

ДВОЙНО ХАОТИЧНО ПРЕВКЛЮЧВАНЕ, БАЗИРАНО НА ХИБРИДНА СИНХРОНИЗАЦИОННА СХЕМА МЕЖДУ ДВЕ ИДЕНТИЧНИ ХАОТИЧНИ СИСТЕМИ

Христина Стойчева

*Технически университет - Габрово, ул. „Хаджи Димитър“ № 4, Габрово, България,
Кореспондиращ автор: hsstoycheva@tugab.bg*

DOUBLE CHAOTIC SWITCHING BASED ON HYBRID SYNCHRONIZATION SCHEME BETWEEN TWO IDENTICAL CHAOTIC SYSTEMS

Hristina Stoycheva

*Technical University of Gabrovo, 4 Str. "Hadji Dimitar", Gabrovo, Bulgaria,
* Corresponding author: hsstoycheva@tugab.bg*

Abstract

In this article, a secure communication system with double chaotic switching has been applied to a digital information signal. The suggested security approach was implemented by switching between two non-identical third order chaotic systems. For practical application purposes, this system was tested with additive white gaussian noise (AWGN) channel. The recovery of the information signal at the receiver is achieved by a hybrid synchronization scheme between two novel identical third-order chaotic systems. The controls are synthesized based on Lyapunov's second stability law. The results obtained by theoretical and graphical analysis are in excellent agreement.

Keywords: chaos, chaos synchronization, chaotic switching, secure communication.

ВЪВЕДЕНИЕ

С течение на времето, въпреки мащабното развитие на комуникационните технологии, една област остава обект на непрекъснат научен интерес, а именно защитеното предаване на информацията. Съществуват различни подходи и методи за шифриране на информационни сигнали, които намират широко приложение в следните области на изследване: оторизиран достъп [1], защита на чувствителна информация в облачно пространство [2], LORA модулация [3], хаотично аудио криптиране [4] и др.

Един от фундаменталните способности за шифриране на информационни сигнали, е превключването. Подходът е базов, но в комбинация със сложната динамика на една хаотична система, се наблюдава не

само високо ниво на защита, но и лесна реализация.

Хаосът намира приложение в множество научни области, като икономика [5], физика [6], химия [7], екология [8], но най-разпространената сред тях остава областта на защитените комуникации [9, 10, 11, 12, 13, 14].

В настоящия доклад е предложен подход за реализиране на защитено предаване на цифров информационен сигнал, посредством хаотично превключване между две неидентични хаотични системи. В приемника се реализира хибридна синхронизационна схема, на база на която след приключване на преходните процеси и установяване в режим на синхронизация, информационният сигнал бива възстановен.

ИЗЛОЖЕНИЕ

Концепцията за защитено предаване на цифрови информационни сигнали посредством хаотично превключване е добре известна и широко разпространена. Най-общо тя се изразява в превключване между два хаотични сигнала в съответствие със стойностите на цифровия информационен сигнал.

В съществена част от публикациите по темата се засяга превключване между две стойности на даден параметър на една хаотична система [15,16], което води до промяна на хаотичния сигнал и съответно до относително добро ниво на защита. Друг разпространен метод е превключването между два от векторите на състоянието на една и съща хаотична система [17,18]. Методът е ефективен и при него се наблюдава по-високо ниво на защита на предаваната информация, породено от различното изменение на сигналите във функция на времето. И двата широко разпространени способа за хаотично превключване обаче споделят един и същ недостатък, а именно използването на една хаотична система.

Представяният в настоящият доклад статия подход за защитено предаване на цифров информационен сигнал чрез хаотично превключване използва две неидентични хаотични системи.

Описание на избраните хаотични системи

Избрани са две различни хаотични системи. Първата е системата на Lorenz [19] - известен математичен модел от трети ред, описван със следните уравнения:

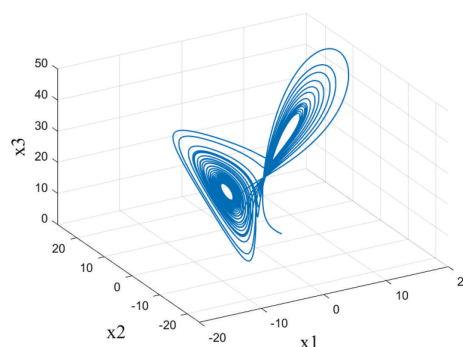
$$\begin{cases} \dot{x}_1 = -\sigma x_1 + \sigma x_2 \\ \dot{x}_2 = -x_1 x_3 + r x_1 - x_2 \\ \dot{x}_3 = x_1 x_2 - b x_3 \end{cases} \quad (1)$$

Оптималните стойности на параметрите, за които в системата възникват хаотични колебания са $\sigma = 10$, $b = \frac{8}{3}$ и $r > 25$.

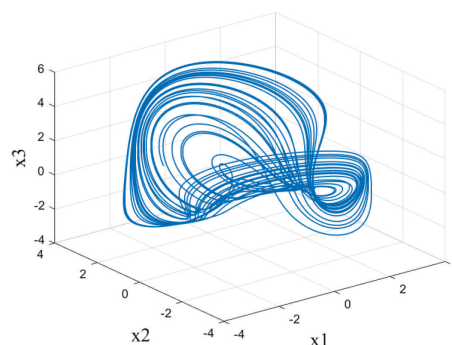
Втората система [20] е нов абстрактен математичен модел от трети ред с тригонометрична нелинейност, описан от Ramar през 2023г.:

$$\begin{cases} \dot{x}_1 = ax_1 - kx_2x_3 \\ \dot{x}_2 = b\sin x_1 + x_1x_3 \\ \dot{x}_3 = gx_1x_2 - cx_3 + d \end{cases} \quad (2)$$

Стойностите на параметрите са както следва: $a = 1.5$, $b = 10$, $c = 4$, $d = 2$, $g = 4$ и $k = 2$.



Фиг. 1. Хаотичен атрактор на система на Lorenz



Фиг. 2. Хаотичен атрактор на система на Ramar

И двете системи са симулирани с произволни начални условия, като атракторите им са представени на фиг. 1 и фиг. 2.

Хибридна синхронизационна схема

При задачите за синхронизация на хаотични системи най-често се синтезира синхронизационна схема между две еднотипни, непрекъснати системи с еднопосочна връзка между тях. Следният обобщен запис представя синхронизационната схема:

$$\begin{aligned} \text{Master: } & \dot{\mathbf{x}} = f(\mathbf{x}) \\ \text{Slave: } & \dot{\tilde{\mathbf{x}}} = f(\tilde{\mathbf{x}}) + u(\mathbf{x}, \tilde{\mathbf{x}}), \end{aligned} \quad (3)$$

където $\dot{\mathbf{x}}, \dot{\tilde{\mathbf{x}}} \in \mathbb{R}^n$ са векторите на състоянието на системата, $f(\mathbf{x})$ е нелинейна функция, а $u(\mathbf{x}, \tilde{\mathbf{x}})$ е управляващ сигнал към подчинената система. Началните условия на системите са различни, т.е. $\mathbf{x}(0) \neq \tilde{\mathbf{x}}(0)$.

За да е възможна синхронизацията между две хаотични системи, е необходимо да се синтезира подходящо управление между тях. Най-надеждният метод за постигане на такъв контрол се основава на втория метод за устойчивост на Ляпунов [21]. В обобщение, този метод изисква избор на такава функция $V(\mathbf{e})$, която отговаря на следните условия:

$$V(\mathbf{e}) > 0, \quad \forall \mathbf{e} \neq 0, \quad (4)$$

$$V(\mathbf{e}) = 0, \quad \mathbf{e} = 0, \quad (5)$$

$$\frac{dV(\mathbf{e})}{dt} < 0, \quad \forall \mathbf{e} \neq 0. \quad (6)$$

Удовлетворяването на първите две условия е лесно постижимо чрез използване на квадратична функция на отделните компоненти на вектора на грешката $\mathbf{e}$. Удовлетворяването на третото условие обаче изисква синтез на подходящо управление, в зависимост както от вида и характера на синхронизираните системи, така и от типа на избраната синхронизация.

При хибридна синхронизация между системите се търси такова управление $u(\mathbf{x}, \tilde{\mathbf{x}})$, че да бъде изпълнено условието

$$\lim_{t \rightarrow \infty} \mathbf{e}(t) = 0, \quad (7)$$

където функцията на разсъгласуване между системите има следния вид

$$\mathbf{e}(t) = \mathbf{x}(t) \pm \tilde{\mathbf{x}}(t). \quad (8)$$

Изборът кои функции $e_i(t)$ да са суми и кои разлики от съответните променливи на състоянието е произволен.

Синтезирана е синхронизационна схема между две идентични хаотични

системи на Ramar с управляваща система (2) и следната подчинена система:

$$\begin{cases} \dot{\tilde{x}}_1 = a\tilde{x}_1 - k\tilde{x}_2\tilde{x}_3 + u_1 \\ \dot{\tilde{x}}_2 = b\sin\tilde{x}_1 + \tilde{x}_1\tilde{x}_3 + u_2 \\ \dot{\tilde{x}}_3 = g\tilde{x}_1\tilde{x}_2 - c\tilde{x}_3 + d \end{cases} \quad (9)$$

Функциите от разсъгласуване за избраната комбинация на хибридна синхронизация имат следния вид:

$$\begin{cases} \dot{e}_1 = \dot{x}_1 + \dot{\tilde{x}}_1 \\ \dot{e}_2 = \dot{x}_2 - \dot{\tilde{x}}_2 \\ \dot{e}_3 = \dot{x}_3 - \dot{\tilde{x}}_3 \end{cases} \quad (10)$$

В този случай за втората и третата двойки променливи ще се постигне идентична синхронизация, а за първата двойка променливи поведението на подчинената система ще бъде обратно спрямо поведението на управляващата система.

Чрез заместване на уравненията на управляващата и управляваната система в (10) се получават следните зависимости:

$$\begin{cases} \dot{e}_1 = a_1e_1 - kx_2x_3 - k\tilde{x}_2\tilde{x}_3 + u_1 \\ \dot{e}_2 = b\sin x_1 + x_1x_3 - b\sin\tilde{x}_1 - \tilde{x}_1\tilde{x}_3 - u_2 \\ \dot{e}_3 = -ce_3 + gx_1x_2 - g\tilde{x}_1\tilde{x}_2 - u_3 \end{cases} \quad (11)$$

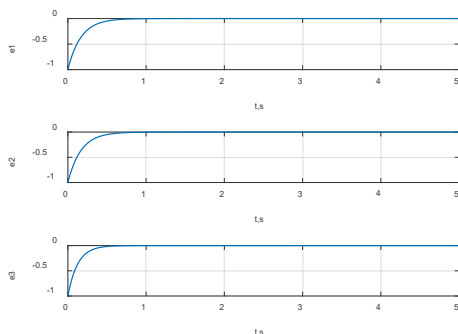
Като се вземе предвид (11) и обобщената форма на функциите на разсъгласуване, управляващите функции се получават, както следва:

$$\begin{cases} u_1 = -a_1e_1 + kx_2x_3 + k\tilde{x}_2\tilde{x}_3 - k_1e_1 \\ u_2 = b\sin x_1 + x_1x_3 - b\sin\tilde{x}_1 - \tilde{x}_1\tilde{x}_3 + k_2e_2 \\ u_3 = -ce_3 + gx_1x_2 - g\tilde{x}_1\tilde{x}_2 + k_3e_3 \end{cases} \quad (12)$$

Функциите на разсъгласуване между управляващата и подчинената системи приемат формата (13) след заместване на управляващите функции в (11)

$$\begin{cases} \dot{e}_1 = -k_1e_1 \\ \dot{e}_2 = -k_2e_2 \\ \dot{e}_3 = -k_3e_3 \end{cases} \quad (13)$$

Управление, базирано на втория метод за устойчивост на Ляпунов, ще бъде постигнато за положителни константи k_i , което ще удовлетвори условие (6).



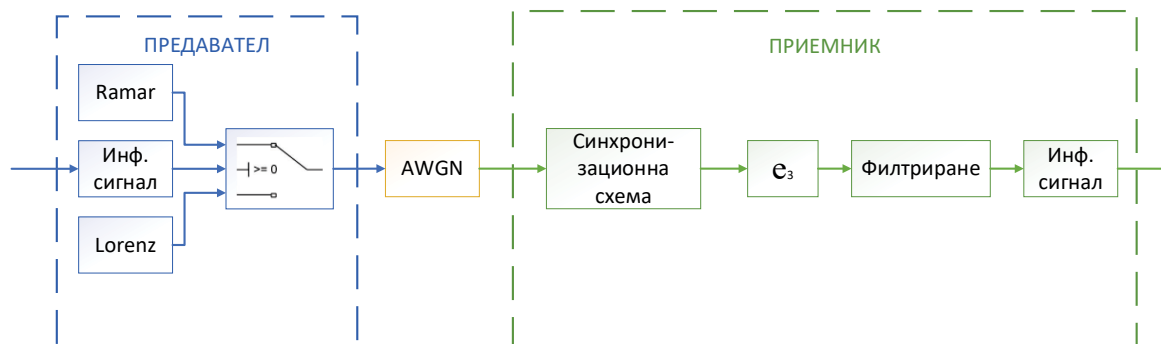
Фиг. 3. Функции на разсъгласуване

Реализирана е схема за синхронизация между (2) и (9) със синтезирани управляващи функции (12). Схемата за синхронизация се изследва в симулационната среда Simulink, а графичните резултати са изведени с помощта на MATLAB. Избрани се следните произволни начални условия $\mathbf{x} = [-1 \ 0 \ 1]^T$ и $\tilde{\mathbf{x}} = [0 \ 1 \ 2]^T$ и положителните константи $k_i = 1, i = 1 \div 3$. Получените функции на разсъгласуване са представени на фиг. 3.

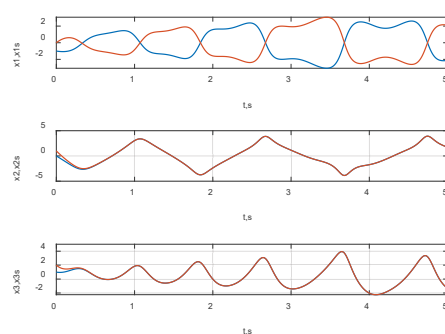
Ясно се вижда, че след установяване на преходният процес, грешките от разсъгласуване между системите се установяват в нула и между управляващата и подчинената системи настъпва режим на хибридна синхронизация (фиг. 4).

Хаотично превключване

Реализираният в настоящия доклад подход за защитено предаване на цифров информационен сигнал, чрез хаотично превключване, използва две неидентични хаотични системи и е представен чрез опростена блокова схема на фиг. 5.

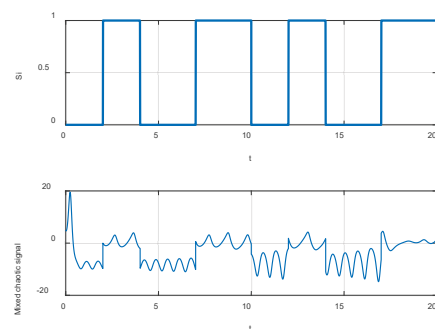


Фиг. 5. Обобщена блокова схема на двойно хаотично превключване



Фиг. 4. Времеви характеристики Master - Slave

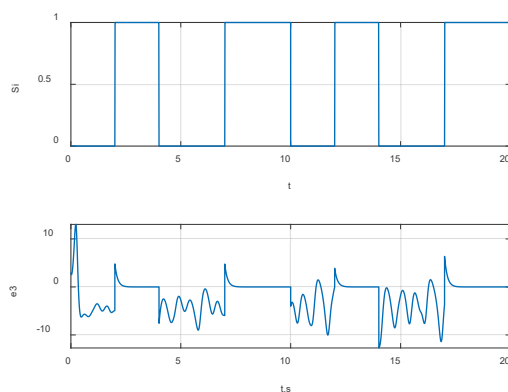
В предавателя са реализирани две неидентични хаотични системи от трети ред – система на Lorenz и система на Ramar, като в зависимост от стойността на цифровия информационен сигнал (0 или 1), се осъществява превключване между променливите на състоянието – x_1 за системата на Lorenz и x_3 за системата на Ramar. Полученият хаотичен сигнал се предава по незащитен канал за връзка с нормално разпределение на шума. Генерираната информационна поредица и полученият смесен хаотичен сигнал са представени на фиг. 6.



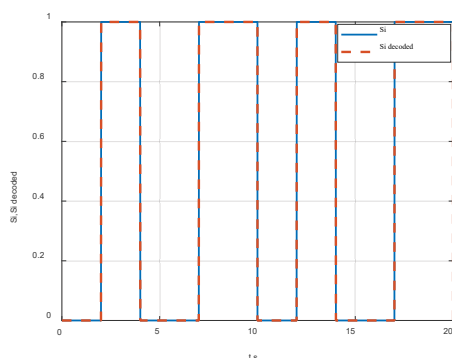
Фиг. 6. Генерирана информационна поредица и смесен хаотичен сигнал

Постъпилият в приемника зашумен хаотичен сигнал преминава през блока за синхронизация, където на база втори метод за устойчивост на Ляпунов е реализирана хибридна синхронизация между две системи на Ramar.

При предадена стойност 1 на информационният сигнал за съответната продължителност от време се предава променливата x_3 за система на Ramar. Следователно при постъпване на сигнала в приемника, хаотична синхронизация ще настъпи само за периода на предаване на стойността „1“. През останалото време системите ще са в режим на десинхронизация. Грешката от разсъгласуване e_3 между системите (2) и (9), заедно с генерираната в предавателя информационна поредица са показани на фиг. 7.



Фиг. 7. Генерирана информационна поредица и грешка от разсъгласуване e_3



Фиг. 8. Генерирана и дешифрирана информационна поредица

Ясно се вижда, че при предадена стойност „1“ на информационния сигнал и след приключване на преходния про-

цес, грешката от разсъгласуване между управляващата и подчинената система се установява в нула.

След подходяща прагова обработка и филтриране, информационната поредица е напълно възстановена – фиг. 8.

ЗАКЛЮЧЕНИЕ

Настоящият доклад представя иновативен подход за защитено предаване на цифрови информационни сигнали чрез хаотично превключване между две неидентични хаотични системи. Използването на хаотични системи за генериране на сигнали, съчетано с хибридна синхронизационна схема, осигурява ефективно решение за преодоляване на предизвикателствата, свързани с шифрирането. Симулационните изследвания потвърждават успешното възстановяване на информационната поредица, подчертавайки надеждността и ефективността на предложения подход.

ЛИТЕРАТУРА

- [1] Umar, Talha, Mohammad Nadeem, and Faisal Anwer. "Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage." *Expert Systems with Applications* 257 (2024): 125050.
- [2] Erkan, Emre, Hidayet Oğraş, and Şehmus Fidan. "Application of a secure data transmission with an effective timing algorithm based on LoRa modulation and chaos." *Microprocessors and Microsystems* 99 (2023): 104829.
- [3] Li, Zongyang, Hongxiang Wang, and Yuefeng Ji. "Hardware fingerprint construction of optical transmitters based on permutation entropy spectrum of chaos for secure authentication." *Optics & Laser Technology* 171 (2024): 109947.
- [4] Haridas, Thejas, et al. "Chaos-based audio encryption: Efficacy of 2D and 3D hyperchaotic systems." *Franklin Open* 8 (2024): 100158.
- [5] Vogl, Markus, Milena Kojić, and Petar Mitić. "Dynamics of green and conventional bond markets: Evidence from the generalized chaos analysis." *Physica A:*

- Statistical Mechanics and its Applications* 633 (2024): 129397.
- [6] Xie, Jiayu, Jie Wang, and Bing Tang. "Circular motion and chaos bound of a charged particle near charged 4D Einstein–Gauss–Bonnet–AdS black holes." *Physics of the Dark Universe* 42 (2023): 101271.
- [7] Zhang, Jianwei, et al. "Complexity analysis of multiscale flow field of dynamic impinging stream based on chaos theory and Stockwell transform." *Chemical Engineering and Processing-Process Intensification* 193 (2023): 109524.
- [8] Kumar, Ajay, et al. "A chaos study of fractal–fractional predator–prey model of mathematical ecology." *Mathematics and Computers in Simulation* 225 (2024): 857-888.
- [9] Zhang, Yu-Kun, et al. "Secure optical communication based on M-ary signals masked by optical chaos." *Optics Communications* 528 (2023): 129017.
- [10] Zhong, Dong-Zhou, et al. "Four-channels optical chaos secure communications with the rate of 400 Gb/s using optical reservoir computing based on two quantum dot spin-VCSLS." *Optics Communications* 529 (2023): 129109.
- [11] Rai, Amrita, et al. "Realization of chaotic oscillator and use in secure communication." *E-Prime-Advances in Electrical Engineering, Electronics and Energy* 6 (2023): 100321.
- [12] Sano, Hideki. "Common Encryption Key Generation and Secure Communication Using PDE Chaotic Synchronization." *IFAC-PapersOnLine* 56.2 (2023): 9942-9947.
- [13] Gokyildirim, Abdullah, et al. "A novel five-term 3D chaotic system with cubic nonlinearity and its microcontroller-based secure communication implementation." *AEU-International Journal of Electronics and Communications* 160 (2023): 154497.
- [14] Wen, Heping, et al. "Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion." *IScience* 27.1 (2024).
- [15] Yang, Tao. "A survey of chaotic secure communication systems." *International journal of computational cognition* 2.2 (2004): 81-130.
- [16] Sathiyamurthi, P., and S. Ramakrishnan. "Speech encryption using chaotic shift keying for secured speech communication." *EURASIP Journal on Audio, Speech, and Music Processing* 2017 (2017): 1-11.
- [17] Ahmad, Israr, Muhammad Shafiq, and M. Mossa Al-Sawalha. "Globally exponential multi switching - combination synchronization control of chaotic systems for secure communications." *Chinese Journal of Physics* 56.3 (2018): 974-987.
- [18] Candido, Renato, Magno TM Silva, and Marcio Eisencraft. "A switching scheme between conventional and chaos-based communication systems." *Proceedings of the 6th International Conference on Nonlinear Science and Complexity*. 2016.
- [19] Shen, Bo-Wen. "A Review of Lorenz's Models from 1960 to 2008." *International Journal of Bifurcation and Chaos* 33.10 (2023): 2330024.
- [20] Ramar, Rameshbabu. "Design of a new chaotic system with sine function: Dynamic analysis and offset boosting control." *Chaos Theory and Applications* 5.2 (2023): 118-126.
- [21] Hamidouche, Baghdadi, Kamel Guesmi, and Najib Essounbouli. "Control and Stabilization of Chaotic Systems Using Lyapunov Stability Theory." *2023 International Conference on Electrical Engineering and Advanced Technology (ICEEAT)*. Vol. 1. IEEE, 2023.