Real-time video communication secured by a chaotic key stream cipher

Gilles Millérioux, Gérard Bloch, Jose Maria Amigo, Alexandre Bastos, Floriane Anstett

Real-time video communication secured by a chaotic key stream cipher

G. Millerioux * G. Bloch* J. M. Amigó† A. Bastos* F. Anstett*

Abstract — **An improvement of the chaotic inverse system encryption approach is suggested by introducing piecewise linearities. The usual design procedure is adapted in order to achieve an Input Independent Global Synchronization. Experiment of the resulting chaotic key stream encryption setup is conducted on a real-time video transmission. The secrecy level is assessed through a linear cryptanalysis.**

1 INTRODUCTION

Chaos-based encryption is currently an active field of research. Indeed, it is reasonable to think that there is likely a connection between the random-look behaviors exhibited by chaotic systems and the required properties for cryptosystems, like confusion and diffusion. Two chaos-based encryption schemes can be distinguished. On one hand, several works have focused on chaotic block encryption ciphers [1][2][3]. On the other hand, since the works of Pecora and Carroll [4], many secure communications schemes based on chaos synchronization have been suggested. A pioneering work involving a chaotic signal masking can be found in [5]. Among many secure communications protocols as chaotic switching, chaotic modulation, the inverse system approach presented in [6] has received a considerable attention.

The objective of this paper is twofold. First, based on a general equation of the encoder including either linear or piecewise linear dynamics, a unified analysis of existing message-embedding found in the literature for encryption purposes is performed. It is shown how the new theoretical results of [7][8] might be useful to equally deal with linear and piecewise linear dynamics while ensuring an Input Independent Global Synchronization (IIGS) which is a required property for inverse system approaches (section 2). Secondly, from a practical point of view, it is shown that the encryption can be included in a real time video transmission protocol over Internet and seems to be robust to linear cryptanalysis attacks (section 3).

*Centre de Recherche en Automatique de Nancy (CRAN, CNRS UMR 7039), CRAN - ESSTIN, 2 Rue Jean Lamour 54500 Vandoeuvre-Les-Nancy (France). Corresponding author E-mail: millerioux@esstin.uhp-nancy.fr

†Miguel Hernandez University, Dept. of Statistics and Applied Mathematics, Avda. del Ferrocarril s/n, 03202 Elche (Spain)

2 THE INVERSE SYSTEM APPROACH

2.1 Encoder side

Consider the general description of a switched discrete-time *encoder* system :

$$\begin{array}{rcccc} x_{k+1} & = & A_i x_k & + E_i & + B_i u_k \\ y_k & = & C_i x_k & + & D_i u_k \end{array} \quad (1)$$

where $x_k \in \mathbb{R}^n$, $y_k \in \mathbb{R}^m$, $u_k \in \mathbb{R}^m$ are respectively the state, the output and the external input. The state space $\mathbb{R}^n$ is partitioned into P distinct regions R_i with $\bigcup_{i=1}^{i=P} R_i \subseteq \mathbb{R}^n$. The matrices A_i, B_i, C_i, D_i, E_i are assigned with a one-to-one correspondence to the region R_i visited by x_k at the discrete time k. In an encryption context, the output y_k consists of the transmitted signal and acts as the ciphertext. The external input u_k results from an encoding function such that $u_k = e(x_k, m_k)$. m_k acts as the plaintext and it is assumed that e admits an inverse decoding function e^{-1} such that $m_k = e^{-1}(x_k, u_k)$. The piecewise linear configuration will correspond to matrices $A_i, \ldots, E_i$ which actually depend on index i whereas the linear configuration will correspond to constant matrices independent from i.

In the following, a brief overview on the connection between the general proposed encrypting scheme and some usual ones encountered in the literature is carried out.

In the masking scheme reported in [9], u_k is simply added to the output of the chaotic system. This scheme will be called output message embedded and amounts to set $B_i = 0$ (case 1).

When u_k is also injected in the dynamical equation of the chaotic system ($B_i \neq 0$), three distinct cases are usually considered and will correspond to dynamical/output message embedded schemes. First, the works of [6][10] are related to the linear configuration, where all the matrices are constant, and $D_i = D = 1$, meaning that the output is a scalar signal (case 2). Secondly, u_k may be mixed to the state vector such that x_k is replaced with $\bar{x}_k = x_k + M_i u_k$ (M_i being a suitable so-called "mixing matrix"). In a linear configuration, substituting x_k by $\bar{x}_k$ into (1) amounts to let $B_i = B = AM$, $D_i = D = CM$ with M a constant "mixing matrix". It corresponds to the works of [11] (case 3).

Thirdly, a less restrictive situation is considered in [12] or more recently in [8]. It corresponds to a piecewise linear configuration and amounts to let $B_i = A_i M_i$, $D_i = C_i M_i$ (case 4).
Finally, u_k may only be injected on the dynamical equation (dynamical message embedding) amounting to let $D_i = 0$. Such a situation is considered in [13] for a linear configuration and extended to a piecewise linear one in [7] (case 5).
The encoder (1) includes the so-called hybrid chaotic encryption scheme described in [14]. It combines a key-based nonlinear data encryption with a chaotic communication. The message m_k is encrypted via a suitable function e using a key stream x_k but is not directly transmitted to the receiver. Only a signal y_k of dimension $m < n$ is accessible from the output such that the reconstruction of the key stream becomes more difficult for an eavesdropper. It may prevent some attacks like the ones given in [15][16].

2.2 Decoder side

The design of a *decoder* system aims at ensuring that the respective state vectors x_k and $\hat{x}_k$ involved in the state reconstruction error $\epsilon_k = x_k - \hat{x}_k$ verify :

$$\lim_{k\to\infty} \|\epsilon_k\| = 0 \quad \forall \hat{x}_0 \quad \text{and} \quad \forall u_k \tag{2}$$

When (2) holds, it is said that an Input Independent Global Synchronization (IIGS) is achieved. When designing the decoder, the above-considered message embeddings must be distinguished into two classes : the dynamical-output embeddings (case 1 to 4) and the dynamical embedding (case 5).

2.2.1 Dynamical/output embedding

For dynamical/output embedding, let the decoder be described by :

$$\begin{cases} \hat{x}_{k+1} = A_i \hat{x}_k + E_i + L_i(y_k - \hat{y}_k) \\ \hat{y}_k = C_i \hat{x}_k \\ \hat{u}_k = D_i^{-1}(y_k - \hat{y}_k) \\ \hat{m}_k = e^{-1}(\hat{x}_k, \hat{u}_k) \end{cases} \tag{3}$$

with D_i assumed to be of full rank. Subtracting $\hat{x}_k$ of (3) from (1) yields :

$$\epsilon_{k+1} = (A_i - L_i C_i)\epsilon_k + (B_i - L_i D_i)u_k \tag{4}$$

Let us analyse the cases for which (2), that is the IIGS, may hold. As far as case 1 is concerned, taking into account (4) and $B_i = 0$, it is obvious that ϵ_k cannot converge towards zero since neither L_i nor D_i can be zero. A residual state reconstruction error will always persist, preventing an exact recovering of u_k. Consequently (2) is never fulfilled.
As for the case 2 (linear configuration), owing to $D = 1$, the second term in (4) vanishes provided that $L = B$ and (2) is fulfilled if the eigenvalues of $A - BC$ lie in the unit circle (discrete-time case).
Concerning the case 3, the second term turns into $(A - LC)Mu_k$. In order to ensure the IIGS, L can be computed such that $A - LC$ is nilpotent (discrete-time case only).
For the special case 4, owing to the presence of piecewise linearities, (4) turns into :

$$\epsilon_{k+1} = (A_i - L_i C_i)\epsilon_k + (A_i - L_i C_i)M_i u_k \tag{5}$$

As a consequence, the pole assignment of case 3 does no longer hold. To handle such a problem, we resort to the theoretical results of [8]. The design of the encoder/decoder setup consists of the computation of the pairs (L_i, M_i) according to Proposition 1.

Proposition 1 *The encoder/decoder (1)-(3) are IIGS and the plaintext m_k is exactly recovered if the gains L_i and the mixing matrices M_i are such that:*

1a) the null space $\mathcal{N}(A_i - L_i C_i) \neq \emptyset$ and $M_i \in \mathcal{N}(A_i - L_i C_i)$,

1b) $\epsilon_{k+1} = (A_i - L_i C_i)\epsilon_k$ is globally stable.

For in-depth study and proofs, we refer the reader to the above-cited paper. The sketch of the proof is the following. If *1a)* is satisfied, the second term of (5) vanishes. Then, *1b)* must be verified to achieve global convergence of ϵ_k. It can be shown that those conditions can be expressed in terms of Linear Matrix Inequalities (LMI), the solutions from which the L_i's $(i = 1, \ldots, P)$ are derived. Global stability is ensured by the existence of a special Lyapunov function called Poly-quadratic Lyapunov function [17].

2.2.2 Dynamical embedding

The dynamical embedding corresponds to the case 5 where u_k does not explicitly appear in the output equation $(D_i = 0)$. To cope with that special situation, the decoder iterative scheme must be modified. Let the decoder be now described by :

$$\begin{cases} \hat{x}_{k+1} = (P_i A_i - L_i C_i)\hat{x}_k + L_i y_k + \\ \qquad\qquad Q_i y_{k+1} + P_i E_i \\ \hat{u}_k = (C_i B_i)^{-1}(y_{k+1} - C_i A_i \hat{x}_k - C_i E_i) \\ \hat{m}_k = e^{-1}(\hat{x}_k, \hat{u}_k) \end{cases} \tag{6}$$

with $P_i = \mathbf{1}_n - Q_i C_i$. The decoder gets the structure of an Unknown Input Observer adapted to the piecewise linear configuration.

Subtracting $\hat{x}_k$ of (6) from (1) yields :

$$\epsilon_{k+1} = (P_i A_i - L_i C_i)\epsilon_k + P_i B_i u_k \qquad (7)$$

In order to ensure global convergence of (7) and so the IIGS, theoretical results of [7] are used. The design of the encoder/decoder setup consists of the computation of the pairs (L_i, Q_i) according to Proposition 2.

Proposition 2 *The encoder/decoder (1)-(6) are IIGS and the plaintext m_k is exactly recovered if :*

2a) $P_i B_i = 0$,

2b) $\epsilon_{k+1} = (P_i A_i - L_i C_i)\epsilon_k$ *is globally stable.*

The sketch of the proof is similar. If *2a)* is satisfied, the second term of (7) vanishes. Then, *2b)* achieves the global convergence of (7). It can also be shown that those conditions can be expressed in terms of LMI's with Q_i's and L_i's as unknowns. Again, global stability is ensured by the existence of a Poly-quadratic Lyapunov function.

3 REAL-TIME PRIVATE COMMUNICATION EXPERIMENT

3.1 Setup description

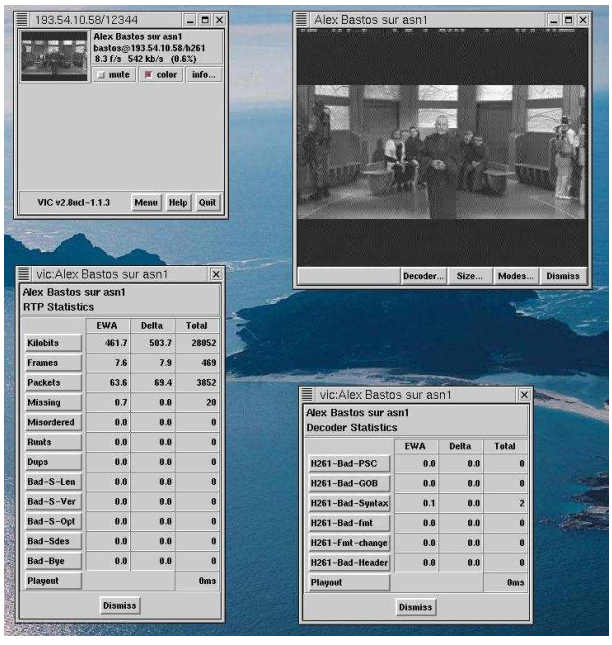

Figure 1: Decoder capture screen: matched keys

A chaotic encryption experiment is conducted within a real-time video communication context. For that purpose, a well-known GNU licensed program for video transmission over Internet, *VIC*, has been chosen. A video tape is connected to a computer through the S-Video port of a *Miro Studio PCTV Rave*^{TM} card. Consequently, the video tape data are dynamically captured by the TV-Card and *VIC* manages the transmission protocol over Internet. The card has been configured to work under *Linux* and is driven by the *bttv* and *video4linux* drivers included in the *VIC* package. *VIC*'s default package contains an implementation of DES cryptographic algorithm. However, it also allows to introduce new cryptographic schemes. We have chosen the encrypting scheme corresponding to case 4. The well-known Second order Markov Map has been considered as the chaos generator. It induces a chaotic behavior which is reckoned to get some good statistical properties for encryption purposes. Here, the key is the parameterization of the chaotic map. The design of the encoder/decoder obeys the equations (1), (3) and Proposition 1.

With the same key in both sides, the video is correctly displayed in the receiver side with a bit rate equaling 500 kB/sec which seems to be a good result. A capture screen is shown in Figure 1. Using slightly different key parameters (up to third decimal) in both sides of the communication system, the bad decrypted image depicted on Figure 2 highlights the sensitivity to key parameters.

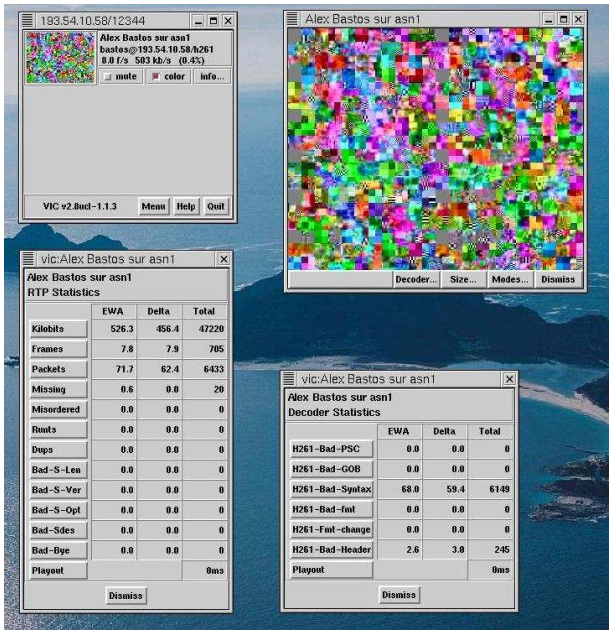

Figure 2: Decoder capture screen: mismatched keys

3.2 Robustness against linear cryptanalysis

In order to assess the level of secrecy of the encryption scheme, we resort to a linear cryptanalysis. For a detailed description of such an attack, the reader can for instance refer to [2]. However, a brief recall is given. Denote by $b[i]$ the ith bit of an l-bit long block b. For a random sample of size N of plaintexts u (binary blocks of l bits) and corresponding ciphertexts $y = e_K(u)$ (K being the key), calculate the values of the *linear approximation*

$$Z_{i_1,...,i_r,j_1,...,j_s} = u[i_1] \oplus ... \oplus u[i_r] \oplus y[j_1] \oplus ... \oplus y[j_s]$$

with $Z_{i_1,...,i_r,j_1,...,j_s} \in \{0,1\}$ for different choices of $1 \leq i_1 < ... < i_r \leq l$, $1 \leq j_1 < ... < j_s \leq l$. Let N_0 be the number of realizations $Z_{i_1,...,i_r,j_1,...,j_s} = 0$ and define the bias of the linear approximation $Z_{i_1,...,i_r,j_1,...,j_s}$ as $\left|\frac{1}{2} - \frac{N_0}{N}\right|$. For good ciphers, the bias converges to $2^{-\frac{l+2}{2}}$ as $N \to 2^l$ [20].
In spite of the fact that there exists a distinction between standard cryptography and chaotic cryptography since the former involves reals instead of integers, after few adaptations, the biases of different linear approximations have been estimated using initial segments of orbits containing 30000 iterates of u, each iterate being the encryption of the previous one. The numerical results were very promising since $|N_0/30000 - 0.5| \leq 0.01$ in all cases, though a more comprehensive analysis is still needed.

4 CONCLUDING REMARKS

Further works have to be pursued for assessing the robustness of the proposed cryptosystem against others standard attacks. However, a special point is worth noting. Indeed, piecewise linearities are likely to make more difficult the problems of identifiability, arising in plaintext encryption attacks as reported in [19][18], or the problems of observability for key stream reconstruction. And yet, identification or observation of switched systems is still a problem under study indicating that piecewise linear systems are likely to be good candidates for encryption purposes.

References

[1] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, 8(6):1259 – 1284, June 1998.

[2] Jakimoski G. and Kocarev L. Chaos and cryptography :block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 48(2):163–169, February 2001.

[3] Masuda N. and Aihara K. Cryptosystems with discretized chaotic maps. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 49(1):28–40, January 2002.

[4] Pecora L. M. and Carroll T. L. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64:821–824, 1990.

[5] Cuomo K. M., Oppenheim A. V., and Strogatz S. H. Synchronization of lorenz-based chaotic circuits with applications to communications. *IEEE Trans. Circuits. Syst. II: Anal. Digit. Sign. Process*, 40(10):626–633, 1993.

[6] Feldmann U., Hasler M., and Schwarz W. Communication by chaotic signals :the inverse system approach. *Int. J. of Circuit Theory Appl.*, 24:551–579, 1996.

[7] Millerioux G. and Daafouz J. Unknown input observers for message-embedded chaos synchronization of switched discrete-time systems. *International Journal of Bifurcation and Chaos*. (accepted for publication).

[8] Millerioux G. and Daafouz J. An observer-based approach for input independent global chaos synchronization of discrete-time switched systems. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 2003. (accepted for publication).

[9] Wu C. W. and Chua L. O. A simple way to synchronize chaotic systems with applications to secure communications systems. *International Journal of Bifurcation and Chaos*, 3(6):1619–1627, 1993.

[10] Liao T-L. and Huang N-S. An observer-based approach for chaotic synchronization with applications to secure communications. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 46(9):1144–1150, 1999.

[11] Lian K-Y., Chiang T-S, and Liu P. Discrete-time chaotic systems : applications in secure communications. *International Journal of Bifurcation and Chaos*, 10(9):2193–2206, 2000.

[12] Milanovic V. and Zaghloul M. E. Synchronization of chaotic neural networks and applications to communications. *International Journal of Bifurcation and Chaos*, 6(12):2571–2585, 1996.

[13] Inoue E. and Ushio T. Chaos communication using unknown input observers. *Electronics and communication in Japan part III: Fundamental Electronic Science*, 84(12):21–27, 2001.

[14] Yang T., Wu C. W., and Chua L. O. Cryptography based on chaotic systems. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44(5):469–472, May 1997.

[15] Short K. Steps towards unmasking secure communications. *International Journal of Bifurcation and Chaos*, 4(4):959–977, 1994.

[16] Parker A. T. and Short K. M. Reconstructing the keystream from a chaotic encryption scheme. *IEEE Trans. on Circ. and Syst.*, 48(5):624–630, May 2001.

[17] Daafouz J. and Bernussou J. Parameter dependent lyapunov functions for discrete time systems with time varying parametric uncertainties. *Systems and Control Letters*, 43:355–359, 2001.

[18] Dedieu H. and Ogorzalek M. Identifiability and identification of chaotic systems based on adaptative synchronization. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44(10):948–962, October 1997.

[19] Zhou H. and Ling X-T. Problems with the chaotic inverse system encryption approach. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44(3):268–271, March 1997.

[20] Amigó J.M. and Szczepański J. Approximations of dynamical systems and their applications to cryptography. *International Journal of Bifurcation and Chaos*, July 2003.