مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (31) العدد (1) 2009
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (31) No. (1) 2009

اقتراح نظام تشفير مستند على نظرية الفوضى والمنطق الغامض

ساري حاج حسين *

(تاريخ الإيداع 8 / 10 / 2008. قُبِل للنشر في 2009/2/15)

□ الملخّص □

لقد كشفت الأبحاث أن قدرة العقل البشري على معالجة مقادير ضخمة من المعلومات لحظياً إنما يعود إلى التطور والتغير الشديدين في الديناميكية الفوضوية، وهذا، حقيقةً، ما يجعل العقل البشري مختلفاً عن آلة الذكاء الصنعي.

ويسود حالياً اعتقاد مفاده أن المنطق الغامض ونظرية الفوضى متصلان بالحجة البشرية ومعالجة المعلومات، كما يُعتقد أيضاً أن البيانات الغامضة والاستنباط المنطقي الغامض مهمان للغاية في المعالجة المعقدة للمعلومات التي تتم داخل العقل البشري؛ وذلك لأنّ تقديم أوصاف رياضية دقيقة لهذه العمليات والنماذج أمرٌ مستحيلٌ في إطار المعرفة العلمية المتاحة للبشر اليوم.

نقدم في هذا البحث تطبيقاً على التكامل ما بين نظرية الفوضى والمنطق الغامض يتمثل بنظام تشفير فوضوي غامض. نحاول فيه أن نقدم مقاربة جديدة وواعدة ربما تستند عليها الأبحاث النظرية والاستقصاءات التي تستهدف الذكاء البشري في المستقبل.

الكلمات المفتاحية: المنطق الغامض– نظرية الفوضى– تكرار الحالة– النموذج الغامض– لامساواة مصفوفية خطية– سلسلة متزايدة بقوة– إشارة التقنيع– طريقة لايبونوف– متمم شور– خريطة هنون.

* قائم بالأعمال معاون– قسم هندسة البرمجيات ونظم المعلومات– كلية الهندسة المعلوماتية– جامعة تشرين– اللاذقية– سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (31) العدد (1) 2009
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (31) No. (1) 2009

Proposal Of A Cryptosystem Based On Chaos Theory And Fuzzy Logic

Sari Haj Hussein *

(Received 8 / 10 / 2008. Accepted 15 / 2 / 2009)

□ ABSTRACT □

Researches have revealed that due to the drastically evolving and changing chaotic dynamics the human brain can process massive information instantly. It is actually what makes the brain different from an artificial-intelligence machine.

Currently, it is widely believed that both fuzzy logic and chaos theory are related to human reasoning and information processing. It is also believed that to understand the complex information processing within the human brain, fuzzy data and fuzzy logical inference are essential, given that precise mathematical descriptions of such models and processes are clearly out of question within the framework of scientific knowledge available to human beings nowadays.

In this paper, a practical example of integrating fuzzy logic and chaos theory, represented by a Fuzzy Chaotic Cryptosystem (FCC), is introduced. An attempt is also being made to provide a new and promising approach that might be adopted by theoretical researches on and investigations about human intelligence in the future.

Keywords: Fuzzy logic, chaos theory, ergodicity, fuzzy model, linear matrix inequality (LMI), superincreasing sequence, masking signal, Lyapunov method, Schur Complement, Hénon Map.

* **Academic Assistant -Department of Software Engineering and System Analysis-Faculty of Informatics Engineering-Tishreen University-Lattakia-Syria.**

مقدمة:

إن علم التشفير Cryptography هو ذاك العلم الذي يدرس الكتابة السرية، ويهتم بالطرق التي يمكن باستخدامها ترميز الاتصالات والبيانات بشكل يمنع كشف محتواها بطرق التجسس أو التقاط الرسائل. يستند علم التشفير في تحقيق ذلك على مجموعة من الطرق أو أنظمة التشفير التي تتيح لأناس محددين فقط الاطلاع على محتوى الرسائل.

إن علم التشفير ضارب في القدم وتعود أصوله الأولى إلى مصر القديمة، وقد شكل هذا العلم بدءاً من يوليوس قيصر إلى ماري ملكة اسكتلندا وصولاً إلى أبراهام لنكولن في الحرب الأهلية الأمريكية جزءاً من التاريخ البشري.

كان استخدام علم التشفير في ذاك الزمن محصوراً بالخدمات العسكرية والدبلوماسية والحكومية بشكل عام؛ إذ كان يستخدم بوصفه أداة لحماية الأسرار والاستراتيجيات القومية.

أما اليوم فقد أصبحت الإنترنت جزءاً لا غنى عنه من حياتنا اليومية، وإن الاتصالات المتنوعة التي تتم عبر هذه الشبكة كرسائل البريد الإلكتروني، ومستعرضات الويب غير آمنة على الإطلاق في إرسال البيانات واستقبالها.

لهذا السبب تم تقديم العديد من طرق التشفير لتأمين الاتصال عبر الإنترنت. نذكر على سبيل المثال خوارزمية معيار تشفير البيانات Data Encryption Standard (DES) التي اعتمدتها الحكومة الفدرالية الأمريكية بوصفها معياراً. ومن الأمثلة الأخرى نذكر خوارزمية تشفير البيانات العالمية International Data Encryption Algorithm (IDEA) و الخوارزمية RSA (التي طورها العلماء Rivest و Shamir و Adleman). تستند كل خوارزميات التشفير هذه على نظرية الأعداد ولم يتمكن أحد على الإطلاق من إثبات أنها آمنة تماماً.

يمكن للتشفير أن يكون ضعيفاً أو قوياً وتقاس قوة التشفير بمقياسين هما الوقت والموارد اللازمة لاسترداد النص الأصلي. إن التشفير القوي يجعل فك تشفير النص المشفر صعباً للغاية من دون امتلاك أدوات مناسبة. بكلمة أخرى، إذا توفر الوقت اللازم والقوة الحسابية اللازمة (حتى ولو كانت بليون حاسوب يقوم كل منها ببليون عملية اختبار في الثانية الواحدة) فإن فك تشفير ناتج التشفير القوي يكون مستحيلاً قبل نهاية الكون. قد يعتقد المرء ببساطة أن التشفير القوي سيصمد وبقوة بوجه أعتى محللي الشفرة Cryptanalysis، إلا أن أحداً لا يستطيع إثبات أن أقوى أنظمة التشفير المتداولة اليوم سيصمد بوجه القوة الحسابية التي ستكون متوفرة غداً. لهذا السبب نجد أن بعضاً من النظريات الواعدة ومنها نظرية الفوضى يمكن تبنيها لتقوية أنظمة التشفير الحالية.

أهمية البحث وأهدافه:

تأتي أهمية هذا البحث من الأهمية المتزايدة لمسألة الأمان نظراً للنمو السريع والاستخدام الواسع للبيانات الرقمية، إضافة إلى العدد الهائل من الأعمال التجارية التي يتم إنجازها على شبكة الإنترنت والبروز المرعب لظاهرة الإرهاب العالمي، والتي غذت بمجموعها الحاجة لطرق أفضل لحماية هذه الحواسيب والمعلومات التي تخزنها وتعالجها وتنقلها، وأدت في نهاية المطاف إلى نشوء منظمات متخصصة كبيرة الحجم تشترك كلها في هدف واحد ألا وهو حماية أمن الأنظمة المعلوماتية وموثوقيتها.

أما أهداف البحث فتتلخص في الاستعانة بنظريات أخرى غير نظرية الأعداد التقليدية لتقوية خوارزميات التشفير المتداولة حالياً والتي لا يمكننا الجزم بأمانها المطلق بأي شكل من الأشكال.

طريقة البحث ومواده:

يبدأ هذا البحث بنقد بعض خوارزميات التشفير المتداولة مؤكداً ضرورة الإتيان بأفكار جديدة في هذا المجال، ثم ينتقل إلى شرح مبسط لنظرية الفوضى وإسهامات العلماء في بناء أنظمة التشفير الفوضوية وتطويرها، كما يختار أحد النماذج الغامضة معللاً سبب الاختيار.

بعدها ينتقل البحث إلى شرح مفصل لنظام التشفير الفوضوي الغامض المقترح وآلية عمله، ويبرهن أخيراً على أن فك التشفير يعطي وبنجاح النص الأصلي مع هامش خطأ ضئيل للغاية.

أُجري البحث في كليتي الهندسة المعلوماتية والهندسة الميكانيكية والكهربائية في الفصل الأول من العام الدراسي 2008/2007 في أثناء عملنا على مقرر أمن المعلومات.

أما بالنسبة إلى أدوات البحث فقد استخدمنا الأدوات البرمجية التالية:

1) الأداة fuzzyTECH [1] التي تحوي محرراً ومحللاً يساعد في تصميم أنظمة المنطق الغامض على اختلافها.

2) الأداة XpertRule Knowledge Builder [2] وهي بيئة تطوير للتطبيقات المستندة على المعرفة، وقادرة على تمثيل المعرفة بوصفها أشجاراً أو قواعد أو حالات مدعومة بمحرك استنباط، إضافة إلى قدرتها على العمل مع الأغراض المعرفية المخصصة.

3) الأداة MATLAB مدعومةً بالحزمة القوية Type-2 Fuzzy Logic [3].

ولا بد من أن نذكر رسالة الأخبار التي تصدر بشكل ربع سنوي عن الاتحاد العالمي لبرمجة المنطق Association for Logic Programming (ALP) [4] والتي نهمّ على قراءتها منذ سنين خلت، كما نشكر الردود الكريمة على استفساراتنا التي تفضل بها الأساتذة الأعضاء في الاتحاد المذكور والتي اختصرت الطرق وهونت عملنا البحثي إلى حد لا يمكن تخيله.

العلاقة بين المنطق الغامض ونظرية الفوضى:

على الرغم من أن العلاقة بين المنطق الغامض ونظرية الفوضى غير مفهومة بعد بشكل كامل، فقد مضى على دراسة التفاعل بينهما أكثر من عقدين من الزمن، على الأقل فيما يخص الظواهر التالية: التحكم الغامض بالفوضى، والأنظمة الغامضة التكيفية من سلاسل الزمن الفوضوية، والعلاقات النظرية بين المنطق الغامض ونظرية الفوضى، والنمذجة الغامضة للأنظمة الفوضوية ذات الخواص المحددة، وتشويش النموذج الغامض Takagi-Sugeno (TS).

لقد دخل المنطق الغامض ونظرية الفوضى المجال العلمي البحثي في الوقت نفسه تقريباً؛ إذ تم تقديم فكرة المنطق الغامض للمرة الأولى من قبل العالم Lotfi Zadeh في العام 1965 في بحثه المعنون "المجموعات الغامضة". في حين شكل اكتشاف العالم Edward Lorenz في العام 1963 أول دليل على الفوضى الفيزيائية، رغم إمكانية نسب دراسة الفوضى إلى بعض الأفكار الفيزيائية التي نشأت منذ مئات السنين وإلى أعمال الرياضي الفرنسي Jules Henri Poincaré في بداية القرن الماضي. والسؤال الذي يلح في طرح نفسه هنا! هل يمكن لهذا التزامن في النضوج العلمي أن يكون مصادفة؟

إن نظرية المجموعات الغامضة تحاكي الحجة البشرية باستخدام المعلومات التقريبية والبيانات غير الدقيقة لإصدار أحكام في بيئات عمل غير مؤكدة. من ناحية أخرى نجد أن نظرية الفوضى عبارة عن دراسة كيفية للسلوك غير الدوري وغير المستقر في الأنظمة الديناميكية غير الخطية المحددة.

الدافع وراء استخدام نظرية الفوضى:

إن السبب الذي يدفعنا إلى تطبيق نظرية الفوضى في التشفير يتمثل في بعض خواصها الأساسية المتمثلة بالحساسية للشروط الابتدائية (أو ما يعرف ببارامترات التحكم) وتكرار الحالة Ergodicity. هذه الخواص توافق متطلبات التشويش Confusion والنشر Diffusion للعالم Shannon التي يجب أن يتمتع بها نظام التشفير. لقد كتب Shannon في إحدى مقالاته [5]: "ليكون تحويل الدمج جيداً، يجب أن تكون التوابع معقدة وتستخدم كل المتحولات بطريقة حساسة بمعنى أن تفاوتاً بسيطاً في أي متحول يغير الخرج بشكل كبير". من الفروق المهمّة بين الفوضى والتشفير أن الأنظمة المستخدمة في الفوضى تكون معرفة على الأعداد الحقيقية، أما التشفير فيتعامل مع أنظمة معرفة على عدد منته من الأعداد الصحيحة. مع ذلك يسود اعتقاد بأنه يمكن لهاتين المقاربتين الإفادة من بعضهما [6].

يمكن لأنظمة التشفير الفوضوية أن تكون تماثلية أو رقمية، والتماثلية منها تكون مستندة على تقنية التزامن الفوضوية التي وردت في [7] لتصميم دارات تماثلية للاتصال الآمن عبر قنوات مفعمة بالضجيج. على أية حال لا يمكننا توسيع هذه الطريقة لتصميم خوارزميات التشفير الحديثة التي تضمن باستخدام التقنيات الرقمية [8]. يمكن تصنيف أنظمة التشفير الفوضوية الرقمية إلى أنظمة تشفير دفقية Stream، وأنظمة تشفير كتلية Block. تستخدم أنظمة التشفير الدفقية الأنظمة الفوضوية لتوليد دفق مفاتيح شبه عشوائي Pseudo-Random يُستخدم لتقنيع النص الأصلي، في حين تستخدم أنظمة التشفير الكتلية النص الأصلي و/أو المفاتيح السرية عدة مرات للحصول على النص المشفر. وبالإضافة إلى ما ذكر، تم تقديم عدد من أنظمة التشفير الفوضوية واختبارها في [9].

وبدءاً من العمل الريادي الأول الذي قدمه العالمان Carroll و Pecora [7] والذي قدم كثيراً من الإسهامات فيما يتعلق بالتزامن بين نظامين فوضويين حيث يولد نظامان فوضويان مقترنان بشكل مناسب ذبذبات متماثلة.

تم تقديم العديد من النظريات [10] لتحقيق سلوك التزامن ذي النوع رئيس–تابع Master-Slave. يتكون نوع رئيس– تابع هذا من نظام فوضوي أصلي يسمى نظام المشغل Drive System، تكون مسؤوليته توليد إشارة مشغل Driving Signal لمزامنة نظام آخر يسمى نظام الاستجابة Response System. بالإضافة إلى ذلك، تكون الإشارات الفوضوية عريضة الحزمة وشبيهة بالضجيج ويصعب التنبؤ بها؛ لذا يمكن استخدامها في سياقات مختلفة لتقنيع الأمواج الحاملة للمعلومات، كما يمكن استخدامها بوصفها أمواجاً معدلة في أنظمة الطيف المنتشر.

إن الفكرة وراء التقنيع الفوضوي [11] تقوم على إضافة الرسالة مباشرةً في إشارة فوضوية شبيهة بالضجيج عند نهاية المرسل أما التعديل الفوضوي [12] فيقوم على حقن الرسالة في نظام فوضوي على اعتبار أنها إرسال ذو طيف منتشر. يقوم كاشف لاحقاً عند المستقبل باستعادة الرسالة. على أية حال فإن مقاربة تقنيع الإشارة أو تعديل البارامترات المطبقة على الاتصال الفوضوي تؤمن فقط مستوىً أدنى من الأمان كما ورد في [13]. نقدم هنا نظامَ تشفير فوضوياً غامضاً يستخدم نظرية نظام التشفير الأساسية للحصول على مقاربة أكثر أماناً.

إيجابيات نظام التشفير المقترح:

إن نظام التشفير الفوضوي الغامض المقترح والمستند على النموذج الغامض Takagi-Sugeno (TS) يتمتع بالمزايا الإيجابية التالية [14]:

1) مناسب لمعظم الأنظمة الفوضوية متقطعة الزمن المعروفة.
2) إن مشكلة التزامن التي ستحل باستخدام تقنية اللامساواة المصفوفية الخطية Linear Matrix Inequality (LMI) بسيطة ويمكن حلها باستخدام الأدوات البرمجية القوية.
3) إن السلاسل المتزايدة بقوة Superincreasing Sequences المولدة من الإشارات الفوضوية متغيرة مع الزمن.
4) يمكن تضمين النص المشفر في الحالة أو إخراجه من نظام المشغل وهذا يعطي مرونة لنظام التشفير.
5) يمكن استخدام هذا النظام من قبل عدة مستخدمين.

مبدأ عمل نظام التشفير المقترح:

نمثل في نظام التشفير المقترح وبدقة الأنظمة الفوضوية متقطعة الزمن باستخدام النموذج الغامض TS ثم نولد سلسلة متزايدة بقوة باستخدام إشارة فوضوية يمكن استخدامها وبسهولة بوصفها خرجاً لنظام المشغل الفوضوي الغامض TS أو في أي حالة أخرى يقترب فيها خطأ التزامن من الصفر. وبالحديث عن التشفير فإن الرسالة (النص الأصلي) تُشفر باستخدام السلسلة المتزايدة بقوة على طرف نظام المشغل الأمر الذي يعطي النص المشفر. يمكن إضافة هذا النص إلى خرج أو إلى حالة نظام المشغل باستخدام الطرق الواردة في [15]. ومن ثم يُرسل النص المشفر متضمناً الإشارة إلى طرف نظام الاستجابة. يتم تحقيق التزامن الفوضوي بين نظامي المشغل والاستجابة بحل مشكلة LMI. وباستخدام التزامن يمكن للمرء أن يعيد توليد السلسلة المتزايدة نفسها بالقوة ويستعيد النص المشفر عند نظام الاستجابة. أخيراً وباستخدام السلسلة المتزايدة بقوة المعاد توليدها، نفك تشفير النص المشفر إلى النص الأصلي.

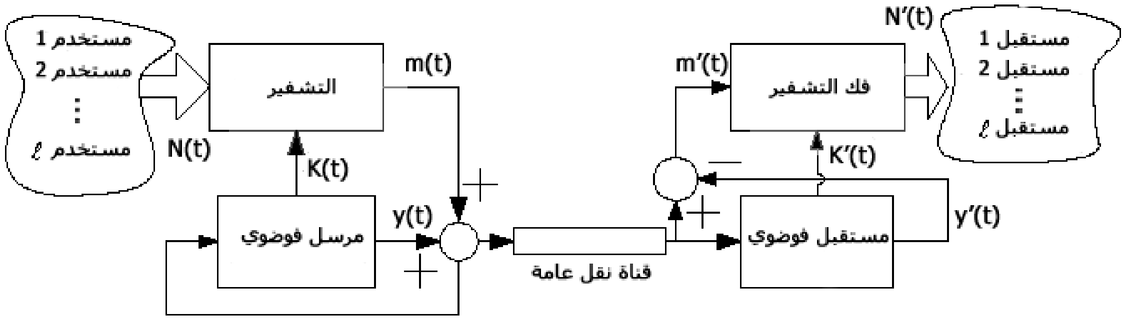
لنعرض أولاً مجموعة المصطلحات المتعلقة بنظام التشفير المقترح. نسمي الرسالة المركبة N التي سيتم إرسالها بالنص الأصلي الذي يتم ترميزه باستخدام السلسلة المتزايدة بقوة S_i. يعطي النص المرمز النص المشفر E. تتم استعادة النص الأصلي من النص المشفر بتنفيذ تابع فك التشفير D. تستخدم عمليتا التشفير وفك التشفير المفتاحين K و 'K على الترتيب. نعرف السلسلة المتزايدة بقوة كما يلي.

<u>تعريف</u>: نقول عن السلسلة الحقيقية $\{S_i\}_{i=1}^{\ell}$ إنها متزايدة بقوة إذا تحقق ما يلي:

$$S_j > \sum_{i=1}^{j-1} S_i , \ell \geq j > 1 \text{ and all } S_i > 0$$

لاحظ في مشاكل السلاسل المتزايدة بقوة التقليدية [16] أن السلسلة تكون مجموعة من الأعداد الصحيحة الموجبة في حين أن السلسلة المتزايدة بقوة المستخدمة عبارة عن مجموعة من الأعداد الحقيقية الموجبة.

إن نظام التشفير الفوضوي الغامض المقترح موضح في الشكل (1).



الشكل (1): المخطط الكتلي لنظام التشفير الفوضوي الغامض.

عند تشفير النص الأصلي، يتم أولاً تمثيل نظام فوضوي متقطع الزمن باستخدام النموذج الغامض TS بوصفه نظاماً مشغلاً يمكننا من خرجه أن نولد دفقاً من المفاتيح $K(t-i), i=0,...,\ell-1$. ثم نستخدم دفق المفاتيح $K(t),K(t-1),...,K(t-\ell+1)$ لتشكيل سلسلة متزايدة بقوة $\{S_i\}, i=1,...,\ell$ حيث ℓ هو عدد الرسائل. و $S_1(t)=|K(t)|+\tau, S_j(t)=\sum_{i=1}^{j-1} S_i(t)+|K(t-j+1)|+\tau$ حيث $j=2,...,\ell$ و $\tau>0$.

وبدمج السلسلة المتزايدة بقوة مع النص الأصلي $N=[n_1 n_2 ... n_\ell], n_i \in \{0,1\}$ ، نحصل على النص المشفر:

$$E(N(t),K(t),K(t-1),...,K(t-\ell+1)) = S(t)N(t)^T = E(t)$$

حيث E هو تابع التشفير. نحول الآن تابع التشفير E(t) إلى $\zeta(t)=(E-\frac{H(t)}{2})/(\gamma\frac{H(t)}{2})$ حيث $H=\sum_{i=1}^{\ell} S_i$ و γ ثابت بحيث يكون $\zeta(t)\in(-0.01,0.01)$ صغيراً كفاية بشكل لا يؤدي إلى إتلاف الخواص الفوضوية لإشارة التقنيع. نضيف $\zeta(t)$ إلى إشارة التقنيع ومن ثم نرسل الإشارة المقترنة بالثابت إلى نظام الاستجابة.

عند فك تشفير النص المشفر، يستعيد نظام الاستجابة الغامض TS أولاً دفق المفاتيح $K'(t-1), i=0,...,\ell-1$ والإشارة $\zeta'(t)$ عن طريق التزامن الذي سنشرحه بالتفصيل في الفقرة التالية.

يمكننا بعدها الحصول على السلسلة المتزايدة بقوة $\{S'_i(t)\}, i=1,...,\ell$ حيث $S'_1(t)=|K'(t)|+\tau, S'_j(t)=\sum_{i=1}^{j-1} S'_i(t)+|K'(t-j+1)|+\tau$ و $j=2,...,\ell$ و $\tau>0$. ثم نحول $\zeta'(t)$ بشكل عكسي للحصول على $E'(t)=\zeta'(t)(\gamma H'(t)/2)+H'(t)/2$. أخيراً نستعيد النص الأصلي بفك تشفير النص المشفر E'(t) كما يلي:

$$N'(t) = D(K'(t), E'(N(t),K'(t),K'(t-1),...,K'(t-\ell+1)))$$

حيث D هو تابع فك التشفير الذي يستخدم المفتاح المستعاد $K'(t-i), i=0,...,\ell-1$. أما خوارزمية فك التشفير فتعرف كما يلي:

```
V' = E'
for i = ℓ down to 1
begin
if V' – S'ᵢ > -ε
n'ᵢ = 1
V' = V' – S'ᵢ
else
```

```
n'i = 0
end
```

حيث $0 < \varepsilon < \tau$.

نلاحظ أنه إذا كانت $n_\ell(t)=1$ (أو $n_\ell(t)=0$) فإن $E(t)\geq S_\ell(t)$ (أو $E(t)\leq S_\ell(t)-\tau$). بعد وقت قصير يعاد تزامن نظام الاستجابة مع نظام المشغل الأمر الذي يعني أن E'(t) = E(t) ولهذا السبب يكون $S'_\ell(t)=S_\ell(t)$. أخيراً يكون $n'_\ell(t)=1$ (أو $n'_\ell(t)=0$) وذلك استناداً إلى الخوارزمية الواردة أعلاه وتستعاد النصوص الأصلية الأخرى $n'_{\ell-1}(t)...n'_1(t)$ في حلقة التكرار.

نلاحظ أيضاً أنه عندما يخدم نظام التشفير هذا ℓ مستخدماً في الوقت نفسه فإن النص الأصلي N يكون مكوناً من رسائل من عدة مستخدمين بمعنى أن بتاً واحداً فقط من كل مستخدم ينقل في وقت واحد أما في حالة مستخدم واحد فإن ℓ بتاً من رسالة المستخدم تنقل في الوقت نفسه. إن هذا يؤكد إمكانية استخدام نظام التشفير هذا من قبل عدة مستخدمين كما يوضح سرعة نقل البيانات العالية التي يتمتع بها عند استخدامه من قبل مستخدم واحد.

النتائج والمناقشة:

لنبين كيفية فك التشفير باستخدام التزامن الفوضوي. يتم أولاً تقنيع النص المشفر بخرج النظام الفوضوي، وتنفذ عملية التعديل بحقن إشارة التقنيع في الناقل الفوضوي الغامض، ثم ترسل الإشارة المقنعة إلى المستقبل الفوضوي الغامض حيث يستخلص النص المشفر استناداً إلى طرق التقنيع.

افترض أن النص المشفر $\zeta(t)$ قد أضيف مباشرةً إلى خرج النظام الفوضوي. يعبر عندها عن المرسل الفوضوي بوصفه نموذجاً غامضاً TS كما يلي:

Transmitter Rule i: IF $\bar{y}(t)$ is F_i THEN

$x(t+1) = A_i x(t) + b_i(t) + L_i M\zeta(t)$

$\bar{y}(t) = Cx(t) + M\zeta(t)$, i = 1, 2, …, r

حيث L_i, i = 1, 2, …, r هي مقادير الكسب التي سيتم تحديدها، و M هو مفتاح تقنيع الخرج العام والذي يقنع النص المشفر xi، و $\bar{y}(t)$ هي الإشارة المقترنة التي سيتم بثها إلى المستقبل عبر قناة نقل عامة. نحصل على النتيجة المستنبطة فوضوياً للمرسل الفوضوي كما يلي:

$$\begin{aligned} x(t+1) &= \sum_{i=1}^{r}\mu_i(\bar{y}(t))\{\bar{A}_i x(t) + b_i(t) + L_i\bar{y}(t)\} \\ \bar{y}(t) &= Cx(t) + M\zeta(t) \end{aligned} \qquad (1)$$

حيث $\bar{A}_i = A_i - L_i C$.

لاستعادة النص المشفر، يتم تصميم المستقبل كما يلي:

Receiver Rule i: IF $\bar{y}(t)$ is F_i THEN

$x'(t+1) = A_i x'(t) + b_i(t) + L_i(\bar{y}(t) - y'(t))$

$y'(t) = Cx'(t)$, i = 1, 2, …, r

أما المستقبل الكلي فيستنبط كما يلي:

$$x'(t+1)=\sum_{i=1}^{r}\mu_i(\bar{y}(t))\{A_i x(t)+b_i(t)+L_i(\bar{y}(t)-y'(t))\}$$
$$y'(t)=Cx'(t) \tag{2}$$

وبافتراض أن إشارات الخطأ $e_x(t) = x(t) - x'(t)$ و $e_y(t)=\bar{y}(t)-y'(t)$. استناداً للعلاقتين (1) و (2) فإن قيم الخطأ الديناميكية لـ $e_x(t)$ و $e_y(t)$ يعبر عنها كما يلي:

$$e_x(t+1)=\sum_{i=1}^{r}\mu_i(\bar{y}(t))(A_i-L_iC)e_x(t) \tag{3}$$

$$e_y(t)=Ce_x(t)+M\zeta(t) \tag{4}$$

نحصل على شرط استقرار العلاقة (4) من طريقة Lyapunov. نوضح هنا النتيجة الرئيسة.

<u>نظرية</u>: افترض المرسل الفوضوي (1) والمستقبل الفوضوي (2). يمكن استعادة النص المشفر من $\zeta(t)=\dfrac{1}{M}e_y(t)$ ومزامنة كل حالات المرسل والمستقبل الفوضويين إذا وجدت مصفوفة P محددة بشكل موجب ومقادير كسب L_i, $I = 1, 2, \ldots, r$ بحيث تتحقق LMI التالية:

$$\begin{bmatrix} P & (PA_i-W_iC)^T \\ PA_i-W_iC & P \end{bmatrix}>0\text{, for all i} \tag{5}$$

حيث $W_i = PL_i$.

<u>البرهان</u>: بإعطاء تابع Lyapunov كما يلي: $V(\tilde{x}(t))=e_x^T(t)Pe_x(t)>0$. بأخذ فرق $V(t)$ على طول قيم الخطأ الديناميكية في العلاقة (3) نحصل على:

$$\begin{aligned}\Delta V(e_x(t)) &= V(e_x(t+1)-V(e_x(t))\\ &=\sum_{i=1}^{r}\mu_i^2(\bar{y}(t))e_x^T(t)[\bar{A}_i^T P\bar{A}_i-P]e_x(t)+\\ &\sum_{i<j}^{r}\mu_i(\bar{y}(t))\mu_j(\bar{y}(t)).e_x^T(t)[\bar{A}_i^T P\bar{A}_j+\bar{A}_j^T P\bar{A}_i-2P]e_x(t)\end{aligned} \tag{6}$$

حيث $P > 0$ و $\bar{A}_i=A_i-L_iC$. لاحظ أنه إذا كان $\bar{A}_i^T P\bar{A}_i-P<0$ فإن $\bar{A}_i^T P\bar{A}_j+\bar{A}_i^T P\bar{A}_i-2P<0$. إن هذا يعني أنه إذا وجد P و L_i بحيث يكون الشرط في العلاقة 5 محققاً فإن $\bar{A}_i^T P\bar{A}_i-P<0$ وذلك استناداً إلى متمم Schur. لتكن Q– المصفوفة المحددة بشكل سالب العظمى لـ $\bar{A}_i^T P\bar{A}_i-P$ من أجل أي i. عندئذٍ يكون $\Delta V(e_x(t))\le -e_x^T(t)Qe_x(t)<0$ وهكذا يقترب خطأ التزامن $e_x(t)$ من الصفر عندما تسعى t إلى اللانهاية. ووفقاً للعلاقة (4) تقترب $e_y(t)$ من $M\zeta(t)$ مع سعي t إلى اللانهاية.

وبما أن معدل اقتراب خطأ التزامن $e_x(t)$ يؤثر في فعالية عملية النقل، فمن الممكن تنفيذ تصميم نظام التشفير الفوضوي بحل المشاكل LMI كما يلي:

نظام تشفير فوضوي مع معدل انحلال:

minimize β

subject to $P>0,\ 0<\beta<1$

$$\begin{bmatrix} \beta P & (PA_i-W_iC)^T \\ PA_i-W_iC & P \end{bmatrix}>0,\ \textit{for all i}$$

حيث $W_i = PL_i$. تصبح العلاقة (6) كما يلي: $\Delta V(e_x(t)) \le -(1-\beta)V(e_x(t))$ حيث يحدد البارامتر β معدل الانحلال.

مثال: تأمل نظام التشفير الفوضوي الذي يستخدم خريطة Hénon متقطعة الزمن التالية:

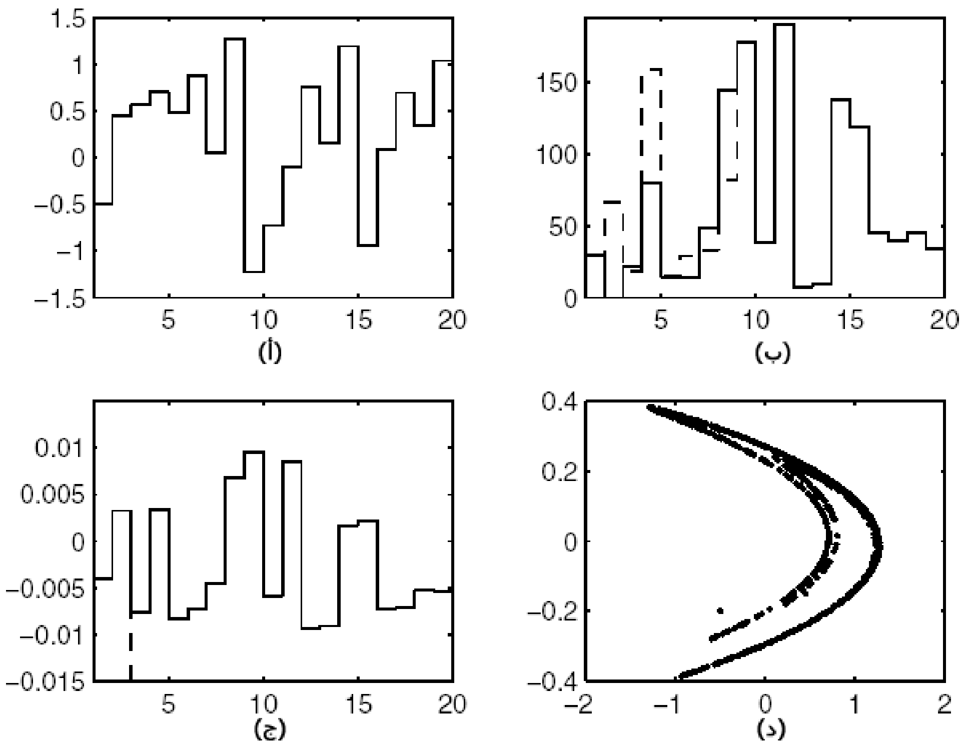
$$\begin{aligned} x_1(t+1) &= -x_1^2(t) + 0.3x_2(t) + 1.4 \\ x_2(t+1) &= x_1(t) \\ y(t) &= x_1(t) \end{aligned} \qquad (7)$$

ليكن $x_1(t)$ متحول الافتراض الأساسي Premise Variable للقواعد الغامضة. إن خريطة Hénon في القواعد الغامضة مكونة من $x(t) = [x_1(t) \quad x_2(t)]^T$, $C = [1 \quad 0]$ ومن المجموعات الغامضة $F_1(y(t)) = \frac{1}{2}(1+\frac{y(t)}{d})$ و $F_2(y(t)) = \frac{1}{2}(1-\frac{y(t)}{d})$ و:

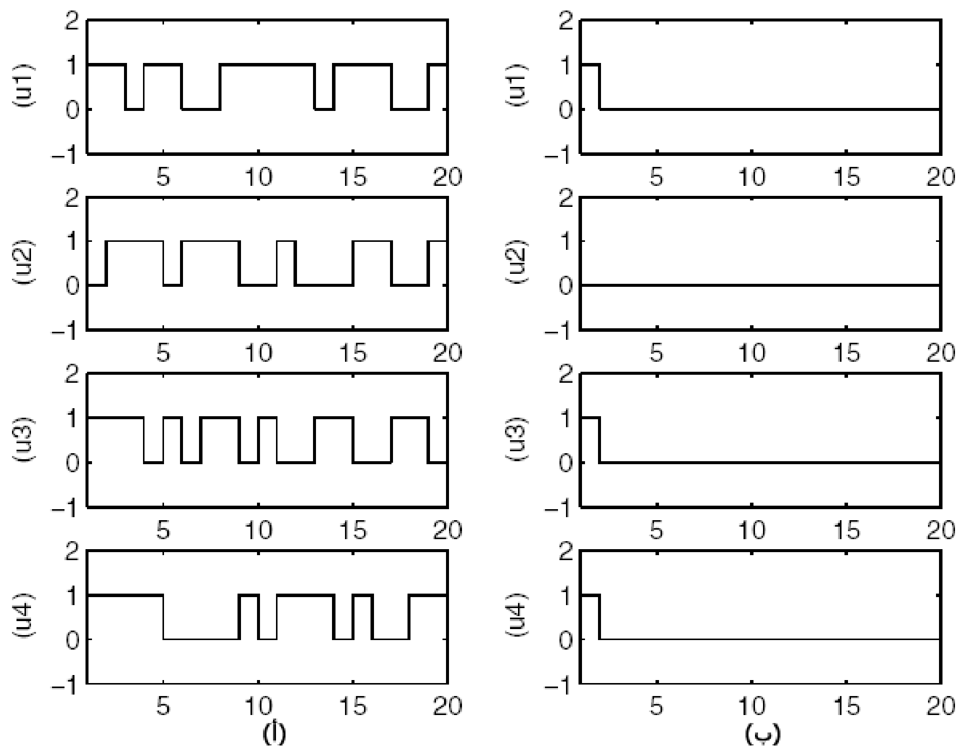
$$A_1 = \begin{bmatrix} -d & 0.3 \\ 1 & 0 \end{bmatrix}, A_2 = \begin{bmatrix} d & 0.3 \\ 1 & 0 \end{bmatrix}, b_1 = b_2 = \begin{bmatrix} 1.4 \\ 0 \end{bmatrix}$$

حيث $d = 2$ و $x_1(t) \in [-d \; d]$.

افترض أن نظام التشفير يخدم ثمانية مستخدمين والنصوص الأصلية بحوزتهم عبارة عن سلاسل ثنائية عشوائية. ولتكن الحالة $x_1(t)$ عبارة عن الخرج الذي يولد دفق المفاتيح $K(t)$. إن النص المشفر الذي ينتج من تطبيق الخوارزمية الواردة في الفقرة السابقة يضاف إلى خرج نظام المشغل $\bar{y}(t)$. ووفقاً للتمثيل الغامض للخريطة Hénon وللنظرية السابقة فإن المرسل الفوضوي (1) والمستقبل الفوضوي (2) يصممان مع أشعة كسب $L_1 = [-2.1384, 5.6608]^T$ و $L_2 = [2.1384, 5.6608]$. لاحظ أن بارامتر معدل الانحلال يحل على أنه $\beta = 0.1$. ومن أجل التبسيط، نضبط مفتاح تقنيع الخرج على أنه $M = 1$. يوضح الشكل (2) الإشارة المقترنة الفوضوية وتابعي التشفير E وفكه 'E والنص المشفر المقيس $m(t)$ و $m'(t)$ وشكل الطور الفوضوي على الترتيب. أما في الشكل (3) فتمثل u1 ~ u4 رسائل النص الأصلي الأربع الأولى المرسلة (عدد المستخدمين الكلي يساوي ثمانية)، كما نرى الأخطاء ما بين النص الأصلي المستعاد والنص الأصلي الأساسي من أجل الرسائل المذكورة نفسها.



الشكل (2): (أ) الإشارة المقترنة الفوضوية، (ب) تابعا التشفير E وفكه 'E، (ج) النص المشفر المقيس m(t) و m'(t)، (د) شكل الطور الفوضوي.



الشكل (3): (أ) النصوص الأصلية المرسلة من المستخدمين من 1 وحتى 4 (وعددهم الكلي 8)، (ب) الأخطاء بين الرسالة الأصلية والرسالة المستعادة للمستخدمين من 1 وحتى 4.

الاستنتاجات والتوصيات:

1) إن الأبحاث التي جرت في نظرية الفوضى والمنطق الغامض ما تزال غير كافية ولا بد من بذل المزيد من الجهود واعتصار المزيد من الأفكار في هذا المجال.
2) إن الأساليب الرياضية المتبعة في حقل أمن المعلومات بحاجة إلى إعادة نظر أكثر مما هي بحاجة إلى زيادة التعقيد واختبارات التقييم.
3) إن معايير الوقت والقوة الحسابية والهجمات على أنظمة التشفير الحالية تحتاج إلى إعادة ضبط بحيث تشمل أساليب التقوية الأخرى ومنها نظرية الفوضى.
4) إن البرمجيات المخصصة لنمذجة المنطق الغامض ما زالت بدائية وبحاجة إلى اهتمام أكبر من صانعي البرمجيات.
5) توجد نماذج غامضة أخرى، كالنموذج الغامض Mamdani، ووضعها قيد التجربة قد يعود بالفائدة.
6) إن إمكانية استخدام نظام التشفير الفوضوي الغامض المقترح من قبل عدة مستخدمين قد تفتح الباب على مصراعيه أمام جيل جديد من بروتوكولات تبادل المفاتيح التشفيرية Cryptographic Key Exchange Protocols.
7) إن سرعة نظام التشفير الفوضوي الغامض المقترح مرضية للغاية لدى استخدامه من قبل مستخدم واحد.
8) استندنا في تصغير الخطأ الحاصل في النظام على حل المشكلة LMI ونعتقد بأن تطوير ميكانيكيات التزامن قد يغنينا عن اتباع مثل هذه المقاربة.

المراجع:

1. http://www.fuzzytech.com, accessed May, 2007.
2. http://www.xpertrule.com, accessed May, 2007.
3. http://sipi.usc.edu/~mendel/software, accessed May, 2007.
4. http://www.cwi.nl/projects/alp/index.html, accessed May, 2007.
5. SHANNON,C.E. "*Communication theory of secrecy systems*," Bell Syst. Tech. J., Vol. 28, 1949, 656 – 715.
6. BAPTISTA, M.S. "*Cryptography with chaos*," Physics Letters A, Vol. 240,1998, 50 – 54.
7. PECORA L.M. and CARROLL,T.L. "*Synchronization in chaotic systems*," Phys. Rev. Lett., Vol. 64, 1990. 821 – 824.
8. FREY, D.R. "*Chaotic digital encoding: an approach to secure communication*," IEEE Trans. Circuits and Systems – II, Vol. 40, No. 10, 1993. 660 – 666.
9. SCHNEIER, B. "*Applied Cryptography – Protocols, algorithms, and source code in C*," 2nd ed., John Wiley & Sons: New York, 1996.
10. GRASSI, G. and MASCOLO,S. "*Synchronizing hyperchaotic systems by observer design*," IEEE Trans Circuits Syst – II, Vol. 46, 1999, 478 – 483.

11. CUOMO, K.M. OPPENHEIM, A.V. and STROGATZ, S.H. "*Synchronization of Lorenz-based chaotic circuits with applicatons to communications,*" IEEE Trans Circuits Syst – II, Vol. 40, 1993, 626 – 633.
12. LIAN,K.-Y. CHIANG, T.-S. and LIU,P. "*Discrete-time chaotic systems: applications in secure communications*," Int. J. Bifurcation Chaos, Vol. 10, 2000, 2193 – 2206.
13. SHORT, K. "*Steps toward unmasking secure communications*," Int. J. Bifurcation Chaos, Vol. 4, 1994, 959 – 977.
14. HALANG, Z. Li, W. and CHEN (EDS.),G. "*Integration of Fuzzy Logic and Chaos Theory,*" Springer-Verlag, Heidelberg, 2006.
15. LIAN, K.-Y. CHIU, C.-S. CHIANG, T.-S. and LIU, P. "*LMI-based fuzzy chaotic synchronization and communications,*" IEEE Trans. Fuzzy Systems, Vol. 9, No. 4, 2001, 539 – 553,.
16. DENNING, D.E.R. "*Cryptography and data security,*" Addison Wesley: New York, 1982.