chaotic standard map. Chaos Solitons and Fractals 2005; 26: 117–29.

[17] V. Patidar, N. K. Preek, K.K. Sud a new substitution-diffusion based image cipher using chaotic standard and logistic maps.

[18] M. Steven, D. Freek Remote Sensing Image Analysis: Including the Spatial Domain Springer 2005.

[19] Notions fondamentales de télédétection Un cours tutoriel du Centre spatial canadien.

[20] Paul M. Mather Computer Processing of Remotely-Sensed Images: An Introduction Third Edition John Wiley & Sons Ltd 2004.

[21] C.E. Shanon, Communication theory of secrecy systems, *Bell. Syst. Tech. J*, pp. 656–715, 1949.

[22] A. Awad, S. Elassad, D. Caragata, H. Noura Etude comparative de deux algorithmes de chiffrement/déchiffrement chaotique visàvis de la cryptanalyse et des erreurs de propagation Rapport scientifique du projet *ACSCOM* Juin 2008.

ANNEXE. A

Les résultants de corrélations

L'image L71196000_00020010603_B10.FST (7036 x 7368)
Comb01 :

Test	PC	HAP	VAP
1	-7.312797E-5	1.7180125606209914E-4	-1.7938329031125737E-5
2	2.5167607E-4	2.779088299201157E-4	-2.937675436917091E-4
3	8.111283E-5	1.9853819579715716E-4	3.1831672233676793E-6
4	-1.957945E-4	5.088998787732041E-4	1.98795425403716E-4
5	1.5349464E-5	4.083636002837779E-4	-2.0121394202919903E-4
6	-1.0088249E-4	3.261022554216382E-4	-1.6479201959620053E-4
7	-1.404663E-4	2.8257212360394867E-4	1.288228092771416E-4
8	2.0832637E-4	3.507111167294024E-4	4.124975844674903E-5
9	1.0298502E-4	3.3605713411756207E-4	-1.8819678796565023E-4
11	1.508687E-4	3.9361825746521406E-4	-2.658128583333507E-5
11	6.4638305E-5	4.362809929035145E-4	2.327587613068821E-4
12	8.304253E-5	4.365933673121858E-4	2.0578569384553454E-4
13	3.879759E-5	2.927989258450818E-4	-1.8911404104217766E-5
14	7.3743184E-5	2.3115648704425648E-4	2.212194557343823E-5
15	2.6218168E-4	4.1627127441537303E-4	-3.531398330855399E-5
16	8.4172294E-5	4.5027810837018823E-4	1.675400451755664E-4
17	-2.698837E-5	6.058514676991066E-5	1.0407875999449113E-4
18	-4.021194E-5	4.407065457612367E-4	-7.933487000814028E-7
19	-1.4793773E-5	4.881940741607351E-4	1.725428422801169E-5
21	8.4472675E-5	8.930840678942786E-6	-3.4633549559890974E-5
21	-1.1048969E-4	1.8168701943000146E-4	-3.542653126752612E-4
22	-2.0892412E-5	2.3463527834238806E-4	1.5459014386064028E-5
23	-2.0530877E-4	3.889062283140632E-4	1.8547454496712943E-4
24	-6.4029795E-5	4.246311861938974E-4	-1.5522433885841014E-4
25	9.339227E-5	3.306915584730089E-4	-3.0245079393700396E-6
26	-8.5073196E-5	4.371200129267789E-4	1.3529723297692602E-4
27	1.7841771E-4	1.7654439356990819E-4	-2.7905830219214168E-5
28	8.568783E-5	4.40789772220076E-4	-2.635317318616102E-4
29	2.4195554E-4	2.969823274365407E-4	-8.034491253733815E-5
31	-1.07375425E-4	4.2496547627599946E-4	2.142366808265464E-4
31	2.3104505E-4	3.026393458524623E-4	-1.2492149025316145E-5
32	5.821629E-5	5.60347814251825E-4	1.911657611026144E-5
33	-9.679984E-5	7.022336788132157E-4	-1.052517267085157E-4
34	1.5630343E-4	4.0434101182836474E-4	3.036730929925016 5E-5
35	4.3906213E-5	6.089328799386828E-4	6.712673554648857E-5
36	-1.03702776E-4	6.09132495445104E-4	2.01041458126048E-5
37	-1.7530797E-4	2.0636721076587884E-4	3.356227153931917E-5
38	1.3680004E-4	5.5993454491299316E-5	1.6105685392678852E-4

39	-2.3290186E-5	3.556264762399563E-4	1.6862676980229157E-5
41	8.835785E-6	5.743013768817986E-4	-2.5663187319467797E-4
41	1.175066E-4	5.51786032086125E-5	7.79775719601798E-5
42	2.4935829E-5	4.93221631178574E-4	2.6198755217003006E-4
43	1.2547892E-4	4.4508896393648744E-4	2.6743410864570613E-4
44	-2.8043176E-4	5.368383221252263E-4	-6.002268125991527E-5
45	2.4968313E-4	4.933190644077106E-4	-6.0834031097948585E-5
46	-1.8004625E-4	3.418402568824008E-4	1.0637097844595967E-4
47	-1.7077232E-6	2.8374970019248415E-4	2.0612167135785676E-4
48	1.382432E-4	2.9791388469011567E-4	1.7399242940167723E-4
49	-4.2379015E-5	3.5572290389246933E-4	-1.6445237107838023E-4
51	2.7687446E-4	3.421400325564196E-4	2.939994574248202E-4

Comb02:

Test	PC	HAP	VAP
1	-7.6034616E-5	-3.696732102052111E-5	-1.3524389852855506E-4
2	-1.8802371E-4	-7.754766151853129E-5	-1.4252667785414784E-4
3	-4.4026452E-5	-1.6264706198579064E-4	-5.6851457360987185E-5
4	-9.351927E-5	9.898433062879138E-5	3.0398784360650837E-5
5	-3.3193958E-4	2.6531862393830356E-5	1.6941466754229336E-4
6	2.5841818E-4	-6.954306222654052E-5	-1.5355972726492151E-4
7	7.844342E-5	1.4675328680775315E-4	-1.0757627993964102E-4
8	-9.496488E-5	-8.875443337052546E-5	1.5488234803912944E-5
9	1.3754086E-4	2.7976313136414963E-4	-1.5800606408102126E-5
11	1.2997887E-4	-2.8760336626851887E-4	8.029767750735372E-5
11	7.8090714E-5	-5.966618297261346E-5	-2.8384715562962913E-4
12	-1.151636E-5	-3.624864396415533E-4	3.766500289882689E-5
13	-1.5430013E-4	5.306038087158069E-5	1.9467738739366967E-4
14	2.907956E-4	1.7060194574601374E-4	-1.3068100291311913E-4
15	-1.9260445E-4	-1.0468718656814525E-4	5.0330830014672337E-5
16	-5.352286E-5	1.4266868092818706E-4	6.85862995007961E-6
17	-1.7646924E-4	-4.8391067185674224E-5	-4.746183373735472E-5
18	-7.860392E-6	-3.246454897239332E-5	-2.7339504036911664E-4
19	4.1863328E-5	1.4246325323000718E-4	-2.7400242454361367E-4
21	1.6028906E-4	-7.90749529260299E-5	6.288531129371599E-5
21	-6.94168E-5	-2.944164617023166E-5	6.652529565403133E-5
22	-1.00874844E-4	2.1547391061743038E-4	-2.488518799370468E-5
23	1.5596689E-4	1.462090241407134E-4	1.177762663493512E-4
24	-5.580628E-6	-1.6825993003745864E-4	-1.3830199642399522E-5
25	-1.9242632E-4	-4.1553930624322606E-5	3.703764979559293E-4
26	4.3160508E-5	-1.5068160872542733E-4	-2.1142095403018035E-4
27	-6.119471E-5	7.414379736410622E-5	2.187310181544332E-5
28	8.700512E-6	1.4971496327333397E-4	-1.7818450986341214E-4
29	-6.673669E-5	-1.1014868242516156E-4	-1.707021984361178E-4
31	-2.0594609E-5	-4.9224424776352596E-5	1.0285204695200046E-4
31	2.582369E-4	-3.6090033614181686E-6	1.1699548220986735E-4
32	-1.1771736E-4	-2.2293021572927183E-4	-1.461746951158693E-4

33	1.4109912E-4	2.3232727763983506E-4	6.473281348847494E-6
34	-1.5690981E-4	-3.757102713354076E-5	*-1.524172618206135E-4*
35	-6.3794105E-5	-1.855966187273435E-5	-1.2328765342143006E-4
36	3.6731464E-5	5.028526895644852E-9	-8.699020356591313E-6
37	1.9704336E-5	1.991398016700973E-4	-2.6397137985077957E-4
38	1.8707357E-4	4.0526291110181674E-5	-1.0283466370842089E-4
39	-1.4331356E-4	1.9233666146776994E-4	-1.9292180972850298E-4
41	1.7735283E-4	-1.4965149957624424E-4	2.2890573165851942E-4
41	-1.3699535E-4	-2.365872750577465E-4	1.0359080446864874E-4
42	1.2685814E-4	-1.4461653412704294E-4	-5.1234297776194115E-5
43	-2.0209375E-4	2.2656178664626157E-4	-1.0450584975478184E-4
44	-1.3955573E-4	5.76642276290974E-5	1.944779945599333E-5
45	-1.2475993E-4	-6.193456531491799E-5	-6.72076736067188E-6
46	-9.1415815E-5	1.813680042199838E-4	1.6453416816424342E-4
47	-2.973192E-4	-2.3529052746937504E-4	-4.95415310081123E-5
48	-7.896061E-5	9.528115084740249E-5	-1.3822295330890753E-4
49	3.3300596E-5	-7.733286175633401E-5	2.251785496718062E-4
51	9.808122E-6	3.272775810024386E-5	-2.4354117920724955E-4

Comb03:

Test	PC	HAP	VAP
1	-1.0503417E-4	-6.8604688917602075E-6	-3.09638149223318E-5
2	-3.2472657E-5	2.9570998600005895E-4	2.9463663447964886E-4
3	9.533042E-5	-4.5779539240643644E-5	2.2102761544458658E-5
4	1.601743E-4	2.2267895838489293E-4	-4.471812749960312E-5
5	4.304524E-6	2.4899989064422773E-5	-5.2195101801853315E-5
6	-1.8220456E-4	7.412341101309549E-5	6.529889620354356E-5
7	1.2185903E-4	4.477325934574136E-4	-9.849909216609236E-5
8	2.2511545E-4	1.434148398124738E-4	-3.8072603544857674E-6
9	-1.9321477E-4	1.7020107324949511E-6	2.1193257899195 09E-5
11	-2.2667252E-4	8.028760322553788E-5	-4.994366365143279E-5
11	-3.3654283E-5	3.0087433768914273E-4	-4.27355762298307E-5
12	-1.6543653E-4	1.6242581438315648E-6	-1.205460719664817E-4
13	-1.3152584E-4	2.2416391634021173E-4	-6.892697233800633E-5
14	6.613131E-6	1.284875372926562E-4	6.726575478071002E-5
15	5.0740194E-4	1.0727735750987944E-4	-8.546003093703523E-5
16	5.232783E-5	9.6087961312655E-6	-7.442327689849098E-6
17	1.5124567E-4	1.8852818255373706E-4	-1.0131747635150179E-4
18	-1.2876814E-4	-1.6117142184459004E-4	2.1924692880333465E-4
19	-8.260209E-5	5.2404028266150646E-5	-1.5866514436811924E-4
21	-1.0964731E-4	1.6550419131385955E-4	-9.698659741756898E-5
21	-6.2832376E-5	-4.135062201890672E-5	1.1519591576415245E-4
22	2.0040681E-4	-7.621674387287793E-5	1.673912149229765E-5
23	7.499355E-5	1.3517499779302196E-4	5.4075004195173634E-5
24	1.7517486E-4	1.141791153717364E-4	2.4282059750617945E-6
25	-7.554069E-7	3.2746212750922864E-4	6.119405922191384E-7
26	-9.275908E-5	-1.2375723877626238E-4	-1.1015958049283364E-4
27	-5.543989E-5	-8.342487750813214E-7	-1.9676608077381995E-5

28	1.3925451E-4	1.3048735898713487E-4	2.603986375495236E-4
29	1.6505521E-4	-1.81759694781151E-5	3.627154497520044E-5
31	9.429599E-5	2.225526035770295E-4	1.519355607317731E-4
31	1.475409E-4	1.928342549996632E-5	-4.205259033025961E-5
32	1.6825143E-5	1.7167995350750474E-4	1.9198714423571738E-4
33	-3.158281E-5	1.2504674767736305E-4	-1.4366610767115186E-4
34	-2.3670381E-4	3.403941313893732E-4	-9.899672461150322E-5
35	1.2037566E-4	1.3858319336974972E-4	-1.0181322342036593E-4
36	1.17573465E-4	-1.6341608637591516E-5	-2.846927168731602E-5
37	1.2415003E-4	1.1201297672759791E-4	9.592161264461305E-5
38	9.672448E-6	-3.224998510672235E-5	-2.7263672115765438E-5
39	1.7866505E-4	1.820110214888094E-4	7.178181478941937E-5
41	-1.2320127E-4	5.116945485801656E-5	-7.846437782585982E-5
41	1.7782606E-6	2.1220785627394474E-4	-1.2395634722024755E-5
42	-7.792801E-5	3.1747861169301433E-4	1.567367401945065E-5
43	-3.9943217E-4	2.3183354119494285E-5	9.679638501206621E-5
44	-3.580895E-6	2.152969177339654E-4	4.0937006116338675E-5
45	1.458852E-4	1.2682795214994912E-4	1.4986371285697782E-4
46	1.8673843E-4	-9.079461400854994E-5	-2.2045809077582786E-4
47	5.0957748E-5	1.9011194297036452E-4	3.8886570926987776E-4
48	-1.4721106E-4	1.4747638229305323E-4	-5.027306649699416E-5
49	1.3799465E-4	2.431726028489517E-4	1.655262970239926E-4
51	1.0796931E-5	1.5438360300535506E-4	2.5817123725829895E-5

Comb04:

Test	PC	HAP	VAP
1	-3.175356E-4	0.0018991185393002772	-8.228314445608755E-5
2	5.928741E-4	0.00202780698561385	-1.5299816149405318E-4
3	-5.671423E-4	0.0018798437858889077	2.803752322496927E-4
4	-3.5590434E-4	0.0015986530029758054	7.47982951443101E-5
5	0.0014091475	0.0013986368047132938	5.344492653685512E-5
6	-0.0014214035	0.0021434887567037264	8.629696035881147E-5
7	-5.5958726E-4	0.0020313666565442393	1.9007711740131423E-4
8	-1.45980275E-5	0.0017747870249661523	2.9778152126259776E-4
9	-6.5661676E-4	0.0017455578563012007	-7.276935210656122E-7
11	4.7964856E-4	0.0023920257938193313	6.555844579288497E-5
11	-5.143837E-4	0.0020764994360117895	-6.983310491565405E-5
12	-5.80876E-4	0.002047624114997173	-1.9096093427808304E-4
13	2.162373E-4	0.0023667942042608268	2.0352978183821828E-4
14	-6.8777765E-4	0.002528231122204618	3.659073318116343E-5
15	1.8227978E-4	0.0023064113325140917	-2.188395838341408E-4
16	-3.3703842E-4	0.0023601513911156555	6.935492616020648E-5
17	-6.658319E-4	0.002124954942780376	1.0462515648518974E-4
18	1.4842277E-4	0.0016571697338686815	2.29884368045606E-4
19	2.2516339E-4	0.0020466064426063186	6.909558022144424E-5
21	-3.4657656E-4	0.0022908980374918785	-1.9200061766263345E-4
21	6.521799E-4	0.0020973685869379415	-1.244901274960128E-4

22	2.0098231E-4	0.0018578196905614513	-1.0776136761069297E-4
23	-2.3889431E-4	0.002256472463432391	-7.476398565097952E-5
24	-8.943642E-4	0.0019435232267787793	-2.964214626356726E-4
25	-3.091506E-4	0.0016923725139082035	2.3488802685322082E-5
26	-1.6856997E-4	0.0023375382489464027	-6.47605117715331E-5
27	9.230802E-4	0.0020919752056791515	-1.8741874471163113E-4
28	-8.0807117E-4	0.002011830956790572	2.1007050441580494E-4
29	-5.779151E-4	0.0020147722628176767	-1.442276868298997E-4
31	-3.5101395E-5	0.001964034398717645	-1.8243397885568183E-4
31	-0.00132631	0.002154594496246368	1.3195347231287813E-4
32	-9.677155E-4	0.0022586549854784763	1.0758429007884646E-4
33	-0.001451328	0.0019948773177428424	1.0973610468701103E-4
34	-3.6951544E-4	0.0021348801957461654	2.4785064644569074E-4
35	-4.9387594E-4	0.0023769752691466966	-1.2941013202454287E-5
36	3.772659E-4	0.0017921165494224833	1.0397659787942119E-4
37	1.8185987E-4	0.0018305865854403322	5.898324234684044E-5
38	-2.242143E-4	0.0021576843474630436	-1.718006097219889E-5
39	5.0746836E-4	0.002235486306081069	-3.52163896836836E-4
41	3.6104585E-4	0.0024260670686293917	1.391979864007661E-4
41	1.811928E-5	0.00212458020801512	1.2114931731241072E-4
42	7.9275103E-4	0.0020142722422305677	5.5613690353171816E-5
43	-2.8065292E-4	0.00207432736239506	2.286426082391146E-4
44	0.0011917434	0.00220736437978206	-1.808955033775037E-7
45	-7.4707886E-4	0.002016122848110325	1.97355716934659E-4
46	8.1255625E-4	0.0020502913000706663	1.0957624206261647E-4
47	3.9538305E-4	0.0020250081317115215	1.0561929361239658E-4
48	1.8365047E-4	0.0022473810750880062	3.6264358175776335E-5
49	-0.0011122131	0.0015840479305542288	6.870268927159261E-7
51	-4.942494E-4	0.002111903500760428	-2.4361073775619975E-4

Comb05:

Test	PC	HAP	VAP
1	1.8671522E-4	-5.876638520907039E-4	-2.980781531019 85E-4
2	2.5255175E-4	-7.114679720502238E-4	2.3315376991471672E-4
3	1.7318812E-4	-0.0011691429688839548	2.954180654801147E-4
4	-2.6019977E-4	-6.179368174852699E-4	-2.027927045940547E-4
5	3.561945E-5	-4.3434744369396863E-4	9.39125652288101E-5
6	1.8288405E-4	-6.420417381754049E-4	2.1107831932180213E-6
7	-1.3684739E-5	-0.001243533890894852	-3.6979469371935036E-4
8	6.938312E-5	-0.0014906271279293843	7.332469726015652E-5
9	-9.8665696E-5	-7.839040141102373E-4	-2.0299654409762434E-4
11	3.2389475E-5	-0.0013188539715305095	-1.0136700111738449E-4
11	3.693295E-5	-7.502773451566264E-4	1.8491317588222172E-4
12	-2.3421131E-4	-7.425931818224201E-4	3.296352083931142E-5
13	4.9844326E-5	-0.0012122600169095846	6.46331772771638E-6
14	1.7496839E-4	-8.542455358958656E-4	2.2790531827702564E-5
15	-4.4119417E-5	-7.348495723296261E-4	-1.0149303187852034E-4

16	2.3177718E-5	-0.0011292283854665499	2.2353020887505348E-4
17	-2.2248464E-4	-6.002433586973879E-4	-2.880796156075196E-5
18	4.1625266E-5	-0.0011575502634780025	2.4256719680575425E-5
19	1.968928E-4	-0.0011931439605584414	-5.657299309907933E-5
21	1.3940138E-4	-7.207603371438334E-4	4.838123035252334E-5
21	2.6600994E-5	-0.0011932015008864548	3.308470483229588E-5
22	1.6899635E-4	-0.0014705053754321086	-4.421146952251555E-5
23	-1.9555142E-4	-0.0013882296274709822	6.313337451251965E-5
24	3.855296E-5	-0.0013642315724880383	-1.9666924452246378E-4
25	-1.178365E-4	-9.226523468749644E-4	-1.440465638293162E-4
26	-3.03004E-4	-0.0010658779595984105	-1.291258990402735E-4
27	1.7665654E-4	-8.216506441904637E-4	2.893467996495949E-4
28	8.912415E-5	-0.0010128922343028501	-1.671049681413369E-4
29	-1.0889721E-4	-0.0015272902507596 78	-2.2737073986746088E-4
31	-1.315782E-4	-8.378038536533804E-4	-3.099647364294867E-6
31	1.7029139E-4	-7.842982503427481E-4	6.312318601687848E-5
32	-5.529068E-5	-0.0014416742296310 28	3.452362291171521E-4
33	-1.3556251E-4	-8.283009657765111E-4	-1.9587119166163747E-5
34	8.725431E-5	-9.901904444586985E-4	-1.5322719291897051E-4
35	1.1945051E-6	-9.346999931911928E-4	-1.9326401810984255E-6
36	-3.3027565E-5	-0.0013693450531617355	5.286637124741065E-5
37	1.0582309E-4	-8.418382526597976E-4	2.730926314412428E-4
38	1.4711528E-4	-0.0012395474311539321	9.1761400490288E-5
39	2.9168028E-4	-0.0012217266176383012	9.03564192305173E-5
41	2.4730267E-4	-0.001122074864233263	-1.604844848351693E-4
41	-7.281263E-5	-0.0013922224398188 29	-3.9802313746273546E-5
42	-7.4436975E-5	-9.82033690641221E-4	-2.2007928047620772E-4
43	-2.1205071E-4	-0.0012857701398214611	4.651273834269289E-5
44	1.9347167E-4	-0.001335247205207794	1.0723547329162303E-4
45	2.2546501E-5	-9.772676964256537E-4	-4.025850596879426E-5
46	4.052038E-6	-9.627094826287676E-4	-5.246355178598037E-5
47	-1.9502275E-4	-0.0010747538303500963	1.8861895945512355E-4
48	-1.4285976E-5	-0.0013836376326113236	3.0337018425896616E-5
49	-1.3809168E-5	-8.961662705594373E-4	1.103814699463915E-4
51	-2.40945E-4	-0.0011886824891007774	-5.8237153068206064E-5

Comb06 :

Test	PC	HAP	VAP
1	-2.677588E-5	1.8974016203246322E-4	1.3285872438351755E-4
2	-2.8218105E-4	-2.796744924121199E-4	9.340554888451032E-5
3	-2.6854818E-6	2.3740294488377257E-4	-3.216884569731844E-5
4	-5.9146838E-5	8.567227045332963E-5	-7.453344181559948E-6
5	4.1700765E-5	-2.7972468885319314E-5	-9.666067384355966E-5
6	8.981556E-5	1.781310863074288E-5	2.4854494529185164E-4
7	-3.3204702E-5	1.416177718355632E-4	4.1640701905713535E-6
8	-3.206891E-4	-2.460363444798617E-4	9.782884093940913E-5
9	4.2419582E-5	1.195611708488722E-4	-1.1418291123704623E-4

11	1.1266734E-4	5.529816218408305E-5	-3.047785574195841E-5
11	1.7233443E-4	-8.86636006209278E-5	8.161473909450935E-6
12	-2.2584308E-4	-7.113289974289535E-5	-1.9719923738504658E-4
13	2.7927183E-4	-1.1717549726308135E-4	2.337278073973402E-4
14	-9.342866E-5	-3.731272914225303E-5	8.250441847145314E-5
15	3.040381E-4	-9.71988554440474E-5	-6.57145621584173E-5
16	-6.677665E-5	-1.3795275076642813E-4	9.694632293975979E-5
17	1.8369351E-4	-2.037961824051007E-4	-3.974639878298724E-5
18	4.281573E-6	2.1762630678451002E-4	-2.877578343761576E-5
19	-7.198703E-5	-3.0471511343124283E-5	-3.7765875389680717E-6
21	5.567833E-5	-3.157694725086884E-4	-2.6421607340472388E-5
21	-1.4687602E-4	1.919956888616662E-4	3.4566782565660214E-4
22	1.3343166E-4	-1.3154755997787733E-4	3.581720733462795E-4
23	-6.4987694E-6	3.3356492591344147E-4	-9.125203005162731E-5
24	-2.4645723E-4	-9.835655041761319E-5	-1.4574955232310665E-5
25	-2.1859056E-4	2.647756470467249E-5	7.654749919495269E-5
26	2.8580273E-4	1.5624368898506038E-4	2.754087924615515E-4
27	-5.5816257E-5	4.1021651422784263E-4	-1.9723327897864433E-4
28	1.4712347E-4	2.0092325862907417E-4	-1.547899384711762E-5
29	1.2981605E-5	-1.819262341179625E-4	2.836863872212912E-5
31	2.8624047E-5	-8.624583730889093E-6	-1.2148632035706621E-5
31	3.2646824E-6	-8.840533479040253E-5	-7.000060510321514E-5
32	7.968281E-5	2.71987669383559E-4	1.4843409244356675E-5
33	9.652143E-5	8.403347251814077E-5	1.6948924830262145E-4
34	9.9623045E-5	-1.1597014620658666E-4	-1.514282796216004E-4
35	1.064314E-4	-7.225792519909055E-5	-8.744864723408883E-5
36	1.7035987E-4	7.245049654813003E-5	1.598602666310783E-4
37	1.9885749E-5	-1.5941206356735175E-5	-6.362473669379101E-6
38	6.133652E-6	-3.830167093794599E-5	7.697384623439351E-5
39	-7.823972E-5	-6.992617137755523E-5	-5.888149365756292E-5
41	2.824353E-4	7.353019473732897E-5	-2.2933288373947375E-4
41	-2.4895748E-5	1.5742267377152812E-4	2.1630926735352264E-5
42	-5.697093E-6	-1.0985343102065E-4	-2.504341580683614E-4
43	8.2694736E-5	-1.7245269694649509E-4	7.254166797585626E-5
44	2.5467292E-5	2.2487876945594622E-4	2.0548529382314118E-4
45	2.4062477E-4	-7.905360501057621E-5	1.5461975032975698E-4
46	3.4126715E-5	1.7112169403164508E-4	1.615700103818281E-4
47	-4.831197E-5	-6.496676085012466E-5	5.152254908236853E-5
48	-1.01670834E-4	2.0111567921464823E-4	1.1241350572772928E-4
49	-2.773388E-7	-1.2298497229653053E-4	-5.90598567093907E-5
51	8.874881E-6	1.1298872074989558E-5	7.840348363832737E-5

Comb07 :

Test	PC	HAP	VAP
1	6.7391906E-5	-3.530503243242834E-5	1.5239856543632478E-4
2	-1.3582835E-4	-1.6129914687785537E-4	-4.3492385765334884E-6
3	1.50113565E-5	-2.44267354570511E-4	2.532701827315373E-4
4	-7.908602E-5	-3.337571618832254E-5	-6.508626899483118E-5

5	-4.2861277E-5	-1.4598046161840136E-4	-3.132107494684784E-5
6	-2.1674461E-4	1.7465167567902654E-4	-1.5017779886351528E-4
7	-1.9623929E-4	2.822169195340762E-4	-1.8255403749061893E-4
8	9.864442E-5	1.3091220166312626E-4	-6.193298411918582E-5
9	-1.9146672E-4	1.599094938792549E-4	-3.561020075555483E-5
11	-1.3703547E-4	2.4073780084843308E-5	2.719578930136534E-5
11	-3.7483085E-4	2.082361539397672E-4	-6.446081150892916E-5
12	-1.4976671E-4	-7.45740638793346E-5	2.989192712645879E-4
13	2.1411768E-4	1.5718540895131845E-4	3.0574723253465516E-5
14	1.8300561E-4	-1.6957865034727425E-4	-7.69798517008767E-6
15	-4.554264E-5	3.975268687665554E-5	3.124487571370722E-5
16	7.1264665E-5	3.614789920876219E-5	4.381375398564385E-5
17	5.5704546E-5	8.912016246762429E-5	-1.798159072049035E-4
18	-8.382948E-5	1.5629151163334902E-4	3.027249177693038E-4
19	-5.348548E-5	2.1454125299370206E-4	-2.6881279670537274E-4
21	2.7711936E-5	-1.693010340596468E-6	1.3837737149131181E-5
21	2.7942643E-4	4.1285484853469204E-4	-1.325552475900618E-4
22	4.955918E-5	6.0578699550828386E-5	-1.5483221462478982E-4
23	-1.631101E-4	-1.2682017330297831E-4	7.129956105964364E-6
24	9.2644965E-5	1.3931230819418003E-4	-3.321968993844066E-5
25	6.8779256E-5	-1.3053668974785204E-4	-9.862205704111141E-5
26	1.4408586E-4	2.2964255103091966E-4	1.258201729141192E-4
27	-4.8110356E-5	-3.3601337799332736E-4	-2.166563601336409E-4
28	-1.17176416E-4	3.8617409817910476E-5	1.1547707810376643E-4
29	-8.794038E-6	-2.021953666749554E-4	-1.779311973120507E-4
31	-3.482095E-5	-1.3621486236410228E-4	9.193493959322453E-5
31	-5.1008796E-5	4.0536346707003994E-5	-1.670197571349994E-5
32	2.2134787E-4	8.64493042894034E-5	-6.106371382051543E-5
33	-3.1610898E-4	-3.57412657844976E-5	-4.448641320940311E-5
34	8.265144E-5	2.9629944051661004E-6	-7.629695629453986E-5
35	-6.676293E-5	1.448391637092962E-4	2.8498505854231956E-4
36	-1.4936038E-4	6.955106123227798E-5	-1.460666807096033E-4
37	-6.464087E-5	2.2711108994000174E-4	-9.391263118167147E-5
38	-5.1768115E-5	2.497199958491144E-4	-8.789803174547761E-6
39	-2.3936307E-5	-8.5645280830061E-5	-3.168896938842285E-5
41	2.5272251E-5	1.0213790980765361E-4	-8.526431150145041E-5
41	1.20282035E-4	4.465014910223323E-5	-5.5588738371592076E-5
42	-8.261648E-6	4.525028941645034E-5	-4.1723686711886194E-5
43	1.4537197E-4	1.8812107565917732E-4	2.3560256581680506E-6
44	4.1403477E-5	2.0856107486869112E-4	-7.272652229422609E-5
45	-7.259222E-5	5.3161811943076705E-5	-1.2125976007015143E-4
46	-3.084714E-5	9.50493245134893E-5	2.807086978369628E-4
47	-2.6997664E-5	9.286442724374556E-5	1.366284039596668E-4
48	-9.455286E-5	1.0430609649137198E-4	1.8834859892772306E-4
49	-6.576964E-5	2.341974694273387E-4	-1.4652999438036495E-4
51	-2.987006E-5	1.6039345416587355E-4	-1.8587736682733408E-5

Comb08 :

Test	PC	HAP	VAP
1	-6.8894435E-5	1.4842692596151813E-4	1.6876216425502647E-4
2	-1.7083388E-4	2.7808695249580855E-4	1.0025905074631686E-4
3	-4.5195968E-5	5.066620488719697E-4	-1.430219906994645E-4
4	-7.431238E-5	2.7150154971519004E-4	-2.953110929651435E-4
5	-1.0659333E-4	-1.508728639103106E-4	-1.2127758648888394E-4
6	1.8103408E-4	-2.4749699031177103E-5	2.501863953669733E-4
7	-2.306216E-5	5.110455050465335E-4	1.8278541693935395E-4
8	-1.0208712E-4	1.326948936541679E-4	-4.090732840342057E-5
9	4.6932724E-5	2.468690468154633E-4	2.284134757197027E-5
11	-5.7922338E-5	1.5814791014467323E-4	-4.9964049196025534E-5
11	2.5465063E-4	3.3374142419720685E-4	7.842072269010406E-5
12	-8.002577E-5	3.5461518168339415E-4	7.414807352523994E-5
13	-1.6423156E-4	1.8808266146249907E-4	1.4996842782884423E-5
14	2.2665947E-4	1.8642700364680264E-4	8.893149822140477E-5
15	-2.2175096E-4	2.530283823385296E-4	1.319392290286567E-4
16	-2.509861E-5	1.0512359537380846E-4	2.524885427514785E-4
17	-7.4797767E-6	2.2999608886819825E-4	-9.370466334669257E-5
18	1.632925E-4	4.719684548567578E-4	2.0260318257574167E-4
19	-2.512458E-4	2.526701506820115E-4	2.4330944348765428E-5
21	-4.5397832E-5	1.9062600234701999E-4	2.0540224518532415E-4
21	8.905703E-5	4.430527553848678E-4	1.4492321679751005E-4
22	1.8128325E-4	1.8692810772617674E-4	-2.448104518422577E-5
23	-1.8236079E-4	2.5256289993471715E-4	1.4860475398717273E-4
24	7.145755E-5	8.080536257218524E-5	-1.530918510655852E-4
25	3.17569E-5	4.967339834277443E-4	-6.834166247915006E-5
26	5.89088E-5	2.2826159331315878E-4	1.0331916474678093E-4
27	1.4365799E-4	1.5200774659818118E-4	1.9415239872081847E-4
28	1.3687112E-4	1.7320593505433941E-6	9.068612296869869E-5
29	3.8116843E-5	8.540956681650143E-5	2.2207193944811765E-5
31	-1.3794457E-4	2.5421274696115165E-5	-1.8006817144049298E-4
31	-1.4809362E-4	2.4636144937414505E-4	-6.3409083923471316E-6
32	7.4486234E-5	4.5358747833472755E-4	-6.193210849455563E-5
33	-1.7347859E-4	3.724299763656502E-4	-4.788110633138673E-5
34	-2.2796994E-4	1.1369312559409248E-4	-3.15811890476443E-4
35	-1.4322199E-4	1.922946363471623E-4	-1.6213814577986137E-4
36	4.6026733E-5	2.9102929794650514E-4	-8.552493378585382E-5
37	-2.1196879E-4	3.238576081724803E-4	-1.8346177268709397E-4
38	-2.9231835E-5	3.746743665527007E-4	-8.785474063140999E-5
39	3.1395914E-5	3.641722476782798E-4	1.772215426754698E-5
41	-3.0675562E-4	1.639406980951306E-4	1.9306475206426983E-4
41	-2.4195916E-4	3.517371694960212E-4	-6.146728213415388E-5
42	-2.6371182E-4	2.812310680833439E-4	1.0753262226560614E-4
43	-4.092081E-5	1.2722621963146897E-4	8.307248671201166E-5
44	-1.02517515E-4	4.5504995631373514E-4	-1.589901021079907E-4
45	-2.1707496E-5	2.623036053787958E-4	3.293699259177024E-5
46	6.943821E-5	3.269393280478309E-4	1.5397426669216954E-4

47	-6.7390494E-5	3.768696593589002E-4	2.0317294384344676E-4
48	-7.3133655E-5	6.013540868436483E-4	-2.039711435922506E-6
49	-2.3523938E-4	2.389606779492859E-4	-3.6793004814999027E-4
51	-2.9713818E-4	8.200307417663952E-5	-2.266206188128192E-4

L'image ETM 20010603 Ismal(ch. 1).tif (2734 x 2561)
Comb01:

Test	PC	HAP	VAP
1	-6.53763E-4	-5.4961668599644586E-5	9.644247022009466E-5
2	5.7950107E-5	4.921091698463763E-4	6.213156331128719E-5
3	-7.454266E-4	4.496140717985498E-4	1.2726821163027628E-4
4	1.495833E-4	7.038586787033794E-5	1.359170739262684E-4
5	-1.526373E-4	3.0356633487592296E-4	-2.507172370916171E-4
6	1.21017765E-4	9.868064100863443E-5	-6.239065607385482E-4
7	4.683562E-4	9.069575713604733E-4	1.475266334826572E-4
8	-4.5401265E-4	5.466212513300538E-4	-1.6434186050508584E-4
9	-1.2387414E-4	3.298714123281245E-4	-2.1427190205863084E-5
11	1.143733E-4	4.496747271837648E-4	-8.89718170159401E-5
11	-2.4696335E-4	6.360673455547351E-4	1.3154689103291498E-4
12	6.3935923E-4	2.485741331729128E-4	-6.462967571555962E-4
13	-1.2277279E-4	4.707570128684271E-5	3.701014579858752E-5
14	-2.9476467E-4	2.1919995314490163E-5	-4.024635387600026E-4
15	5.370555E-4	-2.497335991254837E-5	-3.074345653899289E-4
16	-5.3270377E-4	8.267880729414767E-4	-1.5171562801135775E-4
17	-2.5659177E-4	2.4134964100523793E-4	-1.2428157264812855E-4
18	-6.336124E-4	5.36008385076726E-4	-4.310084076947025E-4
19	-3.3229677E-4	2.1159405331206373E-4	1.0388880639846464E-4
21	1.6932233E-4	9.09218569786676E-5	3.518461557959252E-4
21	-9.302435E-4	0.00131551196843986	3.5062418910519464E-6
22	1.7823406E-4	2.6554313782337966E-5	3.644217851960627E-4
23	1.5055653E-4	2.0650491666858513E-4	-4.790956395987592E-4
24	-7.760063E-5	-1.2644007563816835E-4	-2.1367671402151194E-4
25	-2.463311E-4	-2.2441858327349918E-4	8.787585725623966E-4
26	-1.3960416E-4	-1.8365028681042946E-4	-4.901306671736051E-6
27	-8.265747E-5	3.252166710790409E-4	-6.778455471389647E-4
28	3.31715E-4	5.420490013337534E-4	-2.967507634955421E-4
29	-4.3803413E-4	1.732291308631076E-4	1.3926385033266527E-4
31	2.3089393E-5	3.8730272617324275E-4	-4.251149489315893E-4
31	7.138535E-6	6.988554331308583E-4	4.369849163753158E-4
32	-2.441701E-4	5.042850406569379E-4	-3.261518588151726E-4
33	-3.195493E-4	1.8539884424125498E-4	2.988544651200817E-4
34	-2.424225E-4	-8.201576675806716E-5	4.1489844372644147E-4
35	-1.05544445E-4	-2.1679951543268448E-4	2.769492230494415E-4
36	9.0341107E-4	6.477135371188911E-4	2.2258427716333515E-5
37	2.7409254E-4	3.8942707935765133E-4	-5.32599519582156E-4
38	6.597125E-4	1.6518359737835044E-5	-7.84452074708707E-4
39	-8.543341E-4	4.32321140467352E-4	-2.4268516315919066E-4

41	3.6920162E-4	5.310017162648798E-4	-2.1987163532727932E-5
41	-4.6608297E-4	3.46455348600229E-4	2.432250131802202E-4
42	-2.812906E-5	3.665567267524414E-4	-9.02081902245796E-4
43	-4.511418E-4	9.456651072605166E-5	-9.737226909627133E-4
44	-3.998957E-4	-1.9784026848769775E-4	8.883311606828946E-4
45	2.4761824E-4	3.285361204184251E-4	1.56589268175813E-4
46	-0.001336232	7.280962063957429E-4	3.6172652857066395E-4
47	4.584352E-4	5.064269994145604E-4	8.515763390387732E-5
48	6.9158076E-4	3.9291776530269806E-4	3.8156922342879175E-4
49	-6.228868E-5	2.4175257370352514E-4	-1.788929212155833E-4
51	1.6377706E-5	-2.289939713484968 7E-4	9.967116395014669E-6

Comb02:

Test	PC	HAP	VAP
1	-3.1830044E-4	-6.155073481541183E-4	1.4821156931169849E-4
2	3.7801055E-5	2.5630652521559414E-4	6.310468259705021E-5
3	2.3072433E-5	1.8930383060968613E-4	6.206854942725862E-4
4	-6.7468366E-4	-5.74427900021058E-4	-4.3801784838535595E-5
5	2.9819531E-4	-7.651484016136086E-4	-2.2103769895120599E-4
6	-5.2741426E-4	3.1539622906888107E-4	1.462229968564439E-4
7	8.4415294E-4	1.6401262770578397E-4	-6.519469410945333E-5
8	1.5773869E-4	-2.0358567634094947E-4	1.3695208666188922E-5
9	5.6520676E-6	1.9302220497790968E-5	-4.682030632716269E-4
11	9.004526E-5	-3.5007550569836864E-4	-1.4949590995671317E-4
11	1.4514521E-6	8.408004327359884E-4	2.2195732285894797E-4
12	2.532033E-4	3.442699148810158E-4	9.289810557438298E-5
13	9.8211196E-5	-1.6438504255275284E-4	2.499457844534161E-5
14	3.115573E-4	3.1868166206863805E-4	1.8638208347314012E-4
15	-1.3385266E-4	-9.136563196602923E-4	2.6585666151388097E-4
16	-1.1044361E-4	-4.8695873175559867E-4	1.3515999828196012E-4
17	-2.9364837E-4	-4.980830688644394E-4	-5.779017260185184E-4
18	1.0517595E-4	2.204569932170704E-4	1.676897802676326E-4
19	7.390047E-5	-3.340619300087991E-4	4.544479647398985E-4
21	5.3848076E-4	4.903972930453441E-4	-6.366919719671239E-4
21	-1.3857913E-4	-4.346830818307884E-4	-2.518001289853644E-4
22	-2.1946362E-4	3.107355819753067E-4	6.333196837628676E-4
23	2.941048E-4	8.335053859281361E-4	1.1342621986186533E-4
24	1.6433217E-4	-2.327419453356155E-4	-3.6711515094276734E-4
25	-3.3835336E-4	-2.351770066858035E-5	2.82724834446866E-4
26	5.0314696E-4	4.700071647898828E-4	-5.856578229445834E-4
27	-1.7004813E-5	4.8553713372766784E-5	2.3994255012100722E-4
28	6.241385E-5	-6.114493421576791E-4	-3.0123881569646383E-4
29	8.174874E-5	6.355838342680262E-4	5.289262871229822E-4
31	-6.672485E-5	1.4450760932780955E-4	-2.5982834708845355E-4
31	-3.1793385E-4	1.363479378959461E-4	-1.0095063755750453E-4
32	2.6100525E-4	3.8464300397269755E-4	4.818730165882665E-5
33	1.4224254E-4	3.662635626509689E-6	-5.102459496826106E-4

34	-2.277665E-4	1.6602045153008707E-4	2.1157223359826748E-4
35	-2.914153E-4	-7.239964250028308E-5	3.546917592136603E-4
36	3.5615807E-4	-6.838314383667341E-4	-3.012053377599084E-4
37	-5.331656E-4	-2.155872357784927E-4	-4.704375637017378E-4
38	-2.4147224E-4	6.548578290815682E-5	1.2168351515945487E-4
39	2.10797E-4	5.34641029524196E-4	2.669104335917636E-4
41	-3.1848834E-4	3.050835097361054E-4	-5.350581588488544E-4
41	-7.815172E-6	1.5396365246752919E-4	5.06274961960863E-4
42	4.058959E-4	-6.468962636667911E-4	-1.567203832815638E-5
43	3.5091958E-4	4.093145408902239E-4	-5.767081023741728E-4
44	-1.5328913E-4	-1.8700918605258414E-4	-5.369167950672815E-5
45	2.197627E-4	-8.224993662125858E-4	8.023785167037115E-5
46	3.6881497E-4	-1.7133899900360347E-4	1.580954921365215E-4
47	-1.4172438E-4	3.8395808985348327E-4	3.025216122591878E-4
48	-4.556812E-7	-2.451339248477271E-4	-1.6192824121528552E-4
49	-5.008187E-4	-3.2097773261814384E-4	5.156762104417244E-4
51	2.6126608E-4	2.090484027870625E-6	4.2038532921203096E-4

Comb03:

Test	PC	HAP	VAP
1	-5.8137466E-6	-5.504505480817668E-5	-3.9505046301797377E-4
2	-8.36526E-5	6.181902680790866E-4	-5.564837956090717E-4
3	1.0072659E-4	3.7688294947369887E-4	4.741511205614673E-4
4	-8.13531E-5	4.657047431348071E-4	-2.807755021956064E-4
5	-1.6533877E-4	4.010812447467868E-4	-2.2626175798249934E-4
6	-9.146304E-5	-1.3804467689676022E-4	4.257366998940646E-4
7	1.8120531E-4	3.4753961801216825E-4	1.2578333561006575E-4
8	5.9495237E-6	-0.0010067147285494613	-3.5321433987256935E-4
9	5.04847E-4	-4.3640955749611103E-4	-9.366338486181407E-4
11	2.5078647E-5	-4.557418517399573E-4	-3.136568615620931E-4
11	-1.6526868E-4	-1.0729258705305474E-4	-1.6353987163741758E-4
12	-1.5051794E-4	-9.56571302673396E-4	-8.544888939952431E-5
13	3.3386587E-4	6.241889949239693E-4	-5.30246416503122E-4
14	3.142228E-4	2.530824962973128E-4	-1.2782640281052256E-4
15	1.903913E-4	1.2016672691453174E-4	-3.1214507613412727E-4
16	2.1389402E-4	-2.957383700355402 7E-5	-3.4595592156335493E-4
17	-4.4660206E-5	-8.280641207216001E-4	-6.156059230777472E-4
18	-7.730987E-5	-1.4249786392612636E-4	-5.013426331292062E-5
19	6.448894E-5	9.158095930039703E-5	-2.5060056648871257E-4
21	2.2205907E-4	-1.0117537064504233E-4	-4.3642605177059287E-4
21	3.5891164E-4	-2.634577027808641E-4	-4.9742684357819436E-5
22	6.7681394E-4	-5.653621839516566E-4	1.9371433444146323E-4
23	-5.273601E-4	2.189368219631872E-4	-9.589952460285178E-6
24	-6.1343086E-4	3.833362501974762E-4	-5.546823495358588E-4
25	2.0425793E-4	-1.4598924790089563E-4	4.980398464076866E-4
26	-5.0135277E-4	7.526718317921801E-4	-1.5339837428660416E-4
27	-4.060447E-4	6.760847018577669E-5	-9.020523690490606E-4

28	2.1250058E-4	6.041816378939183E-4	-1.355068810953987E-4
29	-1.7636234E-4	2.6348662530273017E-4	8.599496636262397E-6
31	-1.7011559E-4	5.222694451423154E-4	7.677048569634143E-5
31	1.0120767E-4	4.468639490535896E-4	1.5873083009939748E-5
32	1.2061826E-4	-5.880613135713509E-4	6.124868000810392E-4
33	-1.8134483E-4	5.151710792831066E-4	3.0197471934478826E-4
34	8.315343E-5	3.2949109862269433E-4	9.441440538224137E-5
35	4.5951478E-5	3.3047028345748993E-4	-2.2241037153018764E-4
36	-1.8674381E-4	4.8041099568138106E-4	1.1504506652964973E-4
37	-2.4919474E-4	3.013384709880137E-4	-4.960947280754535E-4
38	9.850083E-5	-2.423581476630441E-4	-1.3533349762282146E-4
39	7.630242E-5	5.075946758671072E-4	-9.685332871764813E-4
41	-8.348629E-6	-4.188045265938876E-4	-2.1697080854949827E-4
41	1.4997953E-4	4.269006701138867E-4	1.0577005547739389E-4
42	7.9149596E-4	3.5332618291249163E-4	2.841837641166982E-4
43	-4.2689778E-4	2.349747362698608E-4	-2.491883486272802E-4
44	-3.5798977E-4	-5.1634278739969935E-5	3.163747736874199E-4
45	-1.481763E-4	4.0861712087816914E-4	7.415188591180011E-5
46	-3.3795215E-5	-6.167864109050767E-6	-2.3205412102803797E-4
47	-2.4957003E-4	5.937464731600297E-4	-1.6881728425087954E-4
48	7.2669087E-4	3.084275761526358E-4	2.1324142262621937E-4
49	-4.4562927E-5	-1.0955599447231078E-4	-2.703376974815588E-4
51	-5.036957E-4	-0.001005016677561647	-1.2045335584447766E-4

Comb04:

Test	PC	HAP	VAP
1	-1.3615847E-4	0.002528756535791656	2.448279748910026E-4
2	-5.3102436E-4	0.0032887660651640905	-3.23915043851957E-4
3	-8.387821E-5	0.002372312024799111	-1.7455654867229328E-4
4	-3.6720245E-4	0.0024870461160992775	3.013246994621692E-4
5	7.286655E-5	0.002802146015267595	5.933260250928449E-4
6	-5.7210866E-5	0.0025163896085600786	-5.409234658337252E-4
7	8.410162E-4	0.0027127100753974835	2.7693336882347934E-4
8	-4.6594997E-4	0.0019940527047324712	3.974488369994387E-4
9	-2.342832E-4	0.0029280155621629086	2.4212935791934116E-4
11	-3.1704686E-4	0.0020632308783814896	4.5470513116945954E-4
11	3.3662893E-4	0.0024952579838556973	-6.252053637255344E-4
12	-2.8676225E-4	0.002586682543061888	4.2147166288871097E-4
13	-1.7268727E-4	0.002662160650470958	1.6224392405967888E-4
14	-6.09249E-6	0.0015871148725152546	-2.221558728047666E-6
15	-1.4853619E-4	0.002616665586489277	2.802109675647696E-4
16	-1.7752104E-4	0.0025941226052300804	1.2358214807459475E-4
17	4.7675127E-4	0.0032664295212459335	-1.5069137653518246E-5
18	-1.8540974E-4	0.002616773557914332	-1.0701714986765883E-4
19	-2.6049488E-4	0.002841870831475301	-2.7077983584445617E-4
21	-5.192828E-4	0.002243843281195442	7.355195030587395E-4
21	8.545008E-5	0.0022001627381695423	1.2552848052549949E-4

22	1.7292167E-4	0.002613314779248774	-1.68076009444401E-4
23	1.5720777E-4	0.0025342405251601295	5.69446046040511E-4
24	3.9642226E-5	0.00242096696661924	7.630223564329613E-4
25	-3.6315672E-4	0.002163285439127791	-2.0513832666622318E-4
26	-7.339014E-4	0.0023193521803028016	-5.672236424999925E-4
27	-8.9496534E-5	0.00264070005472561	5.937059698299484E-4
28	-1.5658257E-4	0.0022034439865657035	5.72452783874761E-4
29	-4.4006828E-4	0.0029675483845333995	9.291093735442897E-5
31	1.1504037E-6	0.0025057695817607534	6.332402689138336E-4
31	-2.6581262E-4	0.003135410947193472	-1.8715656657535568E-4
32	2.1280798E-4	0.0025972595013247775	-3.2357147250506734E-4
33	2.9661515E-4	0.002845724066412457	-1.9854810722591066E-4
34	-8.1281825E-5	0.002180023508225652	-2.173634821407853E-4
35	5.444568E-5	0.002075786853316203	5.651928121448944E-4
36	-9.5544376E-5	0.0027780283358955805	-3.712897712065804E-4
37	-3.2394135E-4	0.0018416988434352766	3.112652830360271E-4
38	2.5643897E-4	0.0027660915092928944	1.5561542589843596E-4
39	3.884766E-4	0.0025039150464709558	-1.2105239236582443E-4
41	7.086223E-5	0.0026568134573604716	1.0437181995401168E-4
41	-4.862694E-4	0.0026030503242037823	-5.544106063321625E-4
42	6.405175E-4	0.0025942732737292726	6.66580359953023E-4
43	-1.643861E-4	0.0022669316656496402	7.176743817929037E-5
44	5.3138664E-4	0.0022576246919776524	3.511968017905704E-4
45	4.931385E-4	0.002761576979113961	-1.9800678955517625E-5
46	2.8759465E-4	0.0025914267087640127	-4.3432722794665583E-4
47	1.2517505E-4	0.0019154598698955445	4.7900018209109935E-4
48	-3.7261858E-4	0.0018706907809719394	7.206120471303198E-5
49	2.3661982E-4	0.0025014203087028323	1.8872613837790162E-4
51	-1.0149054E-4	0.0022532226832478156	2.202709254381329E-4

Comb05:

Test	PC	HAP	VAP
1	-3.0814033E-6	-3.5405956242977977E-4	-5.4746179177540264E-5
2	2.195341E-4	-7.793837426390387E-4	-0.00121719744513913
3	-4.8624328E-4	-2.949607353778422E-4	-2.5807906431827405E-4
4	-4.2966462E-4	-9.844289935278538E-4	-4.1132632440621315E-5
5	-2.9268107E-4	-0.0010686553345168356	6.951043876017045E-5
6	-5.5241183E-4	-0.001121961750148707	-4.274937312838923E-5
7	-5.953546E-4	-0.0012426646914560334	3.2740321342545676E-4
8	3.703444E-4	-0.0014958252485431653	-3.7390473209779557E-4
9	7.0255337E-4	-0.0011661177568569583	1.095871646009901E-5
11	4.6040062E-4	-0.001202826686788107	2.1925840924238857E-4
11	2.993871E-4	-0.0010790064563880395	-2.9193281555784826E-4
12	-2.3471977E-4	-0.001285970130353011	3.4180824125091023E-4
13	2.7694716E-4	-0.0011951190270613732	1.7944519794991877E-4
14	-3.5253118E-4	-0.0016044271217662961	-4.096346081664046E-4
15	4.2364252E-4	-0.0012765664564617775	-4.7362622078473747E-5
16	-2.3919047E-4	-0.0013696819419493184	5.092371421319774E-4

17	2.326824E-5	-0.0013692881967046686	-1.2271583624936738E-4
18	3.2628988E-4	-0.0024314978283808443	3.253372674831796E-4
19	-6.561718E-4	-0.00201618318849881	-8.729231901290269E-5
21	9.929772E-5	-1.439579155487202E-4	-3.275243947988446E-4
21	2.5706936E-4	-0.0014297352979463131	-4.474094273059986E-4
22	5.144352E-4	-0.001678832569043786	-2.5998650353706526E-4
23	2.8505767E-4	-9.134155314998455E-4	2.7663387816626364E-4
24	-3.8087985E-6	-0.0017244503023188238	5.502834970203406E-4
25	2.996614E-4	-0.0017870158906682604	4.7237112629245926E-4
26	-6.37016E-4	-0.0022293384165030417	-6.732039670385692E-4
27	-1.0957653E-4	-0.0020435401486934473	7.180350097522154E-4
28	1.2722133E-4	-0.001160399579840165	-1.336022419745654E-4
29	7.1633345E-5	-0.0016471192706984594	3.4652678014202997E-4
31	-4.2424E-5	-0.0010326611685913022	-2.5479463636508213E-4
31	7.2967836E-5	-0.0015370484049019805	8.494632156959033E-4
32	2.6086732E-4	-0.0021397086010445363	-7.288747498039033E-5
33	-2.4066381E-4	-0.0017336076362960973	-6.040275253220945E-4
34	-5.827565E-4	-5.213952244975265E-4	-3.3689001334933423E-4
35	-1.7326965E-4	-9.599095403018352E-4	-1.4865231874579843E-4
36	-3.151917E-4	-0.0013259891200440128	-1.4729024577532E-4
37	3.880776E-5	-9.980720966596649E-4	2.3748930343967295E-4
38	8.157747E-4	-7.893852836182969E-4	-1.1852831163966438E-4
39	-8.621544E-5	-0.0017219300704279798	-1.4949326867254653E-4
41	-4.577307E-7	-0.0019418537315927266	-7.860634259652841E-4
41	1.80536E-4	-0.0020490103339181032	-2.826653478869498E-4
42	-5.792522E-4	-0.0011481461254261773	-6.206586241457349E-4
43	1.4803556E-4	-0.0010942870971254281	-8.652919766182893E-4
44	2.060556E-4	-0.001134151203004404	2.062933758169175E-4
45	2.2091462E-4	-0.0010004023803381159	4.4099737386426056E-4
46	2.5749413E-4	-0.001099809040193698	-2.640591849208301E-4
47	-2.9044427E-4	-0.0011035720151170028	3.689520651536748E-4
48	5.829217E-4	-0.0019913560023651585	-6.185843505333045E-5
49	9.459505E-5	-0.00105761504582295	6.72836657385835E-5
51	-2.5256307E-4	-0.0013000919886386303	1.5590880724043217E-5

Comb06:

Test	PC	HAP	VAP
1	4.582512E-4	-1.2885623867580538E-	-1.5615342603692584E-4
2	1.4735541E-4	-3.975182223370681E-4	1.7101471921367084E-4
3	-4.727848E-4	3.8763580092229956E-4	-1.863692693404923E-4
4	-3.951817E-4	3.801503732225442E-4	-1.9756257009658344E-4
5	-7.447769E-4	1.6158898204629232E-4	6.289778793209417E-4
6	5.7380163E-4	-3.851194213523303E-5	3.276472102466529E-4
7	-2.343223E-4	-4.5011515720424247E-4	-1.9783284721465994E-4
8	1.418099E-4	-2.63275253226224E-4	5.353074362289716E-4
9	-2.1493118E-4	2.3278073813382737E-4	4.261603991838259E-4
11	4.5017825E-4	-3.1436228122666457E-4	8.20886580875227E-4
11	2.9099535E-4	-8.681593541300314E-4	-3.345773527372199E-4

12	4.1081916E-4	2.490789672337361E-4	2.1547529898467813E-4
13	-4.320799E-4	6.21900901045565E-5	2.3742600578631048E-4
14	8.3656465E-5	-3.877683005916209E-5	-5.379073359211347E-4
15	9.184289E-4	-4.938764766255092E-4	1.87615271454677E-4
16	-5.618258E-4	-6.648591041355092E-4	-3.0068144549419786E-4
17	-8.7212924E-5	5.625461107855422E-4	1.3422249413399864E-4
18	-3.6154734E-4	4.6922765025829216E-4	2.1398496572123154E-4
19	8.522871E-6	-2.785084758708539E-5	-2.5499085438557463E-4
21	8.067238E-4	8.060549748301058E-4	-5.513906325817551E-4
21	9.301865E-4	8.90985344464391E-5	-1.1712381542452626E-6
22	-1.7307489E-4	-4.753206506292571E-4	9.274665471282666E-5
23	5.6454814E-5	-8.37847726631041E-5	6.57429880236005E-4
24	-6.4519903E-4	-4.720740709849715E-5	2.446656025127278E-4
25	-5.198333E-4	1.9668359305831384E-4	-3.766248537996513E-4
26	6.72069E-5	2.6111916900875857E-4	5.473553531516033E-4
27	1.9227194E-4	-2.7896112268648525E-4	-8.401874623807048E-4
28	-6.416429E-5	-4.953341320604063E-5	2.123194947786167E-5
29	9.485456E-4	5.853991283789327E-4	-3.410341013984401E-4
31	-9.281332E-5	4.8299399884259205E-4	-3.796287572215597E-5
31	5.0033367E-4	-2.635770834004589E-4	-2.162245765760001E-4
32	-4.95216E-4	6.59981606365396E-5	-7.828921468307655E-4
33	-5.03798E-5	7.925679244401358E-4	2.4535431311108506E-4
34	6.7046612E-6	4.5212054978971984E-5	-2.530871074738802E-4
35	7.226765E-5	-4.677761755795381E-4	1.395327563609836E-4
36	1.8410865E-5	-3.5732106595781773E-4	-6.608589706839098E-4
37	-4.017688E-4	2.8961337418072756E-4	1.1728315725326164E-4
38	1.1950648E-4	-4.136451514591671E-4	3.183014725905695E-4
39	-7.235002E-4	3.188098021118365E-4	-1.0255763548658773E-5
41	6.9999136E-4	6.803917987674242E-5	3.919788469297769E-4
41	-4.916223E-4	4.7153855558867635E-5	4.896617204112917E-4
42	3.1902426E-4	-1.8904296582780773E-4	3.1993714543058616E-5
43	3.758863E-4	4.538061475184097E-4	5.458575059226079E-4
44	-2.7113665E-5	2.922673943180015E-4	1.7964756101057644E-4
45	3.2713986E-4	-4.5295773961400555E-4	-2.3458826021794432E-4
46	-4.3136213E-4	-1.2642402458688208E-6	-3.7807843964147986E-4
47	1.5460071E-4	1.956856849600834E-5	1.266890863957662E-4
48	-8.4981835E-4	-1.3890837462425115E-5	5.562305033031844E-4
49	5.685604E-4	3.770879578733448E-5	8.565119118970243E-4
51	-8.00245E-4	1.5543927281426415E-5	2.944763780116905E-4

Comb07:

Test	PC	HAP	VAP
1	1.4263502E-4	1.5556670344992495E-5	-1.4624609373072443E-4
2	2.8744485E-4	-4.67633349020335E-4	7.53021787718695E-5
3	-1.7635874E-5	4.6754828483711654E-4	-1.344956241144592E-5
4	-7.0556E-5	-3.7469134385658976E-4	-5.624158110096623E-4
5	4.7689452E-4	2.1175981774317523E-4	-4.8063310695460506E-4
6	-4.1646132E-4	2.885939632477511E-4	-1.4952358263917452E-4

7	-3.0709643E-4	2.536920513573651E-4	-3.6962989342252076E-4
8	1.0947291E-5	-2.360464399059385E-4	-3.169844430810918E-4
9	3.4669845E-4	8.911390994841342E-4	3.880987486070749E-4
11	1.159993E-4	-1.7190412244748226E-4	4.943407271391017E-4
11	1.3763356E-4	3.7996879358362606E-4	2.980048747400306E-4
12	-3.0704116E-4	-1.6387081365467262E-4	-2.3676245376047934E-4
13	5.0879928E-5	-2.6264617061030605E-4	3.367481393807982E-4
14	-8.923498E-4	5.870882743113085E-4	2.8473777225070064E-4
15	-1.9274722E-4	-1.6374870897682106E-4	-2.2664826967414904E-4
16	-4.090161E-5	-3.98129499783951E-4	5.814180284134734E-5
17	2.4892896E-4	1.979134638468736E-4	-9.615728686378679E-4
18	1.7608707E-4	7.444625958274095E-4	-5.014881120241064E-4
19	2.0403603E-4	9.741050655842908E-5	7.836823398300365E-5
21	-6.636263E-4	-2.2486639309708455E-5	-1.7812556218427952E-4
21	3.4584955E-4	-3.785415921728297E-5	3.5961372035823297E-4
22	-2.5985314E-4	9.864138884201624E-5	1.3156965333553568E-4
23	-3.2539928E-4	1.7733336915990927E-4	3.121320967409297E-4
24	2.589777E-4	6.073592908538995E-4	-1.0237464087559549E-4
25	-4.0685854E-4	8.04029281442052E-5	1.1111498943672798E-4
26	-1.0479422E-4	-2.9040382951266933E-4	4.123992257994191E-4
27	-1.5571494E-4	-2.6462120110748715E-4	-9.784433281411066E-5
28	3.2017057E-4	2.422186739957053E-4	3.2351154252426197E-4
29	-8.48312E-5	3.209605929615185E-4	-3.448001037476971E-4
31	0.0010664668	-1.744362844073031E-5	-1.6526472421815702E-4
31	-4.320051E-4	-8.429661675179305E-6	-2.9657792230146346E-4
32	-1.5064591E-4	2.867076723554061E-4	-3.008035804231358E-4
33	6.215771E-4	-7.106871793008552E-4	-2.8318873728855776E-4
34	1.8824734E-4	-1.386145118145008E-4	4.953529632835901E-4
35	4.612428E-4	7.498658226945518E-4	-2.037494098248689E-4
36	-2.2164462E-4	-3.4399852538421447E-4	-2.4105921130980612E-4
37	6.1087124E-4	5.185515210025535E-4	-2.964112069438112E-4
38	-4.3625882E-4	-2.1805260105848707E-4	-6.875198513303977E-4
39	-2.0977229E-4	-7.212219374560418E-4	4.2627654188987895E-4
41	1.8666667E-4	1.7378643644912412E-4	2.107257383957136E-4
41	-9.7043475E-4	3.5465192821770126E-4	8.623919967028204E-5
42	3.9850513E-4	1.3714178046164124E-4	7.150660624611325E-6
43	-3.2273112E-4	1.283017879978339E-4	-9.090652385290631E-4
44	-7.225073E-5	-3.6060513736804067E-4	-4.078957829098791E-4
45	2.768774E-4	1.4704491616873857E-4	7.570580613559461E-4
46	1.1309279E-4	-3.841670545997528E-5	-2.337125147833646E-4
47	-3.5586278E-4	5.169102470327856E-4	4.443417798854774E-5
48	-5.0269722E-5	0.0012959145836844372	3.102543466393283E-4
49	-4.530211E-4	2.0848197999268861E-4	4.4888313250856675E-4
51	-1.4510388E-4	1.5117842256363282E-4	9.720774621083997E-5

Comb08:

Test	PC	HAP	VAP
1	6.2662184E-5	3.468213087424913E-4	1.9732540224968485E-4

2	-6.73652E-5	4.0055699210808285E-4	2.1491994445226528E-4
3	2.322492E-4	8.479325985962126E-4	3.9442927003002673E-4
4	-5.8598054E-4	2.1063719278502957E-4	-8.81079029748206E-5
5	-4.912639E-4	2.9321902043214464E-4	3.663153044853755E-6
6	1.0956569E-4	7.568628759441351E-4	5.404064882124855E-4
7	-4.4889466E-4	5.722066586715684E-4	5.18279903052017E-4
8	5.8692286E-4	3.519194159842054E-4	-3.3829248703123237E-4
9	-3.754841E-4	-7.520732031432831E-4	3.6962876694975137E-4
11	2.53395E-4	-2.4201971897748644E-4	-1.9417631658578416E-5
11	3.632196E-4	6.259244456432511E-4	-1.533634533076621E-4
12	7.711633E-5	7.511957713864516E-4	4.4336920917414615E-4
13	-8.486072E-5	6.457945108004313E-4	-1.1686041902049297E-4
14	-9.593038E-5	-4.8714309081911644E-5	5.79729919309662E-4
15	-6.714798E-5	4.878942113139652E-4	1.1099188028238718E-4
16	1.42275385E-5	-3.68247473030545E-5	-1.0609258226865883E-4
17	5.484808E-4	-3.5239227999046976E-4	-5.008737569467239E-4
18	9.512439E-5	5.584282734434655E-4	-4.291068223471381E-4
19	-1.14450095E-5	1.6318159076281034E-4	-2.586491668916228E-4
21	-3.8764576E-4	3.468526120248754E-4	2.758797274979541E-4
21	1.688315E-4	-6.624474161398489E-4	-9.96196213658692E-5
22	-2.952745E-4	4.910433992738235E-4	-2.804913638067639E-4
23	-3.053897E-5	4.3915791194968817E-5	-3.970051313139156E-5
24	3.7274632E-4	-3.818493253359402E-4	-2.3136483859850765E-4
25	2.4212267E-4	-1.9923402522015028E-4	1.3412265632855628E-4
26	8.4851054E-4	-5.841914894253111E-4	-6.225621154009765E-5
27	1.21573095E-4	1.6871105925766864E-4	-2.6278454924092224E-5
28	-5.7534035E-4	1.9304806256837583E-4	-1.4496631439524075E-4
29	6.1302E-4	-3.483807646369923E-4	-2.673656323550433E-4
31	-3.983316E-4	4.4367217341222007E-4	-8.556419187261775E-5
31	1.16195115E-4	0.0010220180823175122	5.650109647709429E-4
32	5.194109E-5	4.6211119846347663E-4	-7.702480991524149E-4
33	7.740681E-5	5.585878872229988E-4	-4.941375358642332E-4
34	-2.467733E-4	6.764412837362104E-4	4.0902771594230876E-4
35	2.190809E-4	3.4493016069947366E-4	3.3168978863155397E-4
36	-4.4440074E-4	0.0010290501123342386	-4.510580113196215E-5
37	-3.1274327E-4	-6.725566198216066E-5	2.3473141990181597E-4
38	-6.172774E-4	-1.1938481489475163E-4	-3.4611570740335055E-4
39	-7.537002E-4	8.04250548415334E-4	-2.9759910574835713E-4
41	4.4805405E-4	-8.104659351616937E-5	-1.1445114239873825E-4
41	-1.15493494E-4	5.285887568201818E-4	-2.4603982823368084E-4
42	3.9101514E-4	4.3222529555203326E-4	1.506301174581437E-4
43	4.3656377E-4	9.807989995116223E-4	-2.4249191454387935E-4
44	8.4740535E-4	8.722249887380207E-4	-5.561774987054788E-4
45	3.2634882E-4	2.068896616262585E-4	9.109067416765635E-5
46	-3.78617E-4	-3.0030149673180553E-4	3.1008596251643595E-4
47	7.294605E-4	1.4154258920556032E-5	7.325356716220426E-5
48	-6.185231E-4	2.0486825346554264E-4	1.6077187723824692E-4
49	3.3968766E-4	4.1644126911719097E-4	1.1400631775798593E-4
51	-6.427144E-4	2.9644545144867967E-5	-4.893611575269875E-5

ANNEXE. B

Les résultants de NPCR, UACI et le temps d'exécution

L'image L71196000_00020010603_B10.FST (7036 x 7368)

Comb 01 :

Test	**NPCR**	**UACI**	**Temps**
1	99.17784000878991	33.387635012591275	13.187
2	100.0	18.73911803108037	13.187
3	99.66877726400413	33.62008513243969	13.594
4	99.41820652157139	36.03345382073596	13.578
5	99.81045402302044	35.45045734219329	13.594
6	99.7012610498883	25.81298711078983	13.625
7	99.82742892300742	34.970128703587406	13.593
8	99.69138474444134	33.65572163544488	13.594
9	99.68804377548935	35.02341484372494	13.594
10	99.58919777548564	38.39854273088883	13.578
11	99.42403199861238	34.20947068807186	13.594
12	99.49516840335325	29.226606417490412	13.593
13	99.78737008800405	34.216672497041046	13.594
14	99.48595952011033	29.297222523446898	13.609
15	99.71475223744613	32.729787090801125	13.578
16	99.35965276144587	35.50697320594025	13.609
17	99.47502614134598	30.255252375176195	13.594
18	99.68750559400114	35.14815138624043	13.594
19	99.49915171795247	29.536418169078072	13.594
20	99.72267064249688	34.224639979924405	13.609
21	99.75230920366732	36.220982810620434	13.578
22	99.34000817264275	31.803156386095722	13.593
23	99.67792442033803	35.19262563089781	13.61
24	34.136112305134944	99.64856941715601	13.578
25	99.34481129775271	34.016345669719584	13.593
26	99.83820605553323	25.01026225466447	13.61
27	99.46938970296394	37.064080077894964	13.593
28	99.90964723688751	40.77050285190624	13.594
29	99.502710660052	34.35486877075381	13.593
30	99.53120727340514	37.040697401579095	13.594
31	99.28470279110564	32.07509429173703	13.578
32	99.23349839108812	33.47623960317256	13.593
33	99.87038892273581	27.19146568707985	13.594
34	99.919888116891	43.18958012478391	13.593
35	99.80134930393652	34.24671245687404	13.594
36	99.41053502415681	36.000626906053114	13.578
37	99.87323607641544	33.71113304965546	13.594
38	99.21854890530413	33.60859826924334	13.578
39	99.52562870400034	27.437838243804162	13.594
40	99.19951772765965	33.49859954057509	13.594

41	99.83792249754482	30.78708186312002	13.578
42	99.79280205599989	33.635164834864746	13.593
43	99.96400356719808	43.4906647045736	13.609
44	99.93798374607032	42.073224196472566	13.594
45	99.62376870248185	33.75597309506368	13.594
46	99.85995514614154	33.67920930678699	13.61
47	99.85943046741468	35.65176982218864	13.594
48	99.51068693407998	34.483882103134846	13.578
49	99.90412846542583	34.31494462611523	13.578
50	99.24829355959949	33.53713579356736	13.609

Comb02:

Test	**NPCR**	**UACI**	**Temps**
1	99.17784000878991	33.406808313418395	16.969
2	100.0	18.74258337673141	18.484
2	99.66877726400413	33.611281135358645	18.516
3	99.41820652157139	36.03911490450578	18.563
4	99.81045402302044	35.44215324230715	18.563
5	99.7012610498883	25.807098651117833	18.437
6	99.82742892300742	34.94988808701561	18.531
7	99.69138474444134	33.660674675248046	18.359
8	99.68804377548935	35.02934038493641	18.438
01	99.58919777548564	38.39068636291242	18.5
00	99.42403199861238	34.21407208115465	18.5
01	99.49516840335325	29.22290206162269	18.5
02	99.78737008800405	34.22875921587898	18.547
03	99.48595952011033	29.289275713427905	18.562
04	99.71475223744613	32.72201120985035	18.469
05	99.35965276144587	35.495626983082296	18.516
06	99.47502614134598	30.245292783786937	18.516
07	99.68750559400114	35.13116188662168	18.344
08	99.49915171795247	29.531508186822307	18.453
11	99.72267064249688	34.21818939689699	18.219
10	99.75230920366732	36.2252041293548	18.469
11	99.34000817264275	31.79291325941505	18.438
12	99.67792442033803	35.19428283199482	18.344
13	99.64856941715601	34.12877592584337	18.453
14	99.34481129775271	34.01480248186949	18.547
15	99.83820605553323	25.013550952422193	18.5
16	99.46938970296394	37.04918253047818	18.453
17	99.90964723688751	40.75341773611003	18.437
18	99.502710660052	34.343317063850144	18.485
21	99.53120727340514	37.032840352793635	18.531
20	99.28470279110564	32.089853543662045	18.532
21	99.23349839108812	33.4633588614663	18.516
22	99.87038892273581	27.189599703811172	18.453
23	99.919888116891	43.1920276269479	18.438
24	99.80134930393652	34.24455632687711	18.438

25	99.41053502415681	35.97836577712279	18.578
26	99.87323607641544	33.70576591004371	18.359
27	99.21854890530413	33.60201231062521	18.516
28	99.52562870400034	27.430902363214205	18.437
31	99.19951772765965	33.4962957803595	18.468
30	99.83792249754482	30.788903699557917	18.375
31	99.79280205599989	33.641354167833384	18.469
32	99.96400356719808	43.50430839389855	18.422
33	99.93798374607032	42.07483086621402	18.406
34	99.62376870248185	33.7370506505793	18.532
35	99.85995514614154	33.658430501166876	18.437
36	99.85943046741468	35.65402348979265	18.5
37	99.51068693407998	34.475670154868915	18.531
38	99.90412846542583	34.319914898009344	18.531
41	99.24829355959949	33.51544094851496	18.359

Comb03:

Test	**NPCR**	**UACI**	**Temps**
0	99.17784000878991	33.404198853727486	16.906
1	100.0	18.740954255332568	17.828
2	99.66877726400413	33.61029881514264	17.828
3	99.41820652157139	36.030593323168766	17.797
4	99.81045402302044	35.44129115340372	17.812
5	99.7012610498883	25.806939870754096	17.797
6	99.82742892300742	34.951985213360594	17.812
7	99.69138474444134	33.65525582421452	17.797
8	99.68804377548935	35.024176354082876	17.844
01	99.58919777548564	38.38370568491257	17.86
00	99.42403199861238	34.21374032928766	17.828
01	99.49516840335325	29.22101987502624	17.828
02	99.78737008800405	34.22553870516779	17.828
03	99.48595952011033	29.29118941402633	17.828
04	99.71475223744613	32.71927203287983	17.969
05	99.35965276144587	35.49179268298063	18.5
06	99.47502614134598	30.242264882214005	18.203
07	99.68750559400114	35.13063872080766	17.969
08	99.49915171795247	29.529940610781903	17.844
11	99.72267064249688	34.214894329777415	17.875
10	99.75230920366732	36.21841665054058	17.813
11	99.34000817264275	31.794031514990014	17.875
12	99.67792442033803	35.189331214337386	17.859
13	99.64856941715601	34.12575298662902	17.843
14	99.34481129775271	34.01069460145966	17.859
15	99.83820605553323	25.011426820548767	17.843
16	99.46938970296394	37.044655406344205	17.844
17	99.90964723688751	40.74972327468824	17.813
18	99.502710660052	34.33901773924079	17.843
21	99.53120727340514	37.03086415368876	17.828

20	99.28470279110564	32.081386987007676	17.859
21	99.23349839108812	33.457727945228854	17.829
22	99.87038892273581	27.1842929899934	17.844
23	99.919888116891	43.18453059127192	17.828
24	99.80134930393652	34.23998373966416	17.812
25	99.41053502415681	35.97470407030371	17.828
26	99.87323607641544	33.70502574690665	17.843
27	99.21854890530413	33.59691457568654	17.813
28	99.52562870400034	27.433566302948503	17.844
31	99.19951772765965	33.49267837168267	17.812
30	99.83792249754482	30.78797265201207	17.797
31	99.79280205599989	33.63426629986916	17.812
32	99.96400356719808	43.494039683827104	17.813
33	99.93798374607032	42.068347286523725	17.828
34	99.62376870248185	33.738251813864075	17.829
35	99.85995514614154	33.65581769793913	17.813
36	99.85943046741468	35.6487665811253	17.828
37	99.51068693407998	34.47368003695009	17.844
38	99.90412846542583	34.31871193435471	17.781
41	99.24829355959949	33.52199197392338	17.812

Comb04:

Test	**NPCR**	**UACI**	**Temps**
0	99.17784000878991	33.40922508830774	16.141
2	100.0	18.743826145170875	17.203
3	99.66877726400413	33.618746188006035	17.063
4	99.41820652157139	36.03391436703979	17.062
5	99.81045402302044	35.4471948178634	17.063
6	99.7012610498883	25.804721196857965	17.094
7	99.82742892300742	34.95446607531274	17.062
8	99.69138474444134	33.66110759570915	17.078
9	99.68804377548935	35.03242234293303	17.094
10	99.58919777548564	38.38781761992406	17.078
11	99.42403199861238	34.21370117504777	17.079
12	99.49516840335325	29.22553002424772	17.094
13	99.78737008800405	34.218111324048984	17.078
14	99.48595952011033	29.29578864366088	17.078
15	99.71475223744613	32.72766002386949	17.079
16	99.35965276144587	35.492200125977945	17.063
17	99.47502614134598	30.25102039039363	17.078
18	99.68750559400114	35.131808642405815	17.078
19	99.49915171795247	29.53547759017068	17.078
20	99.72267064249688	34.22085038645199	17.094
21	99.75230920366732	36.209689539763204	17.078
22	99.34000817264275	31.795154642157925	17.078
23	99.67792442033803	35.187954885824745	17.078
24	99.64856941715601	34.135665889473245	17.062
25	99.34481129775271	34.010429690116965	17.109

26	99.83820605553323	25.01887990606278	17.062
27	99.46938970296394	37.05205349743482	17.078
28	99.90964723688751	40.749140318482866	17.125
29	99.502710660052	34.347467199962324	17.109
30	99.53120727340514	37.025645113278436	17.125
31	99.28470279110564	32.08530172875681	17.078
32	99.23349839108812	33.471504528936414	17.093
33	99.87038892273581	27.18234995397172	17.11
34	99.919888116891	43.18421437702989	17.125
35	99.80134930393652	34.241517502063395	17.172
36	99.41053502415681	35.978958960623636	17.093
37	99.87323607641544	33.70971189345064	17.094
38	99.21854890530413	33.60147477212206	17.047
39	99.52562870400034	27.438089251453597	17.141
40	99.19951772765965	33.502613302565564	17.063
41	99.83792249754482	30.792597222962613	17.312
42	99.79280205599989	33.631934580993025	17.672
43	99.96400356719808	43.49336646720283	17.922
44	99.93798374607032	42.072182554863225	17.219
45	99.62376870248185	33.745840411142225	17.157
46	99.85995514614154	33.67047502480452	17.25
47	99.85943046741468	35.653090218237196	17.093
48	99.51068693407998	34.47673039015097	17.109
49	99.90412846542583	34.321999179697066	17.11
50	99.24829355959949	33.520138532722605	17.094

Comb05:

Test	**NPCR**	**UACI**	**Temps**
1	99.17784000878991	33.39745299518801	11.344
2	100.0	18.738771029028204	10.75
3	99.66877726400413	33.61904701593312	10.734
4	99.41820652157139	36.03200697528805	10.703
5	99.81045402302044	35.44705833783928	10.734
6	99.7012610498883	25.80981628419315	10.734
7	99.82742892300742	34.96145018763402	10.813
8	99.69138474444134	33.65901860884334	10.766
9	99.68804377548935	35.023271283275314	10.75
10	99.58919777548564	38.39729799565679	10.703
11	99.42403199861238	34.21098711246695	10.719
12	99.49516840335325	29.2273316632834	10.734
13	99.78737008800405	34.218166515183775	10.75
14	99.48595952011033	29.294900169526894	10.765
15	99.71475223744613	32.72929068844231	10.734
16	99.35965276144587	35.49956723257937	10.797
17	99.47502614134598	30.24784832320759	10.765
18	99.68750559400114	35.14302289375128	10.75
19	99.49915171795247	29.533346877120266	10.796

20	99.72267064249688	34.219080715326825	10.781
21	99.75230920366732	36.2250786936207	10.844
22	99.34000817264275	31.800630862896245	10.735
23	99.67792442033803	35.1903513574075	10.719
24	99.64856941715601	34.13358490592084	10.765
25	99.34481129775271	34.012325871186476	10.719
26	99.83820605553323	25.012127451223925	10.735

27	99.46938970296394	37.05422885657363	10.75
28	99.90964723688751	40.76256452933607	10.922
29	99.502710660052	34.345497945148004	10.719
30	99.53120727340514	37.034948099788586	10.781
31	99.28470279110564	32.08237815777813	10.703
32	99.23349839108812	33.468273654789265	10.719
33	99.87038892273581	27.186765107313963	10.719
34	99.919888116891	43.186571906218035	10.703
35	99.80134930393652	34.246056048692466	10.703
36	99.41053502415681	35.98840066625339	10.703
37	99.87323607641544	33.707207868804026	10.735
38	99.21854890530413	33.60310711602364	10.734
39	99.52562870400034	27.4363324703266	10.703
40	99.19951772765965	33.49321545630908	10.687
41	99.83792249754482	30.79131026229433	10.735
42	99.79280205599989	33.63547463436154	10.75
43	99.96400356719808	43.49093506235999	10.781
44	99.93798374607032	42.07289748258982	10.75
45	99.62376870248185	33.747685864168695	10.828
46	99.85995514614154	33.67156450475611	10.953
47	99.85943046741468	35.65062176219369	11.016
48	99.51068693407998	34.48061782381799	10.921
49	99.90412846542583	34.316860596085604	10.844
50	99.24829355959949	33.52750474667912	10.875

Comb06:

Test	**NPCR**	**UACI**	**Temps**
1	99.17784000878991	33.40719318373235	10.907
2	100.0	18.743937783122984	10.297
3	99.66877726400413	33.60983183897701	10.281
4	99.41820652157139	36.03175515068591	10.297
5	99.81045402302044	35.444385880397796	10.296
6	99.7012610498883	25.809609862148225	10.312
7	99.82742892300742	34.94638753584234	10.297
8	99.69138474444134	33.6634353053546	10.313
9	99.68804377548935	35.03186625608832	10.281
10	99.58919777548564	38.38628279850466	10.296
11	99.42403199861238	34.21103404307755	10.297
12	99.49516840335325	29.22140096303802	10.297
13	99.78737008800405	34.231431627932025	10.328

14	99.48595952011033	29.289729481856984	10.297
15	99.71475223744613	32.71768218673661	10.297
16	99.35965276144587	35.49307961340291	10.297
17	99.47502614134598	30.24272456615372	10.312
18	99.68750559400114	35.13366513970757	10.312
19	99.49915171795247	29.53447902125019	10.297
20	99.72267064249688	34.217614640701335	10.313
21	99.75230920366732	36.22402523616847	10.281
22	99.34000817264275	31.790504760159816	10.312
23	99.67792442033803	35.186099795507516	10.313
24	99.64856941715601	34.126846188336984	10.297
25	99.34481129775271	34.0149567537522	10.344
26	99.83820605553323	25.01319956290537	10.313

27	99.46938970296394	37.04395686349189	10.328
28	99.90964723688751	40.75568158562163	10.266
29	99.502710660052	34.337640276054735	10.328
30	99.53120727340514	37.03003642307722	10.297
31	99.28470279110564	32.08849455312861	10.312
32	99.23349839108812	33.46184864001386	10.297
33	99.87038892273581	27.187906086873063	10.281
34	99.919888116891	43.18521448911088	10.313
35	99.80134930393652	34.24109016425525	10.312
36	99.41053502415681	35.97262903250528	10.297
37	99.87323607641544	33.70729812926655	10.312
38	99.21854890530413	33.597390009045135	10.297
39	99.52562870400034	27.436494685011358	10.297
40	99.19951772765965	33.49576480792011	10.297
41	99.83792249754482	30.78838790163082	10.312
42	99.79280205599989	33.637812783110185	10.312
43	99.96400356719808	43.50336742161699	10.328
44	99.93798374607032	42.08068274361253	10.297
45	99.62376870248185	33.738748503662165	10.313
46	99.85995514614154	33.65800647663678	10.313
47	99.85943046741468	35.653696533849	10.313
48	99.51068693407998	34.47739657179217	10.281
49	99.90412846542583	34.31842845958208	10.297
50	99.24829355959949	33.515963751227915	10.344

Comb07:

2	100.0	18.7418646969856	10.687
3	99.66877726400413	33.60840372339507	10.594
4	99.41820652157139	36.03183541079387	10.547
5	99.81045402302044	35.43932903953129	10.594
6	99.7012610498883	25.80556426842365	10.578
7	99.82742892300742	34.947789538520446	10.656
8	99.69138474444134	33.65804398936598	10.734
9	99.68804377548935	35.026232798158965	10.797

10	99.58919777548564	38.38657299061593	10.64
11	99.42403199861238	34.21149926426801	11.047
12	99.49516840335325	29.219386577990043	10.75
13	99.78737008800405	34.226478088860915	10.906
14	29.28780615912162	99.48595952011033	10.953
15	99.71475223744613	32.71922688751314	10.859
16	99.35965276144587	35.49479498604262	10.859
17	99.47502614134598	30.24171020240572	10.875
18	99.68750559400114	35.12888752234187	10.938
19	99.49915171795247	29.52883722715934	10.906
20	99.72267064249688	34.21553102468394	10.89
21	99.75230920366732	36.22052457910536	10.875
22	99.34000817264275	31.791780252929964	10.937
23	99.67792442033803	35.185311037575104	10.938
24	99.64856941715601	34.128602666877605	10.766
25	99.34481129775271	34.014271327862836	10.921
26	99.83820605553323	25.012913077429815	10.875

27	99.46938970296394	37.04585510209203	10.891
28	99.90964723688751	40.75238246387229	10.766
29	99.502710660052	34.33730502933799	10.968
30	99.53120727340514	37.02933373484784	10.797
31	99.28470279110564	32.087097966683615	10.796
32	99.23349839108812	33.461491410664706	10.844
33	99.87038892273581	27.18732093695219	10.828
34	99.919888116891	43.18244104461533	10.75
35	99.80134930393652	34.24174775251393	10.782
36	99.41053502415681	35.96937301371402	10.735
37	99.87323607641544	33.704818250689044	10.75
38	99.21854890530413	33.59764454177528	10.812
39	99.52562870400034	27.432121227607464	10.734
40	99.19951772765965	33.492933116214864	10.797
41	99.83792249754482	30.789283940342226	10.828
42	99.79280205599989	33.636856651441356	10.734
43	99.96400356719808	43.4976055021212	10.734
44	99.93798374607032	42.071188736519055	10.812
45	99.62376870248185	33.73619632291089	10.766
46	99.85995514614154	33.6579656884586	10.719
47	99.85943046741468	35.6507130514533	10.828
48	99.51068693407998	34.47655820537281	10.765
49	99.90412846542583	34.31732164163071	10.812
50	99.24829355959949	33.51339293137406	10.734

Comb08:

Test	**NPCR**	**UACI**	**Temps**
1	99.17784000878991	33.405721738268326	12.781
2	100.0	18.742973254781	11.985
3	99.66877726400413	33.61179082110716	12.0

4	99.41820652157139	36.0319616786252	12.0
5	99.81045402302044	35.44847813239199	12.031
6	99.7012610498883	25.80874311346471	12.062
7	99.82742892300742	34.95578674372442	12.141
8	99.69138474444134	33.65971933029503	12.015
9	99.68804377548935	35.028297623782215	12.062
10	99.58919777548564	38.385604407654185	11.984
11	99.42403199861238	34.21201432086206	11.968
12	99.49516840335325	29.22120756719466	11.969
13	99.78737008800405	34.23128322614961	11.922
14	99.48595952011033	29.290044001644528	12.0
15	99.71475223744613	32.7276812046723	12.109
16	99.35965276144587	35.495459927073234	11.953
17	99.47502614134598	30.244000391752834	11.969
18	99.68750559400114	35.133873074674476	11.953
19	99.49915171795247	29.532018780312775	12.0
20	99.72267064249688	34.21801229513143	12.031
21	99.75230920366732	36.220760987095645	12.031
22	99.34000817264275	31.79502554516837	12.079
23	99.67792442033803	35.19103029288086	12.063
24	99.64856941715601	34.127838070182406	12.031
25	99.34481129775271	34.012578543027665	12.015
26	99.83820605553323	25.012563730358494	12.125

27	99.46938970296394	37.05470474380604	12.016
28	99.90964723688751	40.755678287459475	12.094
29	99.502710660052	34.344247914719055	11.953
30	99.53120727340514	37.034666501029726	11.984
31	99.28470279110564	32.08524022878304	12.047
32	99.23349839108812	33.46473862429543	12.031
33	99.87038892273581	27.189564422641165	12.046
34	99.919888116891	43.19023482334114	12.0
35	99.80134930393652	34.243189378423196	11.921
36	99.41053502415681	35.976899823555414	12.031
37	99.87323607641544	33.70665349156967	11.969
38	99.21854890530413	33.60016638858943	11.859
39	99.52562870400034	27.435626710869936	11.922
40	99.19951772765965	33.49467800583527	11.985
41	99.83792249754482	30.79393799799496	12.078
42	99.79280205599989	33.638780851676735	11.906
43	99.96400356719808	43.503721610023696	12.062
44	99.93798374607032	42.07876631976292	12.032
45	99.62376870248185	33.738625685281804	12.0
46	99.85995514614154	33.663658452646175	12.047
47	99.85943046741468	35.65372113383219	11.953
48	99.51068693407998	34.4798816093876	12.0
49	99.90412846542583	34.31832313047077	12.079
50	99.24829355959949	33.5211930945923	12.031

L'image ETM 20010603 Ismal(ch. 1).tif (2734 x 2561)

Comb01 :

Test	NPCR	UACI	Temps
1	99.61201261280355	33.47315644100617	1.781
2	100.0	27.83255679784934	1.813
3	99.60432884580393	38.625685713739635	1.812
4	99.523992062583	36.925006854039985	1.813
5	99.3033765442872	33.753902994897956	1.812
6	99.2569311720144	33.469104246632284	1.828
7	99.75571905062917	32.51941170443835	1.812
8	99.84038330857294	30.824319328140298	1.844
9	99.63139341544014	33.49164032809036	1.813
10	99.85466540336778	35.09008980126629	1.828
11	99.67433967448821	34.98737387161931	1.828
12	99.7550906384582	39.58273532723174	1.812
13	99.67868143130583	33.928125340625805	1.828
14	99.45229594671294	33.774603463077675	1.813
15	99.98114763487081	33.718474494435725	1.828
16	99.82648683033757	30.99683459948891	1.812
17	99.44511205303114	29.257822261761586	1.813
18	99.24197781876421	33.75342194034194	1.829
19	99.73008269047244	34.14586427690937	1.828
20	99.33092670514644	31.83888556971699	1.829
21	99.75000621271124	26.453002718900077	1.829
22	99.66251409999809	27.7878174918865	1.812
23	99.40183730580279	30.712047893157674	1.813
24	99.97400658747341	28.212583009368952	1.812
25	99.30941787038542	33.15469451524826	1.828
26	99.63774894762385	39.115204905001974	1.813
27	99.39041162996692	35.75955649798151	1.812
28	99.6406482128672	39.106647073798385	1.813
29	99.753433915462	35.56010239548184	1.813
30	99.99301605564533	43.83301919340579	1.828
31	99.56081130296408	33.572527503997115	1.812
32	99.40449377543462	29.96325631370931	1.812
33	99.66010042597776	33.14730327917837	1.813
34	99.81269032676576	41.37687347084448	1.828
35	99.74395060451823	35.230507940768 29	1.812
36	99.62967956406476	32.942391624187515	1.812
37	99.68232336547852	33.62164060354565	1.813
38	99.29250787014834	33.48358567467268	1.828
39	99.39446774488864	35.465071689019005	1.828
40	99.48284534747907	33.829571549406175	1.812
41	99.79875100224601	37.78087169037359	1.828
42	99.99055953534062	33.71401993707347	1.812
43	99.86376309775208	29.78960922827468	1.813
44	99.2729842465638	34.051405358438494	1.813

45	99.39276817560807	35.76850666672807	1.844
46	99.72889727660447	34.151385398710396	1.813
47	99.7478496163972	35.48776985825554	1.828
48	99.74919213330793	35.24394067098004	1.812
49	99.80257860365101	38.653621547185764	1.813
50	99.79112436362556	35.056197438273585	1.828

Comb02:

Test	**NPCR**	**UACI**	**Temps**
1	99.61201261280355	33.46935314716347	2.281
2	100.0	27.838763628220025	2.469
3	99.60432884580393	38.620780738312384	2.469
4	99.523992062583	36.92629896355429	2.421
5	99.3033765442872	33.738766326753954	2.453
6	99.2569311720144	33.47173629668647	2.453
7	99.75571905062917	32.508063992033755	2.438
8	99.84038330857294	30.838092980363573	2.437
9	99.63139341544014	33.478383519677635	2.453
10	99.85466540336778	35.07924381045217	2.453
11	99.67433967448821	34.9695765892392	2.469
12	99.7550906384582	39.570935740547164	2.438
13	99.67868143130583	33.92513506203151	2.438
14	99.45229594671294	33.759829056071744	2.422
15	99.98114763487081	33.69795734112741	2.468
16	99.82648683033757	30.993277181710372	2.421
17	99.44511205303114	29.258867823116784	2.437
18	99.24197781876421	33.752654179733334	2.469
19	99.73008269047244	34.13511674854014	2.422
20	99.33092670514644	31.835014505936076	2.422
21	99.75000621271124	26.453548238909825	2.453
22	99.66251409999809	27.79263576659701	2.438
23	99.40183730580279	30.710701231636843	2.422
24	99.97400658747341	28.200988636788594	2.437
25	99.30941787038542	33.15645709376877	2.468
26	99.63774894762385	39.106566646001234	2.422

27	99.39041162996692	35.756808846973165	2.469
28	99.6406482128672	39.09722156333512	2.422
29	99.753433915462	35.54527937334456	2.454
30	99.99301605564533	43.821992632104546	2.453
31	99.56081130296408	33.5568882181342	2.438
32	99.40449377543462	29.94793963516342	2.437
33	99.66010042597776	33.13638313348726	2.469
34	99.81269032676576	41.37229614347538	2.422
35	99.74395060451823	35.21468416384959	2.454
36	99.62967956406476	32.93477327477926	2.422
37	99.68232336547852	33.62107682485716	2.421
38	99.29250787014834	33.491610195649976	2.422

39	99.39446774488864	35.447636779786286	2.422
40	99.48284534747907	33.826239284648935	2.453
41	99.79875100224601	37.76131104535339	2.422
42	99.99055953534062	33.71534688370158	2.453
43	99.86376309775208	29.78635582308482	2.468
44	99.2729842465638	34.03523802712895	2.453
45	99.39276817560807	35.75802461729323	2.422
46	99.72889727660447	34.149185956108134	2.438
47	99.7478496163972	35.4771135112569	2.406
48	99.74919213330793	35.24015686799942	2.438
49	99.80257860365101	38.63858345350033	2.422
50	99.79112436362556	35.03593041764532	2.437

Comb03:

Test	**NPCR**	**UACI**	**Temps**
1	99.61201261280355	33.466004528015695	2.266
2	100.0	27.845706630567925	2.406
3	99.60432884580393	38.618363087709014	2.39
4	99.523992062583	36.92116726687132	2.391
5	99.3033765442872	33.75457666170815	2.39
6	99.2569311720144	33.470314360128114	2.375
7	99.75571905062917	32.50154385170445	2.39
8	99.84038330857294	30.82860115616926	2.391
9	99.63139341544014	33.48241420686862	2.391
10	99.85466540336778	35.08249867185281	2.39
11	99.67433967448821	34.97462696199524	2.406
12	99.7550906384582	39.57890078080757	2.391
13	99.67868143130583	33.92201238002212	2.407
14	99.45229594671294	33.77148447760944	2.406
15	99.98114763487081	33.69843777959679	2.391
16	99.82648683033757	31.00330119596424	2.406
17	99.44511205303114	29.270108559825758	2.406
18	99.24197781876421	33.75790707819465	2.391
19	99.73008269047244	34.150065117064635	2.406
20	99.33092670514644	31.83552910941637	2.406
21	99.75000621271124	26.451503378986445	2.391
22	99.66251409999809	27.79332029899797	2.407
23	99.40183730580279	30.712684146479567	2.406
24	99.97400658747341	28.20997493083605	2.391
25	99.30941787038542	33.160687506259194	2.406
26	99.63774894762385	39.106322562201825	2.391

27	99.39041162996692	35.74854225849038	2.391
28	99.6406482128672	39.107901433780796	2.406
29	99.753433915462	35.55483448682423	2.391
30	99.99301605564533	43.82979715281994	2.391
31	99.56081130296408	33.574125418365455	2.406
32	99.40449377543462	29.957156122977686	2.421

33	99.66010042597776	33.14399464989199	2.375
34	99.81269032676576	41.37982980845533	2.391
35	99.74395060451823	35.21972087059997	2.391
36	99.62967956406476	32.941191480159546	2.391
37	99.68232336547852	33.620017373460556	2.391
38	99.29250787014834	33.479602706476086	2.39
39	99.39446774488864	35.46214201131359	2.39
40	99.48284534747907	33.81566851820192	2.406
41	99.79875100224601	37.765287292562654	2.39
42	99.99055953534062	33.72387827902455	2.391
43	99.86376309775208	29.78755574308471	2.407
44	99.2729842465638	34.04397598075203	2.391
45	99.39276817560807	35.77519696001053	2.39
46	99.72889727660447	34.15205749728979	2.39
47	99.7478496163972	35.483181441264925	2.39
48	99.74919213330793	35.23745536776158	2.407
49	99.80257860365101	38.64250279636465	2.422
50	99.79112436362556	35.04176512944188	2.407

Comb04 :

Test	**NPCR**	**UACI**	**Temps**
1	99.61201261280355	33.470949941374066	2.172
2	100.0	27.830221367303093	2.297
3	99.60432884580393	38.60554818410779	2.281
4	99.523992062583	36.92251460049271	2.313
5	99.3033765442872	33.7397651772639	2.281
6	99.2569311720144	33.47007867756293	2.312
7	99.75571905062917	32.524052881173056	2.281
8	99.84038330857294	30.83113519184258	2.281
9	99.63139341544014	33.49316095112467	2.297
10	99.85466540336778	35.09101796940417	2.281
11	99.67433967448821	34.97861306664658	2.281
12	99.7550906384582	39.584432712189255	2.281
13	99.67868143130583	33.928003242715235	2.297
14	99.45229594671294	33.77555011393046	2.281
15	99.98114763487081	33.714058246697284	2.296
16	99.82648683033757	30.99699187055564	2.282
17	99.44511205303114	29.264238562860655	2.297
18	99.24197781876421	33.749380051505675	2.297
19	99.73008269047244	34.138536610140385	2.281
20	99.33092670514644	31.833253495646037	2.313
21	99.75000621271124	26.447296153898463	2.297
22	99.66251409999809	27.79560207367326	2.281
23	99.40183730580279	30.701851821672022	2.296
24	99.97400658747341	28.215575640308987	2.281
25	99.30941787038542	33.1635691289167	2.282
26	99.63774894762385	39.11645579247645	2.297

27	99.39041162996692	35.75394917953696	2.282
28	99.6406482128672	39.097572398789175	2.297
29	99.753433915462	35.55831797375747	2.281
30	99.99301605564533	43.83693842425282	2.297
31	99.56081130296408	33.57674111401681	2.297
32	99.40449377543462	29.953310710959556	2.281
33	99.66010042597776	33.15041027888848	2.297
34	99.81269032676576	41.37487308143831	2.297
35	99.74395060451823	35.216213860215625	2.282
36	99.62967956406476	32.9326206550519	2.281
37	99.68232336547852	33.61334701910278	2.282
38	99.29250787014834	33.493891746292896	2.281
39	99.39446774488864	35.45934798550883	2.312
40	99.48284534747907	33.83398286842333	2.281
41	99.79875100224601	37.78172312725392	2.297
42	99.99055953534062	33.712847685135735	2.281
43	99.86376309775208	29.778353929427475	2.281
44	99.2729842465638	34.04327621411319	2.281
45	99.39276817560807	35.77035953048913	2.281
46	99.72889727660447	34.14331517502484	2.282
47	99.7478496163972	35.485268419362825	2.281
48	99.74919213330793	35.24237356112892	2.313
49	99.80257860365101	38.64994012722144	2.281
50	99.79112436362556	35.05876955953313	2.296

Comb05:

Test	**NPCR**	**UACI**	**Temps**
1	99.61201261280355	33.47585469276736	1.531
2	100.0	27.835578665072276	1.437
3	99.60432884580393	38.60402229630537	1.437
4	99.523992062583	36.928574577327936	1.422
5	99.3033765442872	33.74053092157553	1.437
6	99.2569311720144	33.47531802202947	1.422
7	99.75571905062917	32.520319709616494	1.438
8	99.84038330857294	30.826769463509045	1.438
9	99.63139341544014	33.48700777662278	1.453
10	99.85466540336778	35.09742766153612	1.437
11	99.67433967448821	34.97536851075849	1.438
12	99.7550906384582	39.59031861548852	1.438
13	99.67868143130583	33.93062879581254	1.438
14	99.45229594671294	33.78388144791031	1.422
15	99.98114763487081	33.707040193338074	1.437
16	99.82648683033757	30.992532272448464	1.438
17	99.44511205303114	29.25711118146311	1.437
18	99.24197781876421	33.749356976123764	1.437
19	99.73008269047244	34.14119722438021	1.437
20	99.33092670514644	31.83834990715076	1.422
21	99.75000621271124	26.450175648243697	1.438

22	99.66251409999809	27.79423166467115	1.453
23	99.40183730580279	30.71429639894993	1.422
24	99.97400658747341	28.208191965320832	1.438
25	99.30941787038542	33.152302180357	1.437
26	99.63774894762385	39.12125827286722	1.453

27	99.39041162996692	35.754088191929746	1.422
28	99.6406482128672	39.102628148334475	1.437
29	99.753433915462	35.55400242878437	1.437
30	99.99301605564533	43.82580544734854	1.438
31	99.56081130296408	33.57355066206586	1.438
32	99.40449377543462	29.968578886386787	1.437
33	99.66010042597776	33.143253213140056	1.438
34	99.81269032676576	41.37517059707986	1.437
35	99.74395060451823	35.223942545804746	1.422
36	99.62967956406476	32.931370215641955	1.422
37	99.68232336547852	33.622492824543876	1.422
38	99.29250787014834	33.48652543385274	1.437
39	99.39446774488864	35.461460391339	1.422
40	99.48284534747907	33.82892678283226	1.421
41	99.79875100224601	37.77616756040155	1.437
42	99.99055953534062	33.725073382315045	1.437
43	99.86376309775208	29.784346248336984	1.468
44	99.2729842465638	34.037454272189834	1.437
45	99.39276817560807	35.763749104921985	1.453
46	99.72889727660447	34.143734900583276	1.422
47	99.7478496163972	35.483675209683966	1.438
48	99.74919213330793	35.24627542942768	1.422
49	99.80257860365101	38.65508683410076	1.437
50	99.79112436362556	35.05341875871765	1.437

Comb06:

Test	**NPCR**	**UACI**	**Temps**
1	99.61201261280355	33.464233660280165	1.453
2	100.0	27.84549514354955	1.39
3	99.60432884580393	38.62440122134216	1.375
4	99.523992062583	36.92764271264664	1.375
5	99.3033765442872	33.75026010858539	1.375
6	99.2569311720144	33.478333952387324	1.375
7	99.75571905062917	32.5252811413265	1.375
8	99.84038330857294	30.834689025093336	1.375
9	99.63139341544014	33.490929471827904	1.375
10	99.85466540336778	35.08862193797187	1.375
11	99.67433967448821	34.98513175076559	1.39
12	99.7550906384582	39.579117644616154	1.375
13	99.67868143130583	33.92343543674641	1.391
14	99.45229594671294	33.77213719734435	1.375
15	99.98114763487081	33.71336934565711	1.375
16	99.82648683033757	31.003728762676523	1.375
17	99.44511205303114	29.273505570080093	1.375
18	99.24197781876421	33.77490534738529	1.375
19	99.73008269047244	34.15020032089486	1.375

20	99.33092670514644	31.84504512915989	1.375
21	99.75000621271124	26.446283637388827	1.375
22	99.66251409999809	27.79105947139811	1.375
23	99.40183730580279	30.707861167078597	1.375
24	99.97400658747341	28.203995493815505	1.39
25	99.30941787038542	33.151974868353186	1.375
26	99.63774894762385	39.109334571981854	1.375

27	99.39041162996692	35.76188263116432	1.375
28	99.6406482128672	39.109227260245355	1.375
29	99.753433915462	35.55539871358179	1.375
30	99.99301605564533	43.82284810158431	1.375
31	99.56081130296408	33.58180985746772	1.375
32	99.40449377543462	29.968593896588875	1.375
33	99.66010042597776	33.148785144532795	1.39
34	99.81269032676576	41.38903845512069	1.375
35	99.74395060451823	35.22008245963485	1.391
36	99.62967956406476	32.93321187776791	1.375
37	99.68232336547852	33.621862060031276	1.391
38	99.29250787014834	33.487834457855726	1.375
39	99.39446774488864	35.456427941215054	1.375
40	99.48284534747907	33.834161310600805	1.375
41	99.79875100224601	37.76747575755181	1.375
42	99.99055953534062	33.724850469620996	1.375
43	99.86376309775208	29.791860982544303	1.375
44	99.2729842465638	34.04689031220663	1.39
45	99.39276817560807	35.77739147388757	1.375
46	99.72889727660447	34.16029540956948	1.39
47	99.7478496163972	35.473692529495224	1.375
48	99.74919213330793	35.24730250807623	1.375
49	99.80257860365101	38.651643897117296	1.375
50	99.79112436362556	35.04785915927408	1.375

Comb07:

Test	**NPCR**	**UACI**	**Temps**
1	99.61201261280355	33.47561901020239	1.484
2	100.0	27.843517269450636	1.406
3	99.60432884580393	38.61152526879106	1.438
4	99.523992062583	36.919740737640325	1.406
5	99.3033765442872	33.74446941924781	1.406
6	99.2569311720144	33.47575253376022	1.407
7	99.75571905062917	32.51290993480155	1.406
8	99.84038330857294	30.83017375482721	1.406
9	99.63139341544014	33.481797668439796	1.406
10	99.85466540336778	35.08374675891565	1.407
11	99.67433967448821	34.97490084216442	1.407
12	99.7550906384582	39.58585364060131	1.407
13	99.67868143130583	33.92162704350023	1.406
14	99.45229594671294	33.772015323473006	1.422

15	99.98114763487081	33.70253825302611	1.407
16	99.82648683033757	30.990161332698623	1.422
17	99.44511205303114	29.268142111404096	1.406
18	99.24197781876421	33.76805509463721	1.406
19	99.73008269047244	34.133699068604216	1.406
20	99.33092670514644	31.834884006798347	1.407
21	99.75000621271124	26.44877029011515	1.406
22	99.66251409999809	27.78833399964535	1.406
23	99.40183730580279	30.71347845498134	1.406
24	99.97400658747341	28.205366910962514	1.406
25	99.30941787038542	33.14884412115771	1.406
26	99.63774894762385	39.109512006008465	1.406

27	99.39041162996692	35.74843035407762	1.407
28	99.6406482128672	39.10778773710512	1.406
29	99.753433915462	35.550817689667205	1.406
30	99.99301605564533	43.818043380862655	1.406
31	99.56081130296408	33.57232475426124	1.422
32	99.40449377543462	29.963765652413493	1.406
33	99.66010042597776	33.15494862453885	1.391
34	99.81269032676576	41.38196887420383	1.406
35	99.74395060451823	35.22131856093539	1.406
36	99.62967956406476	32.93296936219712	1.406
37	99.68232336547852	33.6081997521382	1.406
38	99.29250787014834	33.48951123179458	1.421
39	99.39446774488864	35.44424189785374	1.406
40	99.48284534747907	33.8352983893764	1.406
41	99.79875100224601	37.76216976330564	1.406
42	99.99055953534062	33.72669201972746	1.422
43	99.86376309775208	29.784247785895417	1.406
44	99.2729842465638	34.03995940763103	1.422
45	99.39276817560807	35.763991284444955	1.391
46	99.72889727660447	34.14181269864998	1.406
47	99.7478496163972	35.48779730228577	1.406
48	99.74919213330793	35.24075234734029	1.391
49	99.80257860365101	38.65443142597363	1.406
50	99.79112436362556	35.04210308301338	1.407

Comb08:

Test	**NPCR**	**UACI**	**Temps**
1	99.61201261280355	33.4590074217312	1.656
2	100.0	27.825743062455345	1.547
3	99.60432884580393	38.60283525820098	1.547
4	99.523992062583	36.91891640873284	1.547
5	99.3033765442872	33.74079147179122	1.547
6	99.2569311720144	33.46708447839003	1.563
7	99.75571905062917	32.508357699112786	1.547
8	99.84038330857294	30.82445150752433	1.546

9	99.63139341544014	33.482610459657245	1.547
10	99.85466540336778	35.08550564089374	1.547
11	99.67433967448821	34.97941544033341	1.562
12	99.7550906384582	39.57765224567825	1.563
13	99.67868143130583	33.9205088954993	1.562
14	99.45229594671294	33.77345596677531	1.562
15	99.98114763487081	33.695745688737475	1.547
16	99.82648683033757	30.983359359032637	1.546
17	99.44511205303114	29.25827144764206	1.546
18	99.24197781876421	33.75379069843042	1.563
19	99.73008269047244	34.12836484621662	1.547
20	99.33092670514644	31.829673450546895	1.578
21	99.75000621271124	26.448639006861107	1.547
22	99.66251409999809	27.788335679891297	1.562
23	99.40183730580279	30.70922743146732	1.547
24	99.97400658747341	28.204856900155168	1.562
25	99.30941787038542	33.153895838104205	1.562
26	99.63774894762385	39.11175983970468	1.563

27	99.39041162996692	35.7488363016183	1.546
28	99.6406482128672	39.09513940193742	1.579
29	99.753433915462	35.55426264294787	1.547
30	99.99301605564533	43.81958674323148	1.547
31	99.56081130296408	33.571719865533694	1.547
32	99.40449377543462	29.951142184888436	1.579
33	99.66010042597776	33.13426042213946	1.562
34	99.81269032676576	41.367498591804704	1.578
35	99.74395060451823	35.212569965754184	1.547
36	99.62967956406476	32.93229401513636	1.546
37	99.68232336547852	33.601087604978176	1.547
38	99.29250787014834	33.48750423341868	1.578
39	99.39446774488864	35.45425247013397	1.546
40	99.48284534747907	33.82607674880781	1.563
41	99.79875100224601	37.76923452751409	1.563
42	99.99055953534062	33.71346590381195	1.578
43	99.86376309775208	29.77746832753146	1.547
44	99.2729842465638	34.04243261838032	1.563
45	99.39276817560807	35.757592681934945	1.547
46	99.72889727660447	34.14066621049334	1.547
47	99.7478496163972	35.488447109590595	1.563
48	99.74919213330793	35.24390673000217	1.547
49	99.80257860365101	38.64191370196225	1.563
50	99.79112436362556	35.043294265726374	1.563