Crypto-Système Chaotique: Détermination du Régime Transitoire de l'Attracteur de Lorenz

Naima HADJ SAID & Adda ALI-PACHA & Lahcen MERAH & Mohamed Sadek ALI-PACHA

Université des Sciences et de la Technologie d'Oran USTO
BP 1505 El M'Naouer Oran 31036 ALGERIE
Phone / Fax : 213 / 041 -- 46 26 85
E.Mail: nim_hadj@yahoo.fr

Résumé :

Depuis quelques années, les chercheurs s'intéressent à la possibilité d'utiliser des signaux chaotiques dans les systèmes de transmission de données afin de transmettre des quantités importantes d'informations sécurisées.

Le chiffrement d'un message par le chaos s'effectue en superposant, en tenant compte de certaines restrictions, à l'information initiale un signal chaotique. Une des ces restrictions est que l'apparition du chaos n'est possible qu'à partir d'un état initial (germe) et après un régime transitoire.

Dans cette communication on essaye de mettre en évidence l'intérêt de bien connaître l'intervalle temporelle du régime transitoire de chaque attracteur, et que sa borne supérieure de cette intervalle est un champ constituant la clé sécrète des crypto-systèmes chaotiques. Des données sous forme de textes et images fixes sont utilisées pour valider l'étude.

Mots Clés : Chaos, Sensibilité aux conditions initiales, Attracteur, Lorenz, Chiffrement à continu.

1. Introduction :

Il existe de nombreuses études [1, 2, 3] qui ont prouvé que les systèmes chaotiques peuvent être l'alternative à l'avenir des communications sécurisées.

Puisque plusieurs systèmes cryptographiques se basent sur la génération des séquences pseudo-aléatoires pour masquer les messages, les attracteurs chaotiques avec ses caractéristiques intrinsèques comme la haute sensibilité aux conditions initiales ainsi que l'aspect aléatoire des signaux générés ; sont devenus capables de remplacer ses générateur pseudo aléatoires.

Un changement très infinitésimal de l'ordre de 10^{-11} sur l'un des paramètres d'un système chaotique donne un état totalement différent à long terme. En effet les attracteurs chaotiques peut être sensibles à des changements inférieure à 10^{-11} selon l'environnement de travail, comme Matlab; on peut atteindre la sensibilité à des erreurs jusqu'à10^{-15}. C'est ce qu'on veut montrer dans ce travail.

2. Théorie du chaos

Une condition nécessaire à l'apparition du chaos est que le système soit non linéaire. A partir d'un état initial x_0 (germe) et après un régime transitoire, la trajectoire d'un système dynamique atteint une région limitée de l'espace des phases. Ce comportement asymptotique obtenu pour t, k $\rightarrow\infty$ est une des caractéristiques les plus importantes à étudier pour tout système dynamique [4] (c'est le but de ce travail). Si dans le cas d'un système linéaire la solution asymptotique est indépendante de la condition initiale et que cette dernière est unique, en présence de non-linéarités, il existe une plus grande variété de régimes permanents, parmi lesquelles on trouve, par ordre de complexité : points fixes, solutions périodiques, solutions quasi-périodiques et chaos.

Le "chaos" est le terme utilisé pour décrire le comportement apparemment complexe de ce que nous considérons être simples [5]. Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe non linéaire. Du point de vue mathématique la notion générale de système dynamique est définie à son tour à partir d'un ensemble de variables qui forment le vecteur d'état $\mathbf{x} = \{x_i \in R\}$, i = 1...*n* où *n* représente la dimension du vecteur. Ce jeu de variables à la propriété de caractériser complètement l'état instantané du système dynamique générique. En associant en plus un système de coordonnées on obtient l'espace d'état qui est appelé également *l'espace de phase* [4], il s'agit d'un espace de dimensions deux ou trois dans lequel chaque coordonnée est une variable d'état du système considéré [6]. Conjointement avec l'espace d'état un système dynamique est défini aussi par une loi d'évolution, généralement désignée par *dynamique*, qui caractérise l'évolution de l'état du système en temps [7, 8, 9].

Un système dynamique est un système classique qui évolue au cours du temps soit de façon discrète (à temps discret) décrits chacun par une équation de la forme $x_{k+1} = f(x_k)$, soit de façon continu (à temps continu) décrits par des équations différentielles. Les seconds, cependant, sont discrétisés pour les besoins du calcul informatique : on les simule par un pas de temps très petits par

rapport à l'échelle de temps du phénomène étudié. Un système dynamique possède en général un ou plusieurs paramètres dits « de contrôle », qui agissent sur les caractéristiques de la fonction de transition. Selon la valeur du paramètre de contrôle, les mêmes conditions initiales mènent à des trajectoires correspondant à des régimes dynamiques qualitativement différents. La modification du paramètre de contrôle peut conduire à une modification de la nature des régimes dynamiques développés dans le système.

La notion de déterminisme provient du fait que le système considéré est complètement caractérisé par son état initial et sa dynamique.

2.1 Systèmes dynamiques à temps continu

Soit l'équation différentielle $\dot{x}$ (t)=$F(x(t), t)$ (1)

Où $\boldsymbol{F}$:$R^n \times R^+ \rightarrow R^n$désigne la dynamique du système en temps continu. Si on associe à cette dynamique un état initial$x_0 = x(t_0)$, pour chaque couple choisi (x_0, t_0) on peut identifier une solution unique $\Phi(.; x_0, t_0) : R^+ \rightarrow R^n$ telle que :

$\Phi_F(t_0; x_0, t_0) = x_0$ et

$$\dot{\Phi}_F(t; x_0, t_0) = F(\Phi_F(t; x_0, t_0), t) \quad (2a)$$

Cette solution unique déterminée avec l'aide des équations (2), et qui fournit l'ensemble d'états successifs occupés par le système à chaque instant *t*, s'appelle généralement trajectoire. Si F ne dépend pas explicitement du temps, mais seulement de *x*, le système est dit autonome.

Notons qu'un système dynamique non autonome peut toujours être ramené à un système autonome [10] en introduisant un nouveau degré de liberté θ=t, régi par l'équation :

$$d\theta/dt=1 \quad (2b)$$

2.2 Systèmes dynamiques à temps discret

Le système dynamique dans ce cas est représenté par des équations aux différences finies, avec le modèle général suivant :

$$x(k + 1) = G(x(k), k) \quad (3)$$

Où G : $R^n \times R^+ \rightarrow R^n$ désigne la dynamique du système en temps discret. De même qu'en temps continu, si on associe à cette dynamique un état initial $x_0 = x(t_0)$, pour chaque couple choisi (x_0, t_0) on peut identifier une solution unique $\Phi(.; x_0, t_0)$ de $R^+ \rightarrow R^n$: telle que :

$\Phi_G(k_0; x_0, k_0) = x_0$ et

$$\Phi_G(K + 1; x_0, k_0) = G(\Phi_G(k; x_0, k_0), t) \quad (4)$$

En temps discret on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k.

2.3 Attracteurs Chaotiques

Un attracteur signifie que la dynamique a tendance à être attirée par lui. Par exemple, le fleuve est un attracteur du bassin fluvial. La notion d'attracteur était développée à partir des systèmes dynamiques afin de fournir une représentation de l'évolution du système en fonction du temps. Dans les systèmes dynamiques possédant peu de degrés de liberté, il est possible de fournir une représentation graphique qui serve de base pour décrire tout phénomène dépendant du temps [11, 12, 13]. Un attracteur est la limite asymptotique des solutions partant de toute condition initiale située dans un bassin d'attraction qui est un domaine de volume non nul.

Dans les systèmes chaotiques, ces attracteurs sont forcément des courbes beaucoup plus complexes qui présentent une symétrie interne, nous les appelons des attracteurs étranges. Dans le plan, ils sont formés d'une suite infinie de points qui dépendent d'une valeur initiale. Au fur et à mesure que le nombre de points augmente, une image se former dans le plan et devient de plus en plus nette. Cette image n'est pas une courbe ni une surface, c'est en fait un objet intermédiaire constitué de points avec entre eux des espaces inoccupés. L'objet est qualifié d'étrange en raison de sa structure pointilliste et de sa nature fractale.

La majorité des attracteurs à temps continu sont définis par un système d'équations différentielles qui n'ayant pas des solutions analytiques sauf des approximations par des méthodes numériques comme les méthodes d'Euler, Runge-Kutta... etc. Les méthodes de Runge-Kutta sont des méthodes d'analyse numérique d'approximation de solutions d'équations différentielles [14]. Elles ont été nommées ainsi en l'honneur des mathématiciens Carl Runge et Martin Wilhelm Kutta lesquels élaborèrent la méthode en 1901. Ces méthodes reposent sur le principe de l'itération, c'est-à-dire qu'une première estimation de la solution est utilisée pour calculer une seconde estimation, plus précise et ainsi de suite.

3. Attracteur de Lorenz

Un exemple très connu dans le monde des attracteurs chaotiques est le célèbre attracteur chaotique de Lorenz. Ce météorologue, Edward Lorenz, a développé un modèle dextrement idéalisé pour l'étude de l'atmosphère terrestre en 1963 [15]. Sa théorie fait intervenir trois variables x, y et z, reliées par les équations suivantes :

$$\begin{cases} \frac{dx}{dt} = \sigma * (y - x) \\ \frac{dx}{dt} = r * x - y - x * z \\ \frac{dx}{dt} = r * y - \beta * z \end{cases} \quad (5)$$

Avec σ, r et β sont des paramètres du contrôle.

Ces équations relativement simples ne le sont pas suffisamment pour pouvoir être résolues de manière analytique. (On ne peut pas exprimer explicitement x (t), y (t) et z (t)). On recourt donc à la résolution numérique par l'une des méthodes citées auparavant. Dans ce qui suit on utilise la méthode de Rung-Kutta d'ordre quatre.

Si l'on fait varier les paramètres σ, r et β on constate que; dans certains cas les suites obtenues semblent complètement chaotiques.

Les différentes courbes (espaces des phases) figures 1, 2, 3 et 4 de l'attracteur sont obtenus pour σ = 10, r = 28, β =8/3 et pour des valeurs initial $x_0 = 8$, $y_0 = 3$ et$z_0 = 4$ et avec un pas h : $h = 0.005$.

Le tableau 1 [16] nous donne l'évolution des amplitudes courbes en x, y et z en fonction du temps.

Position	*dx/dt*	*dy/dt*	*dz/dt*
0	8.0000	3.0000	4.0000
1	7.7791	3.9273	4.0827
2	7.6134	4.8232	4.1959
3	7.4988	5.6932	4.3376
4	7.4317	6.5423	4.5069
5	7.4088	7.3751	4.7036
6	7.4274	8.1958	4.9281
7	7.4849	9.0079	5.1814
8	7.5790	9.8146	5.4647
9	7.7078	10.6190	5.7802
10	7.8695	11.4220	6.1299
11	8.0625	12.2260	6.5165
12	8.2854	13.0320	6.9428
13	8.5367	13.8400	7.4122
14	8.8153	14.6510	7.9278
15	9.1199	15.4630	8.4935
16	9.4492	16.2740	9.1128
17	9.8020	17.0840	9.7895
18	10.1770	17.8870	10.5280
19	10.5730	18.6820	11.3300
20	10.9870	19.4610	12.2020
21	11.4190	20.2210	13.1440
22	11.8670	20.9530	14.1610
23	12.3270	21.6510	15.2540
24	12.7980	22.3050	16.4230
25	13.2770	22.9060	17.6700
26	13.7600	23.4440	18.9930
27	14.2440	23.9070	20.3880
28	14.7250	24.2850	21.8520
29	15.1980	24.5660	23.3790
30	15.6600	24.7380	24.9590
31	16.1050	24.7910	26.5830
			. . .

Tableau 1: Evolution des amplitudes des courbes

Les figures 1, 2 et 3 présentent respectivement l'évolution temporelle des signaux x, y et z de l'attracteur chaotique de Lorenz. Par contre, la figure 4 représente l'attracteur de Lorenz en 3D.

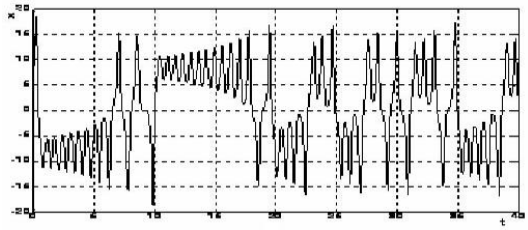


Fig.1 Évolution du signal x de Lorenz attracteur

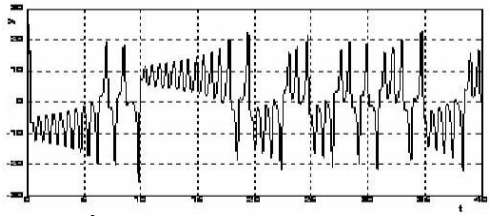


Fig.2 Évolution du signal y de Lorenz attracteur

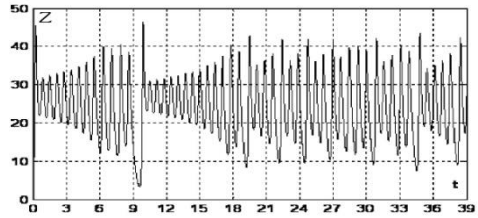


Fig.3 Évolution du signal z de Lorenz attracteur

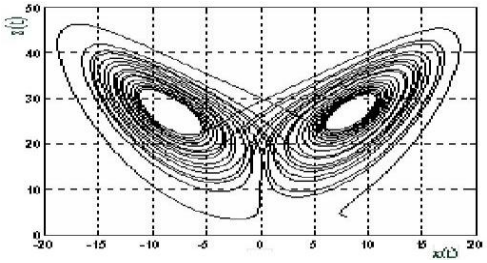


Fig.4 L'attracteur chaotique de Lorenz en 3D

Cet attracteur à la forme de deux ailes déployées d'un papillon. Chaque aile est formée par des séries de cercles concentriques. Les points décrivent plusieurs cercles sur une aile puis bascule sur l'autre sans rythme particulier et sans jamais couper leurs trajectoires [17, 18].

3.1 Sensibilité aux Conditions Initiales

Pour ces différents paramètres le système de Lorenz a un comportement chaotique et devient sensible aux petits changements sur ces conditions initiales.

La sensibilité aux conditions initiales **(S.C.I)** est une caractéristique fondamentale des systèmes dynamiques. Il faut entendre ici qu'un système réagira de façon totalement différente selon la

condition initiale. Ceci a notamment comme conséquence le fait qu'un système chaotique, même si toutes ses états sont imprévisibles car sensible à d'infimes perturbations initiales.

Une valeur différente sur la condition initiale conduit à une tout autre suite qui après une courte phase, dessine la même image. D'où qu'on parte, on se retrouve toujours sur l'attracteur, c'est le côté prévisible de l'évolution [13]. Où se retrouve-t-on exactement sur l'attracteur ? Il est impossible de répondre à la question, c'est le côté imprévisible de l'évolution.

On peut illustrer ça par l'exemple [19] suivant : Considérons deux signaux chaotiques *x(t)* et *x'(t)* de système de Lorenz, le premier généré avec $x_0 = 10$ et l'autre avec $x'_0 = 10+10^{-11}$ comme montre le tableau 2 et la figure Fig.5 :

t (temps)	*x(t)*	*x'(t)*
0	10	10.00000000001
0.01	10.17000000000	10.17000000000
0.08	12.76847439879	12.76847439879
0.12	15.75150052854	15.75150052854
1.50	-8.63801508743	-8.63801508743
5.20	-3.32145260899	-3.32145260899
15.10	-0.55183621194	-0.55184017143
10.15	-7.24735780575	-7.24735781385
12.00	0.28429648200	0.28429648200
13.60	-3.67101193060	-3.67101154419
16.56	8.54532230155	8.54532336503
20.66	4.30890662446	4.30928260576
25.10	-9.60564143809	-9.62529382993
30.60	-8.73087189758	-16.79874348374
32.66	15.726050180100	15.72607392347
32.67	16.182171417781	15.29805570747
33.21	-11.61304067867	-10.23973724797
33.90	-10.78230213042	-6.17899457475
33.92	-11.81303710788	-7.18887959241
34.00	-14.24265733489	-12.56670921212
34.02	-13.96178195843	-14.03818870489
34.50	1.48495699208	7.05194426148
34.90	15.33776756313	4.84564570509
34.99	3.36560974472	3.34918548313
35.01	1.19603065909	3.31410998740
36.02	-11.09587198210	-4.62802134359
37.09	5.38562259151	-1.39601770152
40	5.67023195681	7.93170228937

Tableau 2 : Quelques valeurs de *x(t)* et *x'(t)*

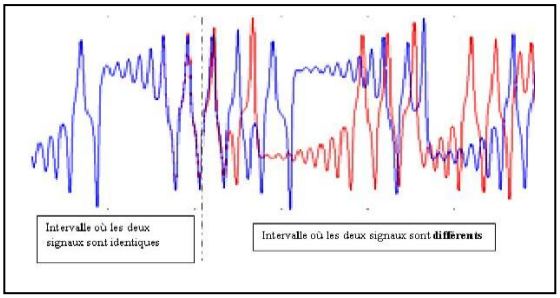


Fig.5 Deux signaux *x(t)* de l'attracteur de Lorenz générés avec deux conditions initiales très voisines.

La figure suivante montre l'état d'espace de phase dans ce cas :

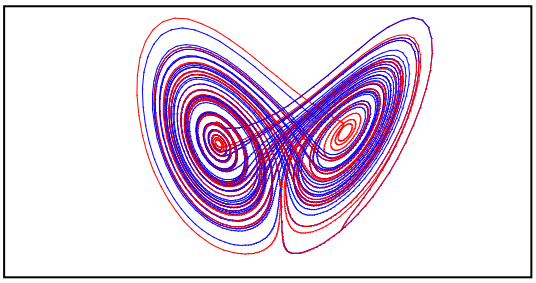


Fig.6 Deux attracteurs chaotiques de Lorenz (en bleu et en rouge) générés par deux valeurs de x_0 très proches.

Nous remarquerons que les deux attracteurs chaotiques de Lorenz différents, mais gardent la même forme.

La divergence des deux signaux ne commence qu'à partir passer un nombre bien défini des échantillons, supérieure à la partie ou les deux courbes coïncides (dans ce cas : 2623 échantillons), après cette période transitoire (à déterminer) nous avons deux signaux différents.

Le nombre 2623 est obtenu [19] en divisant la longueur de l'intervalle de la période transitoire par la valeur du pas. Maintenant, si on veut chiffrer des données d'une taille de 1250 (< 2623) caractères avec le signal chaotique *x(t)*, le déchiffrement de texte chiffré avec une condition initiale très proche de la valeur exacte de l'ordre de 10^{-3} à 10^{-11} donne toujours un texte lisible, du moment que nous opérons toujours dans la partie transitoire, et nous remarquons que la sensibilité du système n'a aucun effet surtout pour des petits écarts sur les paramètres de système.

Pour éviter le maximum possible ce problème, on doit impérativement déterminer l'intervalle stable (transitoire) du système, et le chiffrement commencera qu'à partir de la borne supérieure de cette intervalle. Afin que le système devient sensible aux changements infinitésimaux sur leurs conditions initiales ou les paramètres de contrôle.

3.2 Le crypto-système chaotique de Lorenz

Le principe de fonctionnement d'un crypto-système chaotique [20] est identique à celui du chiffrement continu. Les algorithmes de chiffrement en continu convertissent la donnée à chiffré 1 bit à la fois. La réalisation [21] la plus simple d'un algorithme de chiffrement en continu est illustrée par la figure 7a.

Ce type de générateur engendre un flux de longueur connue de nombres, de zéros et de uns logiques : $K_1, K_2, K_3, \ldots, K_i \ldots$, présentant certaines propriétés du hasard, il est potentiellement difficile de repérer des groupes de nombres qui suivent une certaine règle (comportements de groupe). Les sorties d'un tel générateur ne sont pas entièrement aléatoires; elles s'approchent seulement des propriétés idéales des sources complètement aléatoires. Il est dit aléatoire car cette suite est arbitraire. Cependant, lorsque la suite arrive à son terme, le générateur ne s'arrête pas de fonctionner. La séquence déjà transmise est à nouveau reproduite (générateur **périodique**). D'où le qualificatif de pseudo-aléatoire.

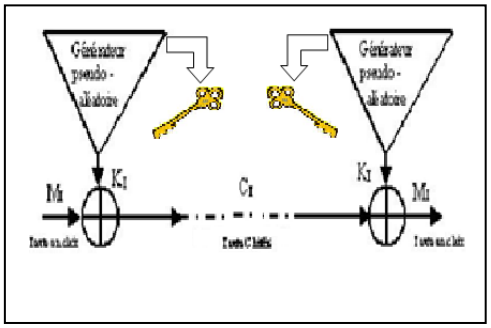


Fig.7a : Chiffrement continu

Ce flux est combiné par ou exclusif avec le flux de bits du texte en clair $m_1, m_2, m_3, \ldots, m_i$ pour produire le flux de bits de donnée chiffrée.

$$C_i = m_i \oplus K_i \qquad (6)$$

Du coté du déchiffrement, les bits de donnée chiffré sont combiné par ou exclusif avec un flux identique de codons pour retrouver les bits du texte en clair

$$m_i = C_i \oplus K_i = (m_i \oplus K_i) \oplus K_i = m_i \qquad (7)$$

Tous algorithmes de chiffrement synchrone en continu utilisent des clefs (secrètes) et, engendrent le même flux de codons au chiffrement et au déchiffrement. Ce flux est engendré indépendamment du flux du message. La sécurité du système dépend entièrement des détails internes du générateur de nombres pseudo aléatoire.

Dans le crypto-système chaotique [20], on choisit une des fonctions temporelles issue de la loi dynamique caractérisant l'attracteur (Lorenz dans notre cas) pour qu'elle nous délivre un flux chaotique (aléatoire) de codon (figure 7b), qui va être additionné aux données à sécuriser. On peut noter, sachant la définition du chaos, que ce flux chaotique de codons a les caractéristiques suivantes :

1. Longue période,
2. Pas de répétitions,
3. Complexité linéaire locale,
4. Critères de non linéarité pour des fonctions booléennes.

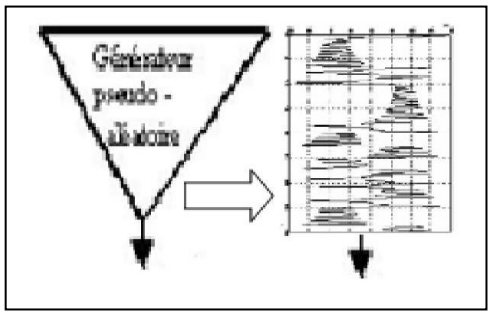


Fig.7b : Générateur Chaotique

Le choix de la clé de chiffrement [20], dans ce cas par exemple, doit être suivant ces champs :

1. le choix d'attracteur,
2. choix des paramètres de contrôles
3. le travail suivant l'axes X/Y/Z ,
4. le pas d'échantillonnage, et
5. l'état initiale X_0 , Y_0 et Z_0 .(graine)

Le fruit de ce travail, est qu'on doit rajouter un autre champ au dimensionnement de la clé qui est la détermination de l'intervalle stable (transitoire) de l'attracteur.

On va maintenant utiliser le générateur chaotique réalisé pour chiffrer un message, en utilisant le signal *x(t)* de l'attracteur de Lorenz comme signal chiffrant comme le montre la fig. 7c. Les paramètres de système sont fixés comme suite:

$$x_0 = y_0 = z_0 = 10, \sigma = 10$$

$$r = 28, \beta = 8/3 \text{ et } h = 0.01.$$

Il est à noter que ces paramètres seront utilisés dans toute la suite de travails avec ce crypto-système.

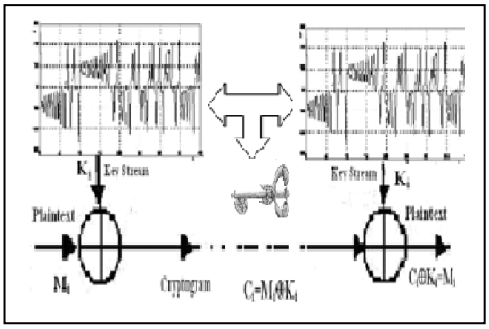


Fig.7c : Crypto Système Chaotique

3.2.1. Chiffrement d'image avec ce système

L'image chiffrée d'Edward Lorenz est une image monochrome noire et blanc d'une résolution de 300x457 pixels. Les résultats [19] de chiffrement et déchiffrement obtenus sont :

Fig. 8a : L'image originale

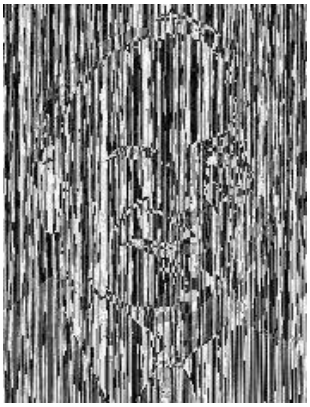
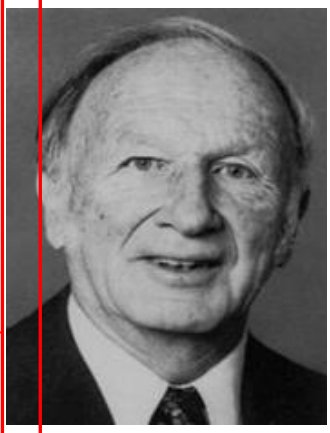


Fig. 8b : Image chiffrée.

Fig. 8c : Image déchiffrée avec les mêmes paramètres utilisés pour le chiffrement.



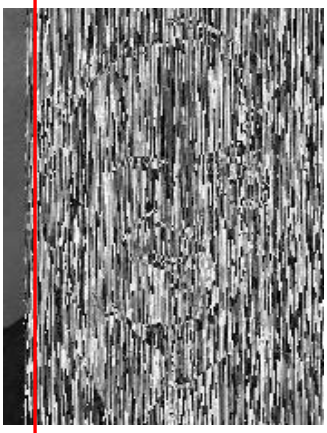


Fig. 8d : Image déchiffrée en changeant r à 10.00000000001

La partie encadrée en rouge de l'image de la figure 8c est identique à celle de l'image originale de la figure 8d mais en général l'image reste illisible. Il est à noter que tous changements infinitésimaux sur chaque condition initiale ou chaque paramètre de contrôle nous ont donné les mêmes résultats.

3.2.2. Chiffrement d'un texte avec ce système :

Le texte chiffré contient 398 caractères [19], chaque caractère est codé sur 8 bits (tableau 3).

Texte Original	De nos jours, la cryptographie est entrée dans la vie courante. Nous nous en servons tous les jours sans même nous en rendre compte. Chaque fois que nous passons un appel téléphonique, que nous envoyons un email, nous cryptons les données que nous manipulons. La plupart du temps ce cryptage se fait automatiquement et il est tellement rapide que nous ne nous en rendons même pas compte.
Texte Chiffré	Cb'iiu&listu*&jg&et□vsh`ufx`am)lz}*od~ yân+ojb□gj+}bo*if|{ifsb)&Hjpv%kjqw$a j$w`wsjkv%risu'kb{(bf|{y*xje□aç`h-cbx~,ie+xoglzb'ejhupa-#@jcswg"dmkq"swg"lmvp#sbpwkjw%pk & gwwmd)}ãgâ|eb`f~eu<0azj.cc~y)mipj}llr! ßÑÝ• Ü• Ø• ÕÓ• ÓÖÙµÛ• Þóô Þßß ÕÓ• ÑÏ×ôðe!pwg#mlqw$j`%kjsu&ch'ubilgfz)d ãgo*{jx+oca|xi"+
Texte déchiffré avec les mêmes paramètres initiaux	De nos jours, la cryptographie est entrée dans la vie courante. Nous nous en servons tous les jours sans même nous en rendre compte. Chaque fois que nous passons un appel téléphonique, que nous envoyons un email, nous cryptons les données que nous manipulons. La plupart du temps ce cryptage se fait automatiquement et il est tellement rapide que nous ne nous en rendons même pas compte
Texte Déchiffré avec en changeant x_0 à 10.00000000001	Ed!oosjouqs, l` crv□togs`qihdesteousèd dan| la vie `our`ote. Ious!oousensj}vnorwlvp#odr!kntsp#pbmp# lëld/a`ur!em#rdndrecnlqud/&Ei`rvd iois#qud!ihrt'vguuihu&sh&gwwbk'qìiítlcbe |yj#-|~n%kkrw%`luozlmh:mf(mehfb&+jkru"`ryqu• • Þý• ÜÛØÙÖº• ÑÖüøÞ×Ì• Ú• • m`vksp`iais'ap%li$aww#vgnmemjnu"vdvocb 8im}'ff□x-`j!llqv&bÙ• Ü• Ý• • ÞÑß
Texte déchiffré en changeant z_0 à 10.00000000001	ºÞÙÝÑ• ÑÝÝÞÐßßÑßõò• • ÝÑÑÚ• ÙÙ Þ• • ÝÐ• Þ• ß• Ñßòõ¼ÐÙÚ• Ü• cqqml q"wm#bssfo#vënëriihowrb*%tqf,bby|-he|j~ikh;kn {q|sw49yf~z/kzpvqßdp#doonébt'qtd!novp m`ni□zmnlq-"Nd%vjsvgtr&dv udb~}"`f$fw}wseca$v`$bemp$eqpkhdqmu qbjbhr&`~*cg*ozz.zkbaiafmv!tewocm7fcs *de|{)dn%hhts#gÜØÞ• • ÜÑÞ
Texte déchiffré en changeant σ à 28.00000000001	Fg!nnu'nkphj48tx8{upz□bi|`sjla'bu• Ù• • Û• ÓÒÐ• ÒÝ÷ð·• ß• ÝÑßßÙÙÛ• ÔÒ• Õ• ÖØôò¼• • ÚÖÒÙ• • • • ÜÝ• • n"w êoêskkjmup`)&wrb(ff|y+nczcva`b1d`.jbo` d'+jjs s'ev}vs×ÐÏ• ÊÐegfz'/Bh)zf□zjy□+ix.{jmq r"`f$gv|uqgac&uc'afns'frshjfsowsldlg})o~* cf+nxx,yhabjbenu"vdy`lm7fbr(ff□x-`j!llqv&bÙ• ÓÒÑÑß

Tableau 3 : Résultats de chiffrement/déchiffrement

Nous remarquons que la moindre du changement sur les conditions initiales ou bien sur les paramètres de contrôle, rendre le texte déchiffré illisible totalement.

4. Conclusion

Les générateurs chaotiques peuvent être qualifiés de cryptographiques, du moment qu'ils font preuve de certaines propriétés nécessaires pour qu'ils puissent être utilisés en cryptologie. Ils sont capables de produire une sortie suffisamment peu discernable d'un aléa parfait et ils résistent à des attaques comme par exemple l'injection de données forgées de manière à produire des imperfections dans l'algorithme, ou encore des analyses statistiques qui permettraient de prédire la suite. C'est pour qu'il faut bien configurer l'intervalle temporelle du régime transitoire de l'attracteur qui est choisit dans le crypto-système et convenablement choisir le germe adéquat.

Le crypto-système chaotique de Lorenz nous a donné des très bons résultats, soit pour le chiffrement des textes, soit pour les images. Il offre aussi une très haute sensibilité aux changements infinitésimaux sur les conditions initiales (CI) et sur les paramètres de contrôle. Un écart de l'ordre 10^{-11} sur l'un des CI ou les paramètres de contrôle provoque des changements massifs sur le message déchiffré.

On peut dire que les systèmes chaotiques peuvent devenir l'alternative à l'avenir des communications sécurisées, mais ils restent plusieurs obstacles qui entravent l'utilisation de chaos dans le domaine de la cryptographie actuellement en temps réel, on peut citer quelques-unes comme :

- Le chaos perd sa diversité en vue de nombre bien déterminé des états possibles. L'utilisation de la précision finie pour créer une séquence récursive définie dans un domaine réel provoque la perte d'une propriété importante, liée au chaos analogique, la longueur de cycle des orbites chaotique qui tend vers l'infini.
- La synchronisation : dans un crypto-système chaotique le récepteur doit être synchronisé avec l'émetteur, la moindre du changement sur les conditions initiales ou si un décalage d'un seul bit va provoquer une déformation totale de message envoyé et rendre le message à déchiffré totalement illisible.

5. Bibliographies :

[1].Nada Rebhi, Mohamed Amine ben Farah, Abdennaceur Kachouri & Mounir Samet, " Analyse de sécurité d'une nouvelle méthode de cryptage Chaotique ", Laboratoire d'Electronique et des Technologies de l'Information (LETI), Ecole Nationale d'Ingénieurs de Sfax, Tunisie, 25-29 mars 2007.

[2] "Sécurisation de l'information : le cryptage par le chaos ", téléchargée le 15/06/09 de :http://www.tout-pour-la-science.com/2284/S%E9curisation+de+l'information+:+le+cryptage+par+le+chaos.html, 9 mars 2005.

[3] Aymane BENSLIMANE Pauline HUET, "Théorie du chaos : Application à la sécurité", ENSICAEN 2008.

[4] Mihai Bogdan Luca, "Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information", l'Université de Bretagne Occidentale, novembre 2006.

[5] Robert C.Hilborn, "Chaos and nonlinear Dynamics, second edition", page 03, Oxford university press, 2000.

[6] ODEN Jérémy, "Le chaos dans les systèmes dynamiques", juillet 2007, chapitre2 , téléchargée le 15/05/09 de : www.spectrosciences.com

[7] "Les systèmes dynamiques", téléchargée le 08/08/09 de : http://fr.wikipedia.org/wiki/Syst%C3%A8me_dynamique

[8] G.L . Baker et J.P Gollub, "Chaotic dynamics", seconde edition page 76

[9] "Dynamique chaotique", téléchargée le 02/01/10 : www.dunod.com/documents/48387/Front_annexe_B.pdf

[10] V.Guglielmi, P-Y.Besnard, D.Fournier-Prunaret, P.Pinel, AK.Taha, L.Beneteau, "Un système numérique de cryptographie basé sur les propriétés des signaux chaotiques discrets", Laboratoire d'études spatiales et d'instrumentation en astrophysique, Toulouse, France.

[11] FaberSperber, Robert Paris, "Qu'est-ce qu'un attracteur étrange ? ", Téléchargée le 15/05/09 de: http://www.matierevolution.fr/spip.php?article706, octobre 2008

[12] Pascale BOURGES, "Attracteurs étranges", téléchargée le 05/05/09 de :http://pagesperso-orange.fr/pascale.et.vincent.bourges/fractales%20et%20chaos1/Chapitre%206.htm

[13] André Lévesque, "Les attracteurs étrange", téléchargée le 06/02/10 de site personnel de l'auteur : http://math.cmaisonneuve.qc.ca/alevesque/Default.htm

[14] François Laudenbach, “ Calcul différentiel et intégral ”, page 07, Edition de l’Ecile polytechnique, Mars 2005.

[15] Laurence Bouquiaux, “L'harmonie et le chaos: le rationalisme leibnizien et la nouvelle science”, page 26 , Editions PEETERS

[16] R. Chalabi, H. Hakim: “Study and implementation of a chaotic attractor with a view of their implementations to cryptography” PFE - USTO July 2006.

[17] “La théorie de chaos ”, téléchargée le 10/11/2009 de : http://just.loic.free.fr/index.php?page=intro

[18] Gleick J, “La Théorie du chaos”, Ed. Flammarion, 1991.

[19] L. MERAH, ‘Étude Implémentation sous XLINX SYSTEM GENERATOR des Crypto Systèmes Chaotiques pour Sécuriser les Systèmes de Communications Modernes’, Magister en Électronique, USTO Oran, Juin 2010.

[20] Adda Ali-Pacha, , Naima Hadj-Said, A. M’Hamed and A.Belgoraf “Lorenz’s attractor applied to the stream cipher (Ali-Pacha generator) ”, National Institute of Telecommunications, Evry, Paris, France, March 2006.

[21] B. Schneier," Applied Cryptography-Protocols, Algorithms and Source Code in C", John Wiley & Sounds, Inc, New York, Second Edition, 1996.