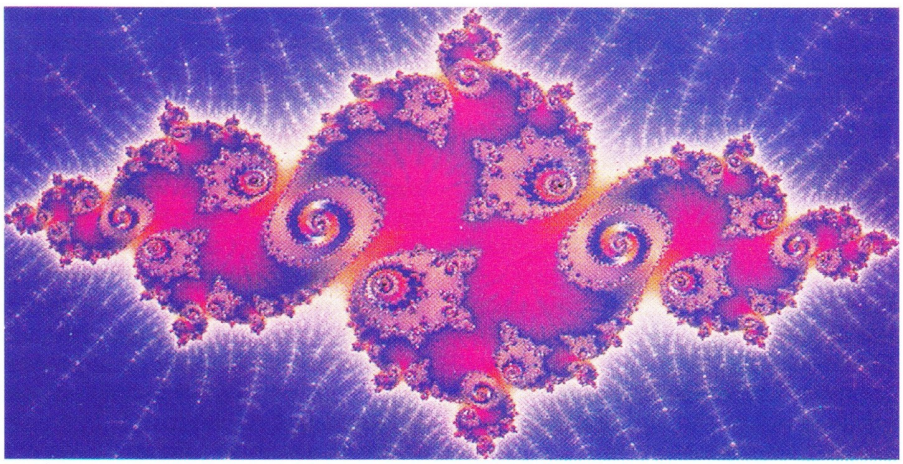
Comunicazioni sicure basate su sistemi caotici

di Fabrizio Argenti, Enrico Del Re, Roberto Genesio e Alberto Tesi

In questo articolo 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. In particolare si discutono la sensitività dello schema rispetto a variazioni delle chiavi della sicurezza e alcuni aspetti implementativi della trasmissione del segnale.



I sistemi caotici sincronizzanti [1] sono già stati proposti e studiati come generatori di sequenze di cifratura nel contesto delle comunicazioni sicure [2]-[6]. 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 sull'uso di 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 si considerano schemi per le comunicazioni sicure basati su sistemi a tempo discreto, per i quali si mette in evidenza la specifica possibilità di realizzare la sincronizzazione in un numero finito di passi. Viene quindi 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.

Ing. Fabrizio Argenti, prof. Enrico Del Re, Dipartimento di Ingegneria Elettronica, Università di Firenze; prof. Roberto Genesio, prof. Alberto Tesi, Dipartimento di Sistemi e Informatica, Università di Firenze.

Sincronizzazione del caos in sistemi a tempo discreto

Viene qui brevemente presentato il problema della 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:

$$x_1(k+1) = 1 - \alpha x_1^2(k) + x_2(k)$$
$$x_2(k+1) = \beta x_1(k) \qquad (1)$$

In Figura 1 è mostrato il tipo di comportamento del sistema al variare dei parametri α e β. È ben noto che questa mappa presenta un comportamento caotico in un'ampia regione dei parametri intorno ai valori $\alpha = 1{,}4$ e $\beta = 0{,}3$ [14]. L'uscita di interesse del sistema caotico (1) sia costituita dalla variabile x_1, ovvero

$$y(k) = x_1(k) \qquad (2)$$

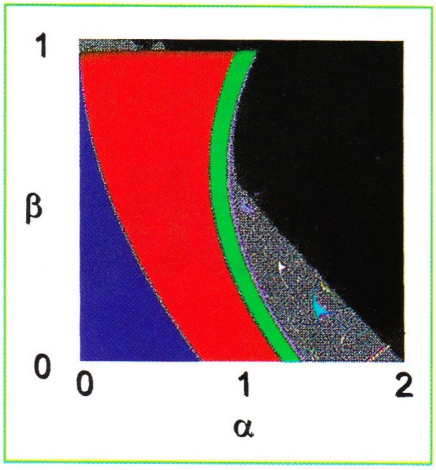


Figura 1 - Insiemi limite della mappa di Hénon al variare dei parametri: per punti (α, β) appartenenti alla zona blu lo stato del sistema tende ad un punto di equilibrio; nella zona grigia si ha un comportamento caotico, nella zona nera il sistema è instabile; altrove si ha un comportamento periodico

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

$$z_1(k+1) = 1 - \alpha y^2(k) + z_2(k)$$
$$z_2(k+1) = \beta y(k) \qquad (3)$$

dove i parametri α e β sono gli stessi dell'equazione (1).
È evidente che l'errore di ricostruzione, ovvero $\Delta x_1 = z_1 - x_1$, $\Delta x_2 = z_2 - x_2$, soddisfa le equazioni della mappa lineare

$$\Delta x_1(k+1) = \Delta x_2(k)$$
$$\Delta x_2(k+1) = 0 \qquad (4)$$

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

Schema per le comunicazioni sicure

Una delle caratteristiche più interessanti di un sistema "dead-beat" sincronizzante consiste nella possibilità che lo stesso segnale caotico venga semplicemente generato, in modo deterministico, sia dal trasmettitore che dal ricevitore. 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, tale che il segnale effettivamente trasmesso sia c(s,y). Ovviamente il ricevitore autorizzato deve conoscere esattamente il segnale caotico 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 precedentemente, 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:

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

In questo schema la chiave risiede nei parametri α_0, β_0, α e β. Lo schema trasmissivo con modulazione caotica è mostrato in Figura 2.
Un vantaggio di tale schema è il fatto di essere senza memoria, caratteristica che garantisce la non propagazione di errori, dovuti per esempio al rumore sul canale, ad altri campioni della sequenza. 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. Sia c(s,y) = y/s la funzione di codifica e si supponga che il segnale informativo s sia suddiviso in pacchetti di 128 campioni. Usando come segnale informativo s l'onda quadra mostrata in Figura 3 si ottiene il segnale mascherato, cioè quello effettivamente trasmesso, riportato in Figura 4. Il ricevitore autorizzato ricostruisce il segnale perfettamente, mentre il segnale decodicato da un ricevitore non autorizzato, il quale non è a conoscenza degli esatti valori α_0, β_0, α e β usati in trasmissione, è mostrato in Figura 5: tale segnale è stato ottenuto variando soltanto il parametro β di 0,0001 rispetto al valore corretto β = 0,3. Cambia-

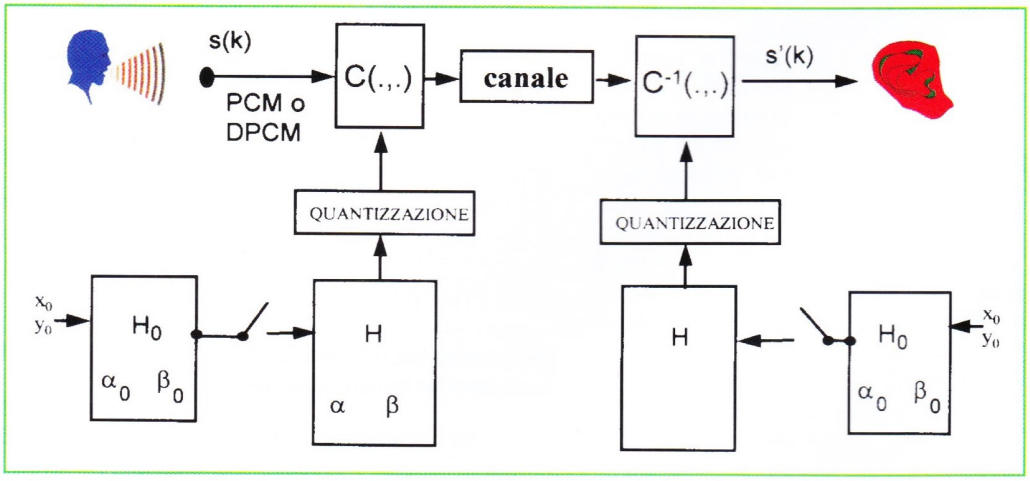


Figura 2 - Schema trasmissivo con modulazione caotica

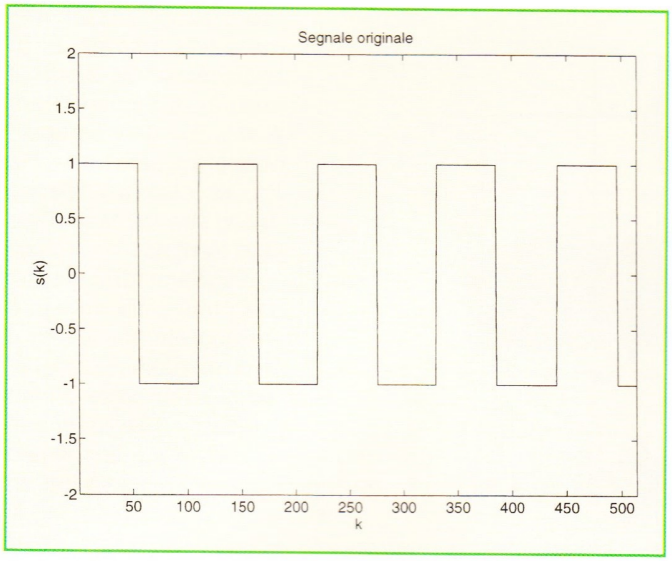


Figura 3 - Esempio di segnale informativo ad onda quadra

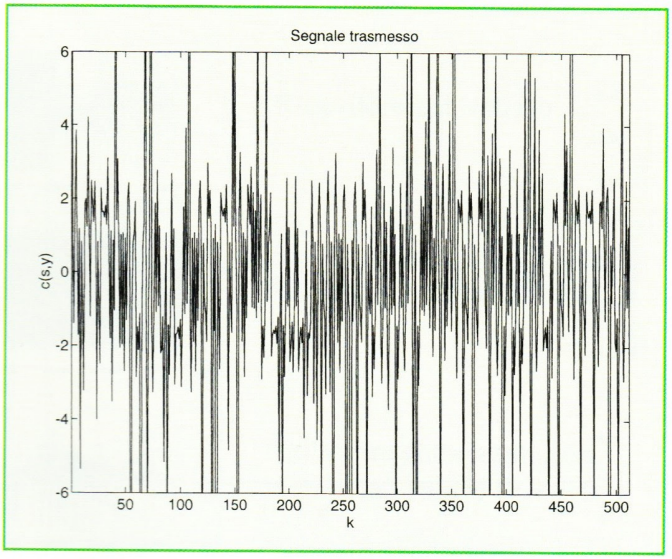


Figura 4 - Segnale dopo il mascheramento

menti delle stesse dimensioni nelle altre chiavi conducono a risultati equivalenti. È pertanto evidente che una piccola differenza nei parametri determina una ricostruzione del segnale simile a rumore, come attesa conseguenza diretta della elevata sensitività della dinamica caotica. Nella successiva parte dell'articolo sono discusse in dettaglio la scelta della funzione di modulazione e la sua influenza sulle prestazioni dello schema di comunicazione proposto.

Aspetti relativi alla comunicazione del segnale codificato

Vengono trattati qui 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 nella parte 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 e 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 ed una rappresentazione con livelli interi tra -2^{b-1} e $2^{b-1}-1$. Sia s_d il segnale ricevuto e decodificato: nel caso la decodifica sia effettuata dall'utente autorizzato il segnale risulterà identico a quello trasmesso, mentre l'utente non autorizzato dovrà ottenere un segnale completamente non intelligibile.

Sia MSE = $E[(s-s_d)^2]$ la potenza dell'errore tra segnale originale e segnale decodificato e sia SNR = $10 \log_{10} (\sigma_s^2/MSE)$ il rapporto tra la potenza del segnale s (σ_s^2) e quella dell'errore (nel nostro esempio σ_s = 43,10); siano SNR_a e SNR_n i valori di SNR misurati, rispettivamente, dall'utente autorizzato e da quello non autorizzato. Si è supposto che l'utente non autorizzato fosse a conoscenza di tutte le chiavi con l'esclusione del solo parametro β, per il quale si è fissata una variazione di $\Delta\beta$ = 0,0001 (risultati simili sono stati ottenuti

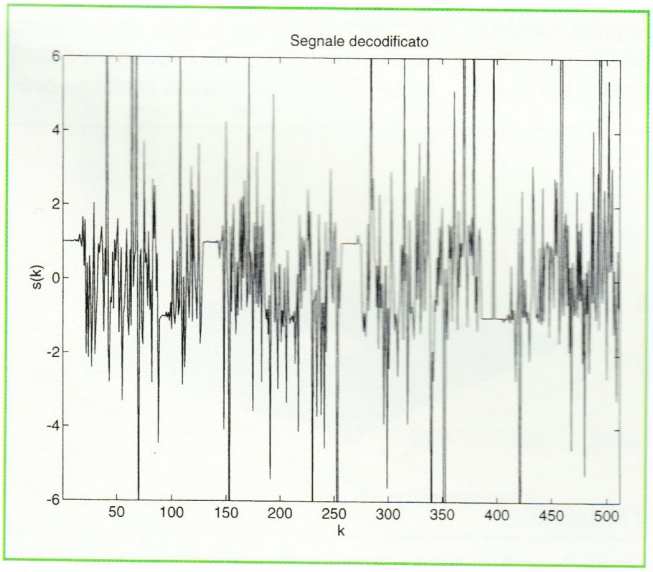


Figura 5 - Segnale decodificato da un utente non autorizzato con variazione della chiave $\Delta\beta$ = 0,0001

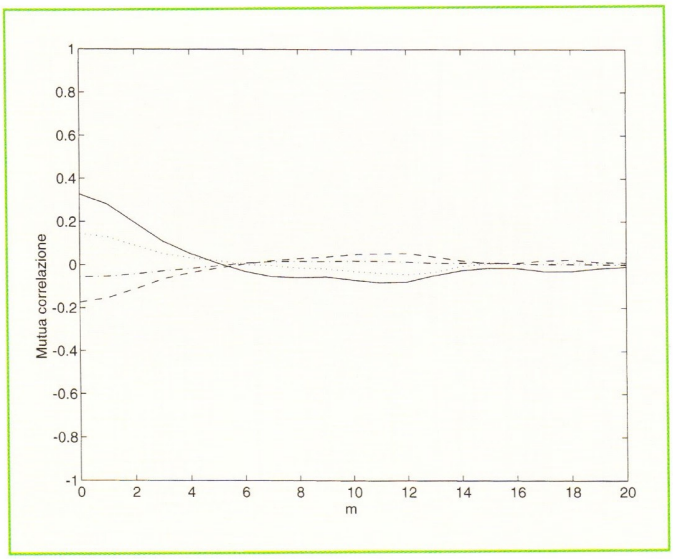


Figura 6 - Funzione di mutua correlazione tra il segnale informativo di tipo vocale (PCM, 8 bit/campione) e il segnale dopo il mascheramento, al variare della funzione di modulazione c(s,y): moltiplicazione (linea continua), divisione (linea a punti), XOR (linea a tratti), XOR-RR (linea tratto-punto)

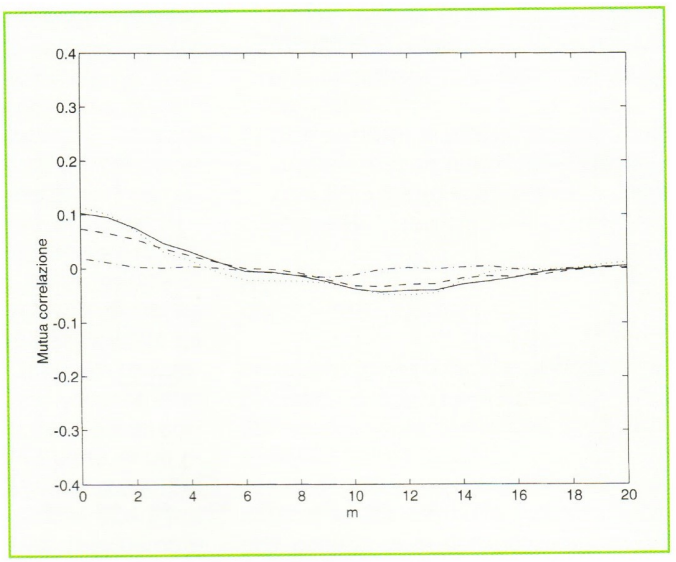


Figura 7 - Funzione di mutua correlazione tra il segnale informativo di tipo vocale PCM e il segnale decodificato da un utente non autorizzato, al variare della funzione di modulazione c(s,y) (vedi didascalia Figura 6 per la corrispondenza funzione-linea)

cambiando le altre chiavi). Utilizzando come funzioni modulanti XOR e RR-XOR si sono ottenuti, rispettivamente, valori di SNR_n uguali a -5,56 e -5,80. Per fare un paragone, se s_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_n = -5,96 dB: ciò indica come il livello di mascheramento ottenuto sia notevole.

Tale fatto è stato confermato anche da prove di ascolto effettuate sul segnale decodificato. L'utente autorizzato, invece, recupera in modo perfetto il segnale informativo ($SNR_a = \infty$).

Sia $C_{xy}(m) = E[x(n)y(n+m)]/(\sigma_x \sigma_y)$ la funzione di mutua correlazione normalizzata di due generici segnali x(n) e y(n). In Figura 6 e 7 sono mostrate, rispettivamente, le funzioni di mutua correlazione 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). Dalla Figura 6 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 8, invece, è mostrato il valore di SNR_n 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 di canale richiesta. Molti sistemi di compressione per segnali vocali, audio e video sono stati peraltro studiati e standardizzati [15]. 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_n per l'utente non autorizzato (si è scelta la stessa variazione della chiave indicata per il caso PCM) sono di -4,90 e -5,12 per le funzioni, rispettivamente, XOR e RR-XOR. Risultati del tutto analoghi a quelli mostrati nelle Figure 6-8 per il caso PCM sono stati ottenuti anche per il caso DPCM e, di conseguenza, non vengono qui riportati.

Implementazione mediante DSP del sistema di comunicazione

Per valutare la semplicità del metodo e verificare un suo possibile utilizzo in applicazioni in tempo reale l'algoritmo di mascheramento è stato implemetato su un Digital Signal Processor (DSP) ADSP 21020, a virgola mobile, pro-

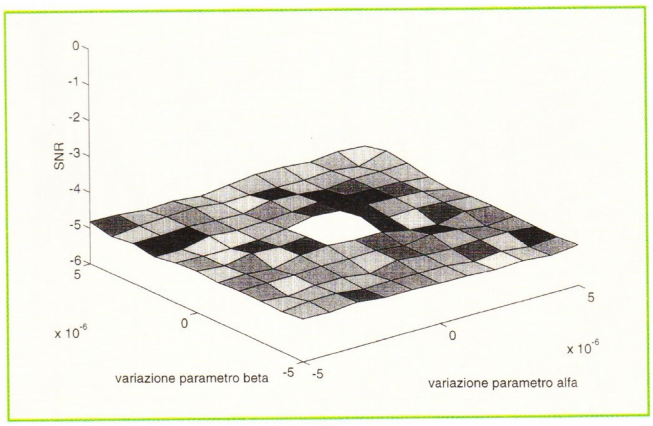


Figura 8 - SNR misurato da un utente non autorizzato in funzione della variazione delle chiavi α e β (segnale compresso con PCM a 8 bit/campione)

grammabile da calcolatore. Il segnale viene acquisito a 16 bit/campione e con frequenza di campionamento f_c = 8 kHz. Il segnale elaborato può essere ascoltato da una porta della scheda che ricostruisce il segnale digitale in forma analogica.
Il test ha dimostrato che è effettivamente possibile una realizzazione in tempo reale dello schema visto nelle sezioni precedenti. La dimensione dei pacchetti usata è di 512 campioni. L'implementazione su DSP ha messo in luce, in particolare, che la sensitività del sistema, mostrata nelle simulazioni, rimane elevata anche nella realizzazione effettiva. È stato rilevato che una variazione di circa $5x10^{-8}$ (corrispondente alla variazione del solo LSB della mantissa della rappresentazione in virgola mobile) su uno dei parametri delle due mappe utilizzate produce un segnale decodificato completamente non riconoscibile. Poiché nella presente trattazione si sono considerati come chiave i quattro parametri delle due mappe di Hénon, una tale risoluzione nei parametri fornirebbe, se si utilizzasse un intervallo di ampiezza 0,2 centrato nei valori nominali delle chiavi, uno spazio delle chiavi formato da circa 10^{26} elementi. Inoltre, i risultati ottenuti mediante realizzazione con DSP del sistema proposto hanno mostrato concordanza con quelli delle simulazioni sia per quanto riguarda gli schemi PCM (sia a 16 che a 8 bit/campione), sia per quelli DPCM (4 bit/campione).
Alcune prove sono state effettuate anche per verificare la robustezza del sistema di comunicazione sicura in presenza di errori introdotti dal canale. Poiché lo schema è senza memoria, gli errori su un campione non si propagano su quelli adiacenti: sperimentalmente, si è verificato che un segnale vocale mascherato, corrotto da rumore con probabilità di errore sul bit di 10^{-2} e decodificato dall'utente autorizzato presenta una degradazione analoga a quella che si ottiene in assenza di mascheramento caotico, cioè, in questo schema, tale operazione è trasparente per quanto riguarda il rumore introdotto dal canale.
In Figura 9 viene mostrato il segnale decodificato da un ricevitore autorizzato, da uno non autorizzato e da uno autorizzato nel caso in cui il canale introduca rumore con probabilità di errore $P_e = 10^{-2}$. I segnali sono stati ottenuti codificando, mediante la realizzazione su DSP e utilizzando il PCM a 16 bit, la parola "UNO": in assenza di rumore sul canale l'utente autorizzato decodifica in modo perfetto il segnale trasmesso. In Figura 10 viene mostrato il confronto tra i vari segnali nel dominio della frequenza.
Come si vede il ricevitore non autorizzato decodifica un segnale che in pratica è un rumore bianco. Nel caso in cui il canale introduca errori, al segnale originale si somma un rumore con spettro bianco.

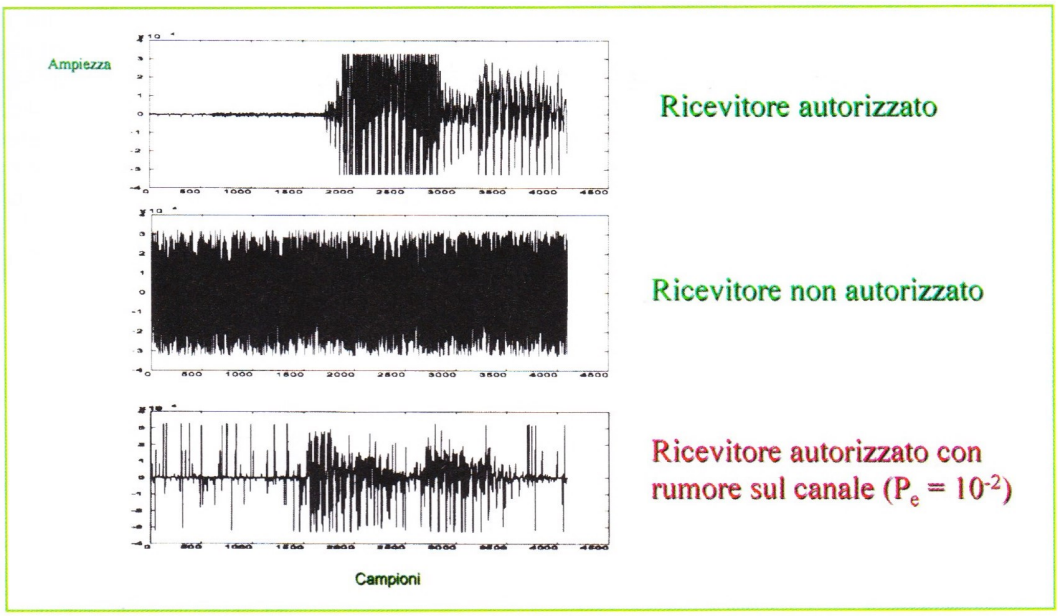


Figura 9 - Confronto tra i segnali decodificati da un ricevitore autorizzato (con e senza rumore sul canale) e da uno non autorizzato.

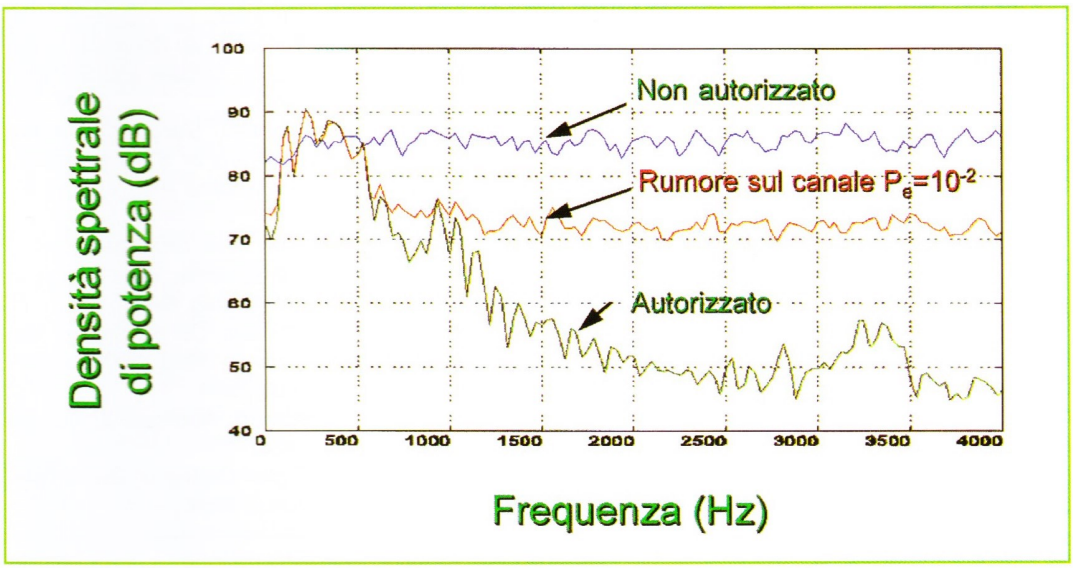


Figura 10 - Confronto nel dominio della frequenza tra i segnali decodificati da un ricevitore autorizzato (con e senza rumore sul canale) e da uno non autorizzato.

Conclusioni

In questo articolo è stato proposto un metodo per proteggere il conte-

nuto informativo di una comunicazione da possibili utenti non autorizzati. Il metodo si basa sull'impiego di sistemi dinamici non lineari che producono una uscita con comportamento caotico utilizzata per mascherare il segnale informativo. Il sistema si è dimostrato semplice, di facile implementazione hardware, con elevata dimensione dello spazio delle chiavi (cioè di possibili utenti che possono accedere al sistema) e, soprattutto, robusto rispetto agli attacchi di utenti non autorizzati. ▲

Bibliografia

[1] L. M. Pecora, T.L. Carroll, *Synchronization in Chaotic Systems,* Physical Review Letters, vol.64, pag. 821-824, 1990.
[2] Lj. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, U. Parlitz, *Experimental Demonstration of Secure Communications via Chaotic Synchronization,* Int. J. of Bifurcation and Chaos, vol. 2, pag. 709-713, 1992.
[3] H. Dedieu, M.P. Kennedy, 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, pag. 634-642, 1993.
[4] C.W. Wu, L.O. Chua, *A simple Way to Synchronize Chaotic Systems with Application to Secure Communication Systems,* Int. J. of Bifurcation and Chaos, vol. 3, pag. 1.619-1627, 1993.
[5] K.S. Halle, C.W. Wu, M. Itoh, L.O. Chua, *Spread-Spectrum Communications Through Modulation of Chaos,* Int. J. of Bifurcation and Chaos, vol. 3, pag. 469-477, 1993.
[6] K.M. Cuomo, A.V. Oppenheim, *Circuit Implementation of Synchronized Chaos with Applications to Communications,* Physical Review Letters, vol. 71, pag. 65-68, 1993.
[7] M.J. Ogorzalek, *Timing Chaos: Part I - Synchronization,* Ieee Trans. on Circuits and Systems (Part I), vol. 40, pag. 693-699, 1993.
[8] M.d.S. Vieira, P. Khoury, A.J. Lichtenberg, M.A. Lieberman, W. Wonchoba, J. Gullicksen, J.Y. Huang, R. Sherman, M. Steinberg, *Numerical and Experimental Studies of Self-Synchronization and Synchronized Chaos,* Int. J. of Bifurcation and Chaos, vol. 2, pag.645-657, 1992.
[9] M.d.S. Vieira, *Proc. of First Experimental Chaos Conference,* World Scientific, Singapore, 1992.
[10] D.R. Frey, *Chaotic Digital Encoding: an Approach to Secure Communication,* Ieee Trans. on Circuits and Systems (Part II), vol. 40, pag. 660-666, 1993.
[11] H.D.J. Abarbanel, P.S. Lindsay, *Secure Communications and Unstable Periodic Orbits of Strange Attractors,* Ieee Trans. on Circuits and Systems (Part II), vol. 40, pag.643-645, 1993.
[12] A. De Angeli, R. Genesio, A. Tesi, *Dead-beat Chaos Synchronization in Discrete-time Systems,* Ieee Trans. on Circuits and Systems - (Part I), vol. 42, pag. 54-56, 1995.
[13] A. Tesi, A. De Angeli, R. Genesio, *On the System De-Composition for Synchronizing chaos,* Int J. of Bifurcation and Chaos, vol. 4, pag. 1.675-1.685, 1994.
[14] J.M.T. Thompson, H.B. Stewart, *Nonlinear Dynamics and Chaos,* Wiley, Chichester, 1986.
[15] N.S. Jayant and P. Noll, *Digital Coding of Waveforms,* Prentice Hall, Englewood Cliffs (Usa), 1984.

Ringraziamenti: Gli autori desiderano rivolgere un ringraziamento all'ingegner Simone Nenti per avere sviluppato parte del software utilizzato per ottenere alcuni dei risultati mostrati in questo articolo.