Systèmes dynamiques hybrides pour les communications privées

Hamid HAMICHE[1,3], Malek GHANES[1], Jean-Pierre BARBOT[1,2], Saïd DJENNOUNE[3]

[1] ECS, ENSEA,
6 avenue du Ponceau, 95014 Cergy-Pontoise Cedex, France

[2] EPI-ALIEN, INRIA.

[3] Laboratoire de Conception et Conduite des Systèmes de Production, UMMTO, BP 17 RP, 15000, Tizi-Ouzou, Algérie.

{hamid.hamiche, ghanes, barbot}@ensea.fr, djennoune@mail.ummto.dz

Résumé— **Dans ce travail, un schéma de transmission à base de dynamique hybride et chaotique pour les communications privées est proposé. L'émetteur est constitué d'un système en temps continu et d'un système en temps discret dans lequel le message est inséré à l'aide de la méthode dite par inclusion. Les états du système continu sont eux aussi après échantillonnage inclus dans le système discret. Le récepteur est constitué d'un observateur en temps discret retardé et d'un observateur en temps continu. Le principe de la méthode hybride proposée est de montrer que la reconstitution des états du récepteur discret ainsi que le message passe d'abord par la synchronisation des deux systèmes chaotiques en temps continu. Cette nouvelle stratégie robustifie le système de transmission, notamment à une attaque à texte clair connu. Les résultats de simulation sont présentés afin d'étudier les performances de la méthode proposée.**

I. Introduction

Depuis quelques années, la théorie des systèmes non linéaires complexes et surtout chaotiques a été appliquée à la cryptographie, afin de proposer d'autres méthodes de chiffrement. En 1990, T. Pecorra et L. Caroll [16] ont montré la possibilité de synchroniser des systèmes chaotiques. Alors, de nombreux schémas de chiffrement basés sur le chaos ont été proposés dans la littérature. En revanche, très peu de travaux ont réellement fait le lien entre les algorithmes de chiffrement standard et ceux basés sur la génération de séquences chaotiques. En cryptographie usuelle, parmi une grande variété de mécanismes de chiffrement, on distingue le chiffrement symétrique et le chiffrement à clé publique. Un lien entre le chiffrement symétrique standard et le chiffrement par inclusion basé sur le chaos a été proposé par F. Anstett [1]. D'autres méthodes de chiffrement utilisant les systèmes chaotiques ont été proposées dans la littérature, parmi lesquelles, on peut citer la méthode par addition [18], la modulation paramétrique [15], la modulation chaotique [4], etc. Ces méthodes sont toutes basées sur la synchronisation du récepteur avec l'émetteur, afin de pouvoir extraire le message initialement noyé dans la porteuse chaotique. En 1997, H. Nijmeijer et I. Mareels [13], [14] ont montré que la synchronisation unidirectionnelle des systèmes chaotiques peut être considérée comme un problème de synthèse d'observateur. Différents types d'observateurs sont alors proposés pour les systèmes chaotiques (observateurs destinés uniquement à reconstruire les états de l'émetteur) [7] et aussi pour les systèmes chaotiques à entrées inconnues (observateurs destinés à reconstruire les états de l'émetteur et récupérer l'information) [2], [10]. Le fonctionnement correct de ces observateurs dépend de plusieurs conditions : la condition d'observabilité pour retrouver les états du système ; la condition de recouvrement de l'observabilité ("observability matching condition") pour retrouver les états du système et l'information noyée dans le système (inversibilité à gauche du système) ; la condition d'identifiabilité des paramètres qui représentent les clés de codage. Dans notre travail, nous nous sommes intéressés à l'étude d'un schéma de transmission constitué de systèmes dynamiques hybrides. L'émetteur est composé d'un système chaotique continu dit de Colpitts et d'un système chaotique discret dit de Hénon modifié. Le récepteur est composé d'un observateur continu et d'un observateur discret. Au niveau de l'émetteur, des états du système continu seront introduits dans la dynamique du système discret dans le but de rendre sa structure plus complexe. Le nouveau système hybride ainsi obtenu rend le système difficilement observable. En plus, cette stratégie augmente la complexité d'identification des paramètres qui constituent les clefs de codage même dans les attaques à textes clairs connus. La sortie transmise au récepteur est composée d'un signal de synchronisation issu du système continu et d'un signal utile qui contient le message (ajouté par la méthode d'inclusion) issu du système discret. Pour avoir une bonne transmission, il est nécessaire d'avoir un rapport signal utile sur signal de transmission le plus proche de un possible. La reconstitution des états ainsi que le message de l'observateur discret passe par la synchronisation des deux systèmes chaotiques continus (émetteur et récepteur) avant la synchronisation des systèmes en temps discret[1]. Cette méthode présente néanmoins l'avan-

[1]Dans cette étude, nous avons supprimé les retards qui sont une partie des clés de codage entre le système continu et le système discret. Ces retards se traduisent par une infinité de choix sur la période d'échantillonnage discrète. C'est en ce sens que nous utilisons le terme

tage que les deux systèmes peuvent se resynchroniser en cas de perte de synchronisation. Notre travail est structuré comme suit : Dans la section 2, nous présentons le principe de notre méthode en étudiant séparément l'émetteur et le récepteur du système de transmission. La section 3 est consacrée à la présentation des résultats de simulation. Enfin, nous terminons, comme il est de tradition, par une conclusion.

II. Présentation de la méthode

Dans ce travail, nous avons réalisé un système de communication basé sur la synchronisation de systèmes chaotiques hybrides à l'aide d'observateurs. Le schéma global de notre système pour les communications privées est montré par la figure 1.

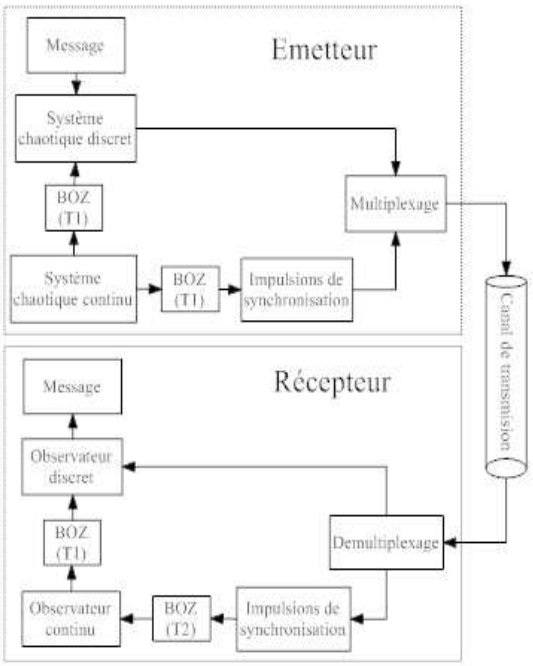

Fig. 1. Chaîne de transmission basée sur un système dynamique hybride

Le développement de la méthode se fait comme suit :

A. Etude de l'émetteur

L'émetteur est constitué de trois blocs : un système chaotique continu, un système chaotique discret et un bloc de synchronisation d'impulsions. Ces blocs sont détaillés de la manière suivante :

hybride car une simple discrétisation du système continu nous impliquerait autant de système discret à simuler que de retards différents

A.1 Etude du système chaotique continu

Ce système a été largement étudié dans la littérature ([11], [12]). Les équations normalisées du Colpitts en temps continu sont données comme suit :

$$\begin{cases} \dot{z_1} = a_1(-exp(-z_2) + 1 + z_3) \\ \dot{z_2} = a_2 z_3 \\ \dot{z_3} = -a_3(z_1 + z_2) - a_4 z_3 \end{cases} \quad (1)$$

avec $a_1 = \frac{g}{q(1-k)}$, $a_2 = \frac{g}{qk}$, $a_3 = \frac{qk(1-k)}{g}$, $a_4 = \frac{1}{q}$.

Pour avoir un comportement chaotique, les paramètres du système (1) sont donnés comme suit : $g = 4.46$; $Q = 1.38$ et $k = 0.5$ avec $z_1(0) = 1.6$; $z_2(0) = 8$ et $z_3(0) = 0.1$, les conditions initiales du système.
Tout d'abord, nous étudions l'observabilité du système avec $y_1 = z_1$ sa sortie. En utilisant les travaux de [10], il est aisé de montrer que le rang de la matrice d'observabilité du système (1) est égal à 3, donc le système est localement faiblement observable. Par conséquent, il est possible de retrouver tous les états à partir de la sortie $y_1 = z_1$ et de ses derivées.

A.2 Etude du système chaotique discret

Le système chaotique en temps discret utilisé dans notre travail est dit système de Hénon modifié. Ce système a été largement étudié dans la littérature, on peut citer par exemple les travaux de Dmitriev [6] et Vesely [17]. Il est donné par les équations suivantes :

$$\begin{cases} x_1(k+1) = a - x_2^2(k) - bx_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) \end{cases} \quad (2)$$

Pour avoir un comportement chaotique, les paramètres du système (2) sont donnés comme suit : $a = 1.76$ et $b = 0.1$ avec $x_1(0) = 0.1$ $x_2(0) = 0.1$ et $x_3(0) = 0.1$, les conditions initiales du système. Au niveau de l'émission, notre objectif est de rendre la structure du système en temps discret discret plus complexe. Pour cela, nous allons introduire dans la dynamique du système en temps discret, les états z_1, z_2 et z_3 du système en temps continu. Il est à noter que les états du système en temps continu seront d'abord échantillonnés avec une période $T1$ avant d'être introduits dans le système en temps discret. Cette période $T1$ (dont la valeur est donnée en simulation) est choisie pour assurer la synchronisation entre l'émetteur et le récepteur des deux systèmes en temps continu (cet argument est détaillé en section (II-B.1)). Malgré le fait que le système de Hénon modifié soit un système en temps discret pur, sans aucun lien avec le temps, ici, chaque itération sera faite après une période de temps fixe $T1$. Ce choix de fréquence fixe a été fait pour simplifier la mise en oeuvre du récepteur.
Dans cette partie, nous allons utiliser le système donné par (2) comme émetteur avec $y_2(k) = x_2(k)$, la sortie du système.
Dans notre travail, nous avons ajouté les deux états (z_2, z_3) et le message m sur la troisième dynamique du système (2). Le détail de la reconstruction des états et du message m est donné dans la section (II-B.2). Le nouveau système hybride

obtenu est donné comme suit :

$$\begin{cases} x_1(k+1) &= a - x_2^2(k) - bx_3(k) \\ x_2(k+1) &= x_1(k) \\ x_3(k+1) &= x_2(k) + Az_2(n) \\ &+ Bz_3(n) + Cm(k) \end{cases} \quad (3)$$

Avec : A, B et C des nouveaux coefficients du système en temps discret et m le message à envoyer. Pour conserver le comportement chaotique du système défini par (3), ces paramètres doivent être choisis avec précaution. Dans notre cas, il faut respecter les valeurs suivantes : $A \leq 0.04$, $B \leq 0.1$ et $C \leq 1$. En utilisant les travaux ([3],[5]), il est facile de montrer que le rang de la matrice d'observabilité du système (3) est égale à 3, donc le système est localement observable. De plus, la condition de recouvrement d'observabilité a été vérifiée, ici, le message n'intervient qu'après 3 itérations. En conséquence, il est alors possible de reconstruire tous les états et le message à partir de la sortie et de ses sorties retardées. Dans notre travail, nous avons rendu la structure de l'émetteur discret complexe . Ceci augmente la complexité de l'identification des paramètres par rapport à un système ou seule une dynamique discrète aurait été utilisée.

A.3 Etude du bloc de multiplexage

Le signal de sortie $y_1 = z_1$ issu du système en temps continu sera d'abord échantillonné avec un pas d'échantillonnage $T2$ mais bloqué uniquement durant $T1$. Le signal $y_1 = z_1$ joue le rôle du signal de synchronisation, il est envoyé dans le canal pendant une durée $T1$. Quant au signal y_2, il sera envoyé pendant 9 durées $T1$. Le système en temps discret n'est pas itéré pendant le dixième cycle (T1)qui correspond à l'envoi du signal de synchronisation. Le cycle se compose donc de 10 durées $T1$, comme l'illustre le chronogramme ci-dessous.

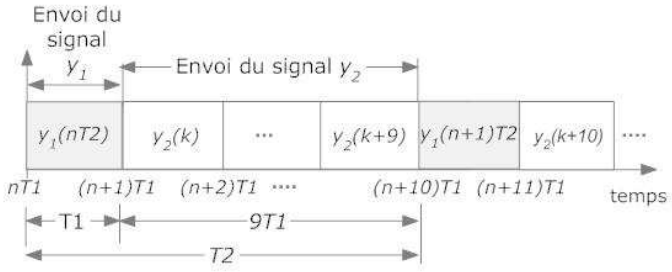

Fig. 2. Cycles de transmission des signaux y_1 et y_2

B. Etude du récepteur

Le récepteur est constitué de trois blocs : un observateur chaotique en temps continu, un observateur chaotique en temps discret et un bloc de synchronisation d'impulsions. Dans ce qui suit, nous allons nous intéresser à l'étude de la synchronisation entre les émetteurs et les récepteurs du schéma de transmission proposé. Nous allons présenter les deux observateurs respectivement continu et discret permettant de synchroniser les systèmes (1) et (3) respectivement avec leurs récepteurs.

B.1 Etude de l'observateur chaotique à temps continu

Soit le système (1), avec la sortie $y_1 = z_1$. Le but est de concevoir un observateur adaptatif (voir [8]) qui permet à partir, de la sortie $y_1 = z_1$, de reconstruire tous les états du système (1) (notés $\hat{z}_1, \hat{z}_2, \hat{z}_3$). Le système (1) peut être representé par :

$$\begin{cases} \dot{Z} &= AZ + g(Z) \\ Y &= CZ \end{cases} \quad (4)$$

où

$$A = \begin{pmatrix} 0 & 0 & a_1 \\ 0 & 0 & a_2 \\ -a_3 & -a_3 & -a_4 \end{pmatrix} \quad (5)$$

$g(Z) = \begin{pmatrix} a_1(1 - exp(-z_2)) & 0 & 0 \end{pmatrix}^T$,
$C = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$ et $Z = \begin{pmatrix} z_1 & z_2 & z_3 \end{pmatrix}^T$.
En appliquant la condition de rang [9], nous remarquons que le rang de la matrice d'observabilité définie par :

$$O = \begin{pmatrix} dh \\ dL_f h \\ dL_f^2 h \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & a_1 \\ -a_1 a_3 & -a_1 a_3 & -a_1 a_4 \end{pmatrix}$$

est égale à 3, donc le système (4) est observable. dans le but de concevoir un observateur pour le système (1), nous introduisons les hypothèses suivantes :

Hypothèse. II.1:

1. Due au caractère chaotique, le vecteur d'état du système (4) est dans un domaine ouvert borné $D \subset \mathbb{R}^3$.

2. $g(Z)$ est globallement Lipschitzienne avec z_2 appartenenant au domaine D.

Nous introduisons maintenant un observateur pour le système (1). les équations de l'observateur sont données par :

$$\begin{cases} \dot{\hat{Z}} = A\hat{Z} + g(\hat{Z}) + P^{-1}C^T(Y - \hat{Y}) \\ \dot{P} = -\theta P - A^T P - PA + 2C^T C \\ \hat{Y} = C\hat{Z} \end{cases} \quad (6)$$

où $\hat{Z} = \begin{pmatrix} \hat{z}_1 & \hat{z}_2 & \hat{z}_3 \end{pmatrix}^T$. Il est à noter que $P^{-1}C^T$ est le gain de l'observateur (6).

Convergence de l'observateur : Posons l'erreur d'estimation suivante :

$$E = Z - \hat{Z}$$

sa dynamique est donnée par :

$$\dot{E} = [AE - P^{-1}C^T C(Z - \hat{Z})] + g(Z) - g(\hat{Z}) \quad (7)$$

Dans le but de garantir la convergence de l'observateur proposé, une condition suffisante est établie par le résultat suivant :

La valeur de θ est choisie telle que l'inégalité suivante est satisfaite.

$$\theta > \frac{2LK}{\lambda_{min}(P)} \quad (8)$$

où K, L et $\lambda_{min}(P)$ des paramètres positifs constants définis ci-dessous.

Théorème. II.1: Considerons le système (6) et que l'hypothèse (II.1) est vérifiée. Si θ satisfait linégalité (8) alors l'observateur donné par (6) est un observateur exponentiel pour le système (4).

Preuve. Considerons la fonction de Lyapunov suivante :

$$V = E^T PE$$

En calculant la dérivée de V par rapport au temps, nous obtenons :

$$\dot{V} = -\theta E^T PE + 2(g(Z) - g(\hat{Z}))PE$$

En introduisant les normes :

$$\dot{V} \leq -\theta E^T PE + 2(g(Z) - g(\hat{Z}))\|P\|\|E\| \quad (9)$$

En utilisant la condition de Lipschitz avec l'hypothèse $1-2$, c'est à dire,

$$\|(g(Z) - g(\hat{Z})\| \leq L(\|Z - \hat{Z}\|)$$

nous obtenons :

$$\dot{V} \leq -\theta E^T PE + 2LK\|E\|^2 \quad (10)$$

où $\|P\| \leq K$ et L la constante de Lipschitz. Nous avons :

$$\lambda_{min}(P)\|E\|^2 \leq \|E\|_P^2 \leq \lambda_{max}(P)\|E\|^2$$

où $\|E\|_P^2 = E^T PE$
(10) devienne :

$$\dot{V} \leq -(\theta - \frac{2LK}{\lambda_{min}(P)})\|E\|_P^2$$

Donc, en choisissant θ satisfaisant la condition (8), ceci conduit à la convergence exponentielle des erreurs d'estimation lorsque t tend vers ∞. □

B.2 Etude de l'observateur chaotique discret

Dans cette partie, nous considérons le système donné par (3) avec $y_2(k) = x_2(k)$ sa sortie correspondante. Pour la reception, en utilisant les travaux de ([3], [5]), nous allons concevoir un observateur en temps discret retardé, fonctionnant à la période $T1$, de la façon suivante :
- Reconstruction de l'état $\hat{x}_1$:
A partir du système (3), on a :

$$\hat{x}_2(k+1) = \hat{x}_1(k)$$

En appliquant un retard sur la sortie, on déduit l'état $\hat{x}_1$ comme suit :

$$\hat{x}_1(k-1) = y_2(k) \quad (11)$$

- Reconstruction de l'état $\hat{x}_3$:
Du système (3), on a également :

$$\hat{x}_3(k) = \frac{a - \hat{x}_1(k+1) - \hat{x}_2^2(k)}{b}$$

Appliquant cette fois deux retards sur la sortie et en utilisant l'équation (11), on obtient l'état $\hat{x}_3$:

$$\hat{x}_3(k-2) = \frac{a - y_2(k) - y_2^2(k-2)}{b} \quad (12)$$

- Reconstruction du message $\hat{m}$:

Du système (3), on a :

$$\hat{m}(k) = \frac{\hat{x}_3(k+1) - \hat{x}_2(k) - A\hat{z}_2(n) - B\hat{z}_3(n))}{C}$$

En appliquant cette fois-ci trois retards sur la sortie et en utilisant l'équation (12), on aura :

$$\begin{aligned} \hat{m}(k-3) &= \frac{a - y_2(k) - y_2^2(k-2)}{bC} \quad (13) \\ &- \frac{y_2(k-3) + A\hat{z}_2(n-3) + B\hat{z}_3(n-3)}{C} \end{aligned}$$

L'équation (13) permet de reconstituer le message mais ceci uniquement après synchronisation des deux sytèmes continus ((1) et (6)).

B.3 Etude du bloc de démultiplexage

A la réception, le signal reçu sera d'abord démultiplexé en deux signaux y_1 et y_2. Le signal y_1 qui n'est accessible que durant la période $T1$ est maintenant mémorisé sur une période $T2 = 10T1$ (voir figure 2). Ensuite, il est introduit dans l'observateur continu. L'autre signal y_2 est accessible pendant 9 cycles et change tous les cycles. Il est introduit dans l'observateur discret (voir figure 2).

III. RESULTATS DE SIMULATION

Dans cette section, les performances de la méthode proposée seront étudiées en utilisant le logiciel Matlab/Simulink.

Nous allons d'abord présenter les résultats de simulation sur les synchronisations des deux sysèmes continus. La valeur de θ est égal à 5. elle est choisie pour assurer la stabilité de l'observateur (convergence des différentes erreurs de synchronisation données dans la section II-B.1). Les conditions initiales choisies de l'observateur (6) sont : $\hat{z}_1(0) = 1.8$, $\hat{z}_2(0) = 3$ et $\hat{z}_3(0) = 0$. Celles du système émetteur sont données dans la section II-A.1.

A. Résultats de synchronisation des deux systèmes continus

Les figures (3 et (4) présentent respectivement les états et leurs écarts de synchronisation. À partir de $t = 2s$, nous pouvons remarquer que les pourcentages d'erreurs sur e_1, e_2 et e_3 (Figure (4)) sont de l'ordre de 0.5%, 0.2% et 0.1%. Ce constat nous permet d'affirmer que les erreurs sont négligeables et tous les états sont bien estimés par l'observateur en temps continu.

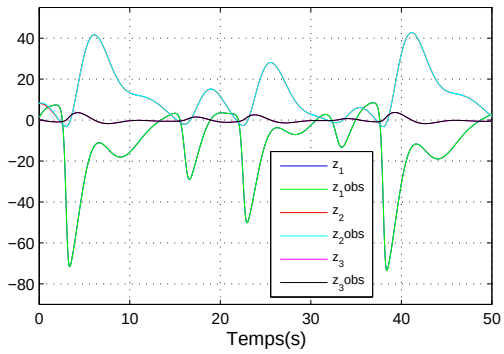

Fig. 3. $(z_1, \hat{z}_1)$, $(z_2, \hat{z}_2)$ et $(z_3, \hat{z}_3)$

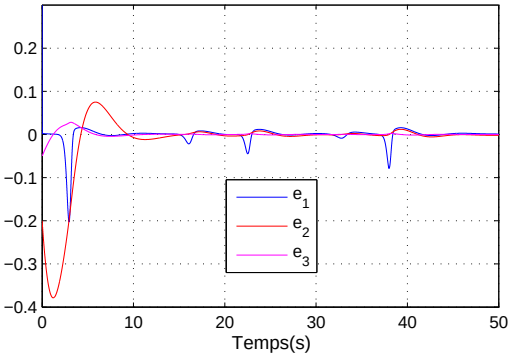

Fig. 4. Erreur de synchronisation sur les états z_1, z_2 et z_3

B. *Résultats de synchronisation des deux systèmes hybrides*

Dans ce qui suit, nous allons présenter les résultats de simulation sur la synchronisation des deux systèmes hybrides, c-à-d le système (3) et l'observateur détaillé dans la section (II-B.2). Les nouveaux paramètres A, B, C de cet observateur sont : $A = 0.04$, $B = 0.1$ et $C = 1$ et le message à envoyer est un signal carré d'amplitude égale à C (le choix de ces amplitudes est justifié juste après l'observateur (3)). Dans notre cas, tous les systèmes en temps continu (1) et (6) et en temps discret (3) et (II-B.2) fonctionnent toujours à la période $T1 = 0.001s$. Quand à la sortie (y_1 et y_2) du système émetteur, elle est transmise dans le canal de transmission à chaque période $T2 = 10T1$.

Les figures (5, 7) et (6, 8) présentent respectivement les états et les écarts de synchronisation du système hybride avec son observateur correspondant. Notons que les états x_1 et x_3 ne dépendent pas des états z_1, z_2 et z_3 du système continu. Ceci permet de bien constater que l'écart sur $e_1 = x_1 - \hat{x}_1$ s'annule après une période $T1 = 0.001s$ qui correspond à un retard d'un pas sur la sortie (en accord avec l'équation (11)) et l'écart sur e_3 s'annule après une période $T = 2T1 = 0.002s$ qui correspond à un retard de deux pas sur la sortie (en accord avec l'équation (12)). Par contre, la reconstitution du message m (voir équation (13)) dépend de la synchronisation des états z_1, z_2 et z_3 de l'émetteur en temps continu (1) et du récepteur en temps continu (6). On peut remarquer sur les figures précédentes ((3) et (4)) que le temps de synchronisation de ces deux systèmes ((1) et (6)) se produit à $t = 2s$. Ce n'est qu'à partir de cet instant que le message est reconstitué (voir figures 9 et 10).

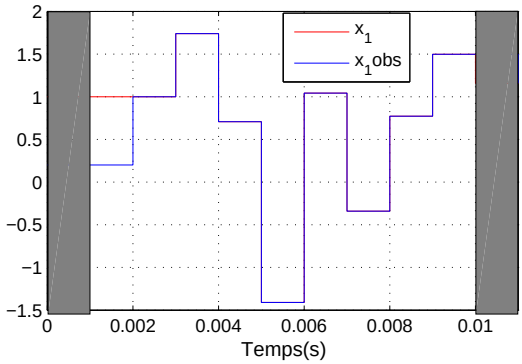

Fig. 5. x_1 et $\hat{x}_1$

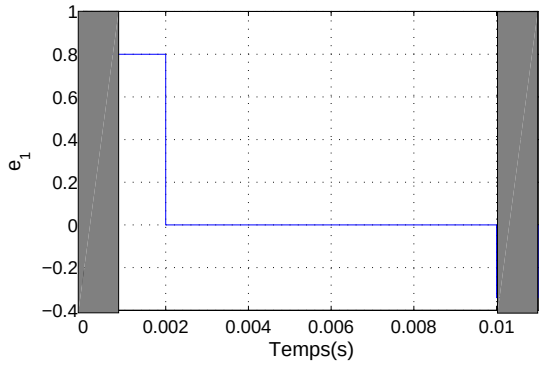

Fig. 6. Erreur de synchronisation sur l'état x_1

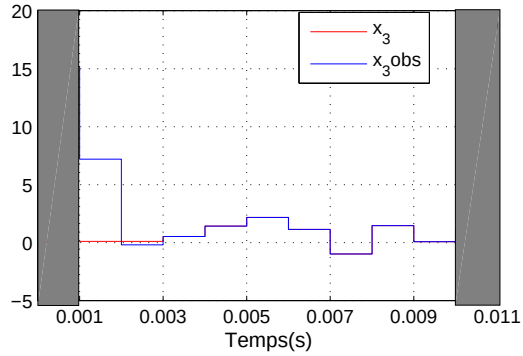

Fig. 7. x_3 et $\hat{x}_3$

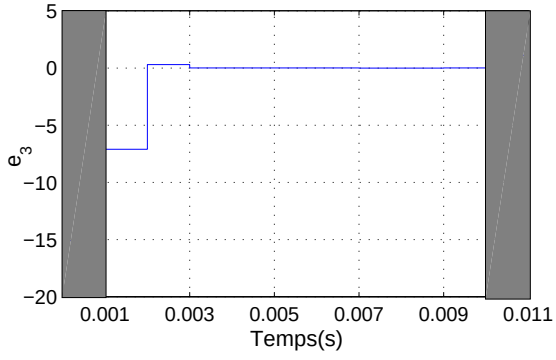

Fig. 8. Erreur de synchronisation sur l'état x_3

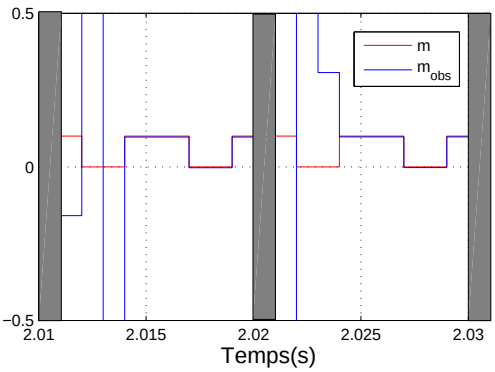

Fig. 9. Zoom sur les messages : m et $\hat{m}$

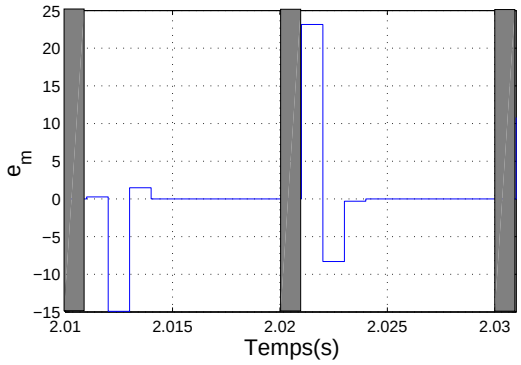

Fig. 10. Zoom sur la synchronisation du message m

IV. Conclusion

Dans ce papier, un schéma de transmission basé sur des systèmes dynamiques hybrides a été conçu pour les communications privées. Dans la partie émetteur, un système chaotique en temps continu dit de Colpitts est combiné avec un système en temps discret dit de Hénon modifié dans le but de réaliser une structure complexe de l'émetteur qui soit "robuste" notamment à une attaque à texte clair connu. Ici, le système doit encore être robustifié par rapport à une attaque à texte clair connu en introduisant des retards [19] et aussi en faisant intervenir les états continus de façon à ne pas respecter la condition de recouvrement de l'observabilité. Ceci sera développé dans nos travaux ultérieures. Dans le canal de transmission, les sorties envoyées ont été choisies en accord avec la condition de rang d'observabilité pour le système en temps continu (Colpitts) et pour le système en temps discret (Hénon modifié). Pour la sortie, la stratégie consiste a multiplexer les deux sorties : le signal continu échantillonné $y_1 = z_1$ (Colpitts) et le signal en temps discret $y_2 = x_2$ (Hénon modifié) dans un signal de sortie composite. Dans notre étude, nous avons montré que la reconstitution du message de l'émetteur discret est subordonnée à la synchronisation de l'émetteur et du récepteur (observateur) en temps continu et que l'échange d'informations se fait de façon discrète. Cette étude est illustrée en simulation. Les résultats de simulation obtenus ont confirmé que le message est reconstitué avec succès (au niveau du récepteur (observateur) en temps discret) si et seulement si les deux systèmes en temps continu (Colpitts et son observateur) sont synchronisés.

En perspectives, nous envisageons de :

- robustifier le système par rapport à une attaque à texte clair connu en introduisant des retards [19].
- faire intervenir les états continus de façon à ne pas respecter la condition de recouvrement de l'observabilité
- appliquer cette méthode de transmission pour crypter une image.
- implémenter le schéma de transmission sur une carte dspace.

Références

[1] Anstett F., Millerioux G et Bloch, G., "Chaotic Cryptosystems : Cryptanalysis and Identifiability", IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications,vol 53, n°.12, December 2006.

[2] Barbot J.P., Belmouhoub I et Boutat-Baddas L., "Observability Bifurcations : Application to Cryptography", in Chaos in Automatic Control, Taylor and Francis, 2005.

[3] Belmouhoub I., Djemaï M. et Barbot J. P., "Observability quadtatic Normal Form for Discrete-Time systems" ,IEEE Transactions on Automatic Control,vol. 50, n°.7, July 2005.

[4] Dedieu H., Kennedy M.P et Hasler M., "Chaos shift keying : modulation and demodulation of a chaoticcarrier using self-synchronizing Chua's circuits", IEEE Transactions on Circuits and Systems, Circuits and Systems II : Analog and Digital Signal Processing, vol 40, n°.10, pp 634-642, 1993.

[5] Djemaï. M., Barbot.J. P. et Belmouhoub I., "Discrete-Time Normal Form for Left Invertibility Problem", European Journal of Control, vol. 15, n°.02, pp 194-204, 2009.

[6] Dmitriev A. S., Kassian G.A et Khilinsky A. D., "Chaotic synchronization of henon mappings : The information approach, Technical Physics Letters", vol. 28, n°.05, may 2002.

[7] Freeland, G.C.et Durrani T.S., "Nonlinear state observers for chaotic systems and their application to communications Signal Process", Exploiting Chaos in Signal Processing, IEE Colloquium on,1994.

[8] Ghanes. M., DeLeon J., Glumineau A et J. P. Barbot, "A robust output feedback controller of the induction motor drives : new design and experimental validation", International Journal of Control, vol. 83, pp. 484-497, 2010.

[9] Hermann R. et Krener A. K, "Nonlinear observability,", IEEE Trans on Automatic Control, vol. 22, pp. 728-740, 1977.

[10] L'Hernault M., Barbot J.P et Ouslimani A., "Feasability of Analogue Realization of Sliding Mode Observer : Application to Data Transmission", IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications,vol 55, n°.02, March 2008

[11] Maggio G. M. et Feo. O.D., "Nonlinear Analysis of the Colpitts Oscillator and Application to Design", IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications,vol 49, n°.09, September 1999.

[12] Maggio G. M. et, Kennedy M. P., "Experimental manifestations of chaos in the Colpitts oscillator",Proc. of ICECS, Seville, spain, pp 194-204, 1997.

[13] Nijmeijer H., "On Synchronization of Chaotic Systems", Proc. 36th Conference on Decision and Control, San Diego, California USA, December 1997.

[14] Nijmeijer H. et Mareels Iven M.Y., "An observer Looks at Synchronization", IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications, vol. 44, n°.10, October 1997.

[15] Parlitz U., Chua L.O., Kocarev L.,Halle K.S et Shang A., "Transmission of digital signals by chaotic synchronization", International Journal of Bifurcations and Chaos", vol.3, n°.02, pp.973-977, 1993.

[16] Pecora L. M. et Carroll T.L., "Synchronization in Chaotic Systems", Physicals Review and Letters, pp. 821-824, 1990.

[17] Vesely K et Podolsky J.," Chaos in a modified Hénon- Heiles system describing geodesics in gravitational waves", Technical Physics Letters A, vol.271, pp.368-371, July 2000.

[18] Wu C.W et Chua L.O., "simple way to synchronize chaotic systems with applications to secure communications systems", International Journal of Bifurcations and Chaos, vol.3, n°.06, pp.1619-1627, 1993.

[19] Zheng G., Boutat D.,Floquet T et Barbot J.P., "Secure data transmission based on multi-input multi-output delayed chaotic system", International Journal of Bifurcations and Chaos, vol.18, n°.02, 2007.