Tecniche per l'impiego di sistemi caotici nelle comunicazioni sicure

F.Argenti[*], *E.Del Re*[*], *R.Genesio*[**], *A.Tesi*[**]

[*] Dipartimento di Ingegneria Elettronica, Università di Firenze
[**] Dipartimento di Sistemi e Informatica, Università di Firenze
Via di Santa Marta, 3 - 50139 Firenze

Sommario

In questo lavoro viene proposto uno schema per le comunicazioni sicure. La caratteristica fondamentale di tale schema è l'utilizzazione di mappe non lineari come generatori di segnali caotici a tempo discreto per mascherare l'informazione. La sensitività dello schema rispetto a variazioni delle chiavi della sicurezza e alcuni aspetti implementativi della trasmissione del segnale sono discussi in dettaglio.

1. Introduzione

I sistemi caotici sincronizzanti [1] sono già stati proposti e studiati come generatori di sequenze di cifratura nel contesto delle comunicazioni sicure [2]-[6]. In particolare nella tecnica nota come "chaotic masking" un segnale informativo di piccola ampiezza viene sommato al segnale caotico in modo da permettere la ricezione solo da parte di un ricevitore autorizzato. Se l'informazione è binaria, allora la tecnica detta di "chaotic switching" consente di codificare i dati attraverso due diversi attrattori caotici. Nella tecnica di "chaotic modulation" l'informazione modula una portante caotica attraverso una trasformazione non lineare invertibile. Per maggiori dettagli su questi schemi si rimanda al lavoro [7].
Fatta eccezione per qualche esempio [8]-[11], la maggior parte della ricerca si è finora concentrata su sistemi analogici. Uno svantaggio di tali sistemi rispetto a quelli a tempo discreto sembra essere la non soddisfacente robustezza in presenza di variazioni dei componenti del sistema e di disturbi di canale. Per tale motivo in questo lavoro viene posta l'attenzione su schemi per le comunicazioni sicure basati su sistemi a tempo discreto. In particolare, viene proposto uno schema di comunicazione che utilizza come generatore caotico una mappa non lineare la cui uscita è modulata dal segnale informativo. Si esamina la sensitività rispetto a variazioni delle chiavi della sicurezza dello schema e si discutono alcuni problemi relativi alla trasmissione del segnale codificato.

2. Sincronizzazione del caos in sistemi a tempo discreto

In questo paragrafo viene brevemente presentata la sincronizzazione di sistemi a tempo discreto con riferimento a problemi di comunicazioni sicure. Si rimanda a [12]-[13] per maggiori dettagli.
Si consideri come esempio la mappa non lineare del secondo ordine, detta mappa di Hénon, riportata di seguito

$$\begin{aligned} x_1(k+1) &= 1 - \alpha x_1^2(k) + x_2(k) \\ x_2(k+1) &= \beta x_1(k) \end{aligned} \tag{1}$$

E` ben noto che questa mappa presenta un comportamento caotico in un'ampia regione dei parametri intorno ai valori α=1.4 e β=0.3. L'uscita di interesse del sistema caotico (1) sia costituita dalla variabile x_1, ovvero

$$y(k) = x_1(k) \tag{2}$$

Il trasmettitore è quindi definito dalle equazioni (1) e (2) e fornisce un segnale caotico di uscita y una volta che sono fissate le condizioni iniziali $x_1(0)$ e $x_2(0)$.
Si consideri un ricevitore costituito dalla mappa seguente

$$\begin{aligned} z_1(k+1) &= 1 - \alpha y^2(k) + z_2(k) \\ z_2(k+1) &= \beta y(k) \end{aligned} \tag{3}$$

dove α e β sono gli stessi dell'equazione (1).
E` evidente che l'errore di ricostruzione, ovvero $\Delta x_1 = z_1 - x_1$, $\Delta x_2 = z_2 - x_2$, soddisfa alla mappa lineare

$$\begin{aligned} \Delta x_1(k+1) &= \Delta x_2(k) \\ \Delta x_2(k+1) &= 0 \end{aligned} \tag{4}$$

Pertanto, indipendentemente dalle condizioni iniziali $z_1(0)$ e $z_2(0)$ del ricevitore, l'errore di ricostruzione va a zero in al più due passi, ovvero $\Delta x_1(k) = \Delta x_2(k) = 0$ per k maggiore o uguale a 2.
Un sistema che gode ti tale proprietà è detto "dead-beat" sincronizzante.
Per maggiori dettagli su tali sistemi si rimanda a [12].

3. Schema per le comunicazioni sicure

Una delle caratteristiche più interessanti di un sistema sincronizzante dead-beat consiste nella possibilità che lo stesso segnale caotico venga semplicemente generato, in modo deterministico, sia dal trasmettitore che dal generatore. Questo segnale caotico può venire utilizzato per mascherare l'informazione in un sistema per le comunicazioni sicure.

Sia y(k) il segnale caotico generato dal trasmettitore definito dalla mappa di Hénon (1) e dall'equazione di uscita (2), e sia s(k) il segnale informativo da trasmettere. L'idea è quella di utilizzare y(k) in modo da mascherare s(k) rendendo pertanto impossibile la corretta ricezione di s(k) da parte di un ricevitore non autorizzato. Un modo per ottenere ciò consiste nello scegliere una funzione di codifica c(s,y), continua ed invertibile, in modo che il segnale effettivamente trasmesso sia c(s,y). Ovviamente il ricevitore autorizzato deve conoscere esattamente il segnale y(k) per ricostruire l'informazione s(k). Questo è chiaramente possibile se sono noti i valori dei parametri α e β e le condizioni iniziali della mappa di Hénon o equivalentemente, secondo quando visto nel paragrafo precedente, almeno due campioni del segnale y.
Il sistema di comunicazione proposto è riportato schematicamente di seguito. Si assume che l'informazione sia suddivisa in pacchetti a lunghezza fissa pari a M, ovvero [s(nM), s(nM+1), ... s(nM+M-1)] è il pacchetto n-esimo.

1. Si impiega una mappa di Hénon con parametri α_0, β_0 e con una assegnata condizione iniziale in modo da generare una sequenza caotica $y_0(k)$ composta da 2N campioni, dove N è il numero di pacchetti da trasmettere.
2. Si usano i campioni $y_0(2n-1,2n)$, n = 1,...,N per inizializzare una seconda mappa di Hénon con parametri α e β. Ogni volta essa genera una sequenza $y_n(k)$ costituita da M campioni.
3. Si trasmette il blocco n-esimo del segnale mascherato dalla sequenza $y_n(k)$, ovvero si trasmettono i dati seguenti:

$$[c(s(nM),y_n(1)), \ldots\ldots , c(s(nM+M-1),y_n(M))] \qquad (5)$$

In questo schema la chiave risiede nei parametri α_0, β_0, α e β.
Un vantaggio di tale schema è il fatto di essere senza memoria, caratteristica che garantisce la non propagazione ad altri campioni della sequenza di un errore su un singolo campione, per esempio dovuto al rumore sul canale.

Si descrive ora un esempio di comunicazione sicura. Sia il trasmettitore definito da una mappa di Hénon con parametri α=1.4 e β=0.3, mentre una seconda mappa di Hénon, ancora con parametri α_0=1.4 e β_0=0.3, è usata per inizializzarne lo stato. Scelta la funzione di codifica c(s,y)=y/s, l'informazione è stata suddivisa in pacchetti di M=128 campioni. L'onda quadra mostrata in Fig. 1 è stata usata come segnale informativo *s*, mentre il segnale mascherato, cioè quello effettivamente trasmesso, è riportato in Fig. 2.
Il ricevitore autorizzato ricostruisce il segnale perfettamente, mentre il segnale individuato da un ricevitore non autorizzato è mostrato in Fig. 3 (soltanto il parametro β è stato modificato, con una differenza di 0.0001 rispetto al valore corretto β=0.3). Cambiamenti delle stesse dimensioni nelle altre chiavi conducono a risultati equivalenti. E` pertanto evidente che una piccola differenza nei parametri determina la ricostruzione di un segnale simile al rumore, come attesa conseguenza diretta delle elevata sensitività della dinamica caotica. Nel paragrafo seguente sono discusse in dettaglio la scelta della funzione di modulazione e la sua influenza sulle prestazioni dello schema di comunicazione proposto.

4. Aspetti relativi alla comunicazione del segnale codificato

In questo paragrafo verranno trattati alcuni problemi relativi alla trasmissione del segnale codificato.
In un sistema di trasmissione numerico l'informazione da trasmettere è codificata mediante simboli binari. Supponendo che il segnale di ingresso sia di tipo PCM con b bit/campione si consideri lo schema di mascheramento descritto nel paragrafo precedente. In [12] vengono indicate funzioni modulanti $c(s,y)$, e quindi segnali trasmessi, di tipo reale. Per una trasmissione di tipo numerico, è dunque necessaria una quantizzazione dei campioni codificati: ciò introduce una distorsione anche nel segnale decodificato da parte dell'utente autorizzato.
Per evitare tale problema si può introdurre una funzione modulante $c(s,y)$ di tipo invertibile e a valori discreti, con argomenti anch'essi a valori discreti. Per esempio si può scegliere $c(s,y) = XOR(s,y)$, dove la funzione XOR è calcolata sulla rappresentazione binaria degli operandi. Tale scelta implica che anche il segnale y usato per il mascheramento deve essere rappresentato, come il segnale informativo s, a b bit. Ciò è ottenuto quantizzando y a 2^b livelli, scelti tra il valore massimo e minimo di y. In questo modo, l'utente autorizzato può ricostruire in modo perfetto la sequenza di mascheramento eseguendo il processo di quantizzazione nello stesso modo di come esso è effettuato in trasmissione. In questo caso la funzione inversa è $c^{-1}(x,y)=XOR(x,y)$.
Un altro esempio di funzione invertibile è $c(s,y) = XOR(RR(s,y))$, dove $RR(a)$ è l'operatore di rotazione a destra operante sulla stringa di bit che rappresenta a, con il LSB che diventa il MSB (tale operatore è stato utilizzato anche in [10]). In questo caso $c^{-1}(x,y)=LR(XOR(x,y))$, dove $LR(\ )$ è l'operatore di rotazione a sinistra.
Per valutare l'efficienza dell'algoritmo di mascheramento, sono state effettuate alcune prove utilizzando un segnale vocale campionato ad una frequenza di campionamento $f_C=11.025$ KHz, con 8 bit/campione. Siano SNR_a e SNR_u il rapporto segnale-rumore misurato, rispettivamente, dall'utente autorizzato e da quello non autorizzato. Per quest'ultimo si è supposta la conoscenza di tutte le chiavi con l'esclusione della chiave β_0, per la quale si è fissata una variazione di $\Delta\beta_0 = 0.001$ (risultati simili sono stati ottenuti cambiando le altre chiavi). I rapporti tra potenza di segnale e di rumore sono calcolati come $SNR = 10\ log_{10}\ (\sigma_s^2 /MSE)$, dove σ_s è la deviazione standard del segnale di ingresso (nelle prove effettuate $\sigma_s = 43.10$), mentre $MSE = E[(s-s_d)^2]$ è l'errore quadratico medio tra il segnale originale e il segnale decodificato σ_d. Per fare un paragone, se σ_d fosse una variabile aleatoria con distribuzione uniforme nell'intervallo $(-2^{b-1}, 2^{b-1}-1)$, con $b=8$, e non correlata con il segnale di ingresso, si avrebbe $SNR = -5.96\ dB$. Utilizzando come funzioni modulanti XOR e RR-XOR si sono invece ottenuti, rispettivamente, valori di SNR_u uguali a -5.56 e -5.80, che indicano come il livello di mascheramento sia notevole. Prove di ascolto hanno confermato questa indicazione. L'utente autorizzato, invece, recupera in modo perfetto il segnale informativo.
In Figura 4 e 5 sono mostrate, rispettivamente, le funzioni di mutua covarianza tra segnale originale e segnale dopo il mascheramento (sono state usate diverse funzioni modulanti) e tra segnale originale e segnale decodificato da un utente non autorizzato (con la variazione della chiave descritta in precedenza). Dalle figure si nota che la prima funzione riportata dipende in modo abbastanza evidente dalla funzione modulante. A tale correlazione non trascurabile corrisponde una certa intelligibilità del segnale codificato, come verificato in test di ascolto, se si usa la moltiplicazione e la divisione come funzione modulante. In Figura 6, invece, è

mostrato il valore di SNR_u in funzione delle variazioni delle chiavi α e β (α_0 e β_0 sono supposte note) rispetto al valore usato in trasmissione. Come si può vedere la sensitività è elevata, e ciò implica un'alta risoluzione nello spazio delle chiavi e dunque una buona sicurezza.
La codifica PCM rappresenta il sistema di codifica binaria più semplice, anche se non efficiente da un punto di vista di capacità richiesta. Molti sistemi di compressione per segnali vocali, audio e video sono stati peraltro studiati e standardizzati [14]. Per valutare l'efficienza dell'algoritmo di mascheramento su un segnale compresso, è stato scelto il semplice metodo del DPCM di ordine zero, in cui ogni campione è predetto utilizzando il campione precedente. Solo la differenza tra campione attuale e predizione viene quantizzata e trasmessa. Il "bit rate" considerato è stato di 4 bit/campione. In questo caso anche l'utente autorizzato misura una certa distorsione, dovuta all'algoritmo di compressione, uguale a $SNR_a = 13.84$. La qualità del segnale ricostruito è comunque molto elevata. I valori di SNR_u per l'utente non autorizzato (si è scelta la stessa variazione della chiave mostrata per il caso PCM) sono di *-4.90* e *-5.12* per le funzioni, rispettivamente, *XOR* e *RR-XOR*.
Nelle Figure 7 e 8 sono mostrate, riferite al caso DPCM, le stesse funzioni riportate nelle Figure 4 e 5 per il caso PCM, mentre in Figura 9 viene mostrata la sensitività rispetto al variare delle chiavi.
Per valutare la semplicità del metodo e verificare un suo possibile utilizzo in applicazioni in tempo reale l'algoritmo di mascheramento è stato implementato su un "Digital Signal Processor" (DSP) ADSP 21020, a virgola mobile. Il test ha dimostrato che è effettivamente possibile realizzare lo schema visto nelle sezioni precedenti. Inoltre, le prove di ascolto hanno indicato un completo mascheramento del segnale di ingresso qualora si vari anche solo il LSB della mantissa di uno qualsiasi dei parametri della mappe di Hénon utilizzate: la sicurezza dello schema si conferma quindi assai elevata.

Bibliografia

[1] L.M. Pecora and T.L. Carroll, "Synchronization in chaotic systems", *Physical Review Letters*, Vol.64, pp. 821-824, 1990.
[2] Lj. Kocarev, K.S. Halle, K. Eckert, L.O. Chua and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization ", *Int. J. of Bifurcation and Chaos*, Vol. 2, pp. 709-713, 1992.
[3] H. Dedieu, M.P. Kennedy and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits ", *IEEE Trans. on Circuits and Systems (Part II)*, Vol. 40, pp. 634-642, 1993.
[4] C.W. Wu and L.O. Chua, "A simple way to synchronize chaotic systems with application to secure communication systems ", *Int. J. of Bifurcation and Chaos*, Vol. 3, pp. 1619-1627, 1993.
[5] K.S. Halle, C.W. Wu, M. Itoh and L.O. Chua, "Spread-spectrum communications through modulation of chaos ", *Int. J. of Bifurcation and Chaos*, Vol. 3, pp. 469-477, 1993.
[6] K.M. Cuomo and A.V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications ", *Physical Review Letters*, Vol. 71, pp. 65-68, 1993.
[7] M.J. Ogorzalek, "Timing chaos: Part I - Synchronization ", *IEEE Trans. on Circuits and Systems (Part I)*, Vol. 40, pp. 693-699, 1993.