№ 4 (2), 2020 ISSN: 2682 – 9517 (print) ISSN: 2683 – 0930 (online)

Design of chaotic synchronization system based on combined type of synchronization with application to secure communications

Hristina Stoycheva
Automation, Information and Control Systems
Technical Univercity - Gabrovo
Gabrovo, Bulgaria
hsstoycheva@abv.bg

Dragomir Chantov
Automation, Information and Control Systems
Technical Univercity - Gabrovo
Gabrovo, Bulgaria
dchantov@abv.bg

***Abstract* — In this paper, based the second Lyapunov stability law, a chaotic synchronization system that combines projective, marginal and hybrid synchronization is designed. The main functional dependencies in the synthesis of the synchronization scheme are presented. The proposed synchronization type is demonstrated via two identical Zhou-Li systems. The achieved synchronization system is applied to digital signal encryption, through chaotic switching.**

Keywords— chaos, synchronization, secure communications, chaotic switching.

I. Introduction

Considered as the third revolutionary discovery in physics after the theory of relativity and quantum mechanics, chaos theory has been studied in detail in recent decades. Chaos is a complex dynamic behavior of nonlinear systems with a number of specific properties, the most characteristic of which is a strong sensitivity to small changes in the initial conditions and/or parameters of the system [1]. Such behavior describes processes in various fields such as physics [2], chemistry [3], ecology [4], evolutionary dynamics [5], protected communications [6] and others.

Control and synchronization of chaotic systems have been the subject of intensive research in recent years. The concept of synchronization of chaotic systems means processes in which two or more chaotic systems, equivalent or not in structure and parameters, adapt their dynamics to each other by connecting them [7]. An essential characteristic of the predominant part of the known methods for chaotic synchronization is that they aim at the error functions or the differences between the respective variables of the chaotic systems to tend to zero, ie. systems to synchronize their dynamics [8]. Despite the increased interest in the field of chaotic synchronization, which leads to new types of synchronization, such as LAG synchronization [9], robust synchronization [10], fuzzy synchronization [11, 12], etc. most publications are based on the main types of chaotic synchronization, namely identical [13], anti- [14], scaled [15], and offset [16]. However, the choice of only one type of synchronization does not lead to a high degree of protection of the transmitted information.

The possibilities for control and synchronization of chaotic systems give rise to many practical applications in the field of secure communications. One of the basic applications of chaotic synchronization schemes for secure transmission of digital information signal is chaotic switching. Although there are many modifications and variations, the use of its classic version emphasizes the synchronization scheme itself. In practice, the combination with a chaotic synchronization scheme is a new option for signal protection. The achieved level of protection and decoding quality will be mainly due to the realized synchronization.

In the present article, a synthesis of a chaotic synchronization system with a combined synchronization method is realized. A new abstract mathematical model of a chaotic third-order system was chosen as a basis. The proposed combined method combines three main synchronization methods - scaled, shifted and hybrid. To achieve the selected type of synchronization, active control is applied, the synthesis of which is based on the application of the second method for Lyapunov stability. The aim is to obtain a stable chaotic synchronization between two nonlinear systems, which will serve as a good basis for secure data transmission over unsecured communication channels.

II. Design of the sinchronization control

The combined type of synchronization is proposed in [17] and considers the classical problem of chaotic synchronization. This new type of synchronization combines three main synchronization methods - projective, marginal and hybrid. The slave system, when in projective synchronization, has the same quality behavior as the control, but the attractors of the two systems will be of different scale. In marginal synchronization, at least one of the error functions tends not to zero, but to a certain constant. A hybrid synchronization scheme gives the ability to choose which pair of variables between Master and Slave systems will be in anti-synchronization mode, and which will be in synchronization mode.

The system that provides the connecting signal is called Master (Controlling) (1), and the system that receives this signal and adjusts its dynamics - Slave (Controlled) (2). Both can be represented by the following generalized form:

$$\dot{\boldsymbol{x}} = f(\boldsymbol{x}), \tag{1}$$

$$\dot{\tilde{\boldsymbol{x}}} = f(\tilde{\boldsymbol{x}}) + u(\boldsymbol{x}, \tilde{\boldsymbol{x}}), \tag{2}$$

where $\dot{\mathbf{x}}, \dot{\tilde{\mathrm{x}}} \in \Re^n$ are the state vectors of the system, $f(\mathbf{x})$ and $f(\tilde{\mathbf{x}})$ are nonlinear functions, and $u(\mathbf{x}, \tilde{\mathbf{x}})$ is control signal to the Slave system (2). The initial conditions of the system are different, ie. $\mathbf{x}(0) \neq \tilde{\mathbf{x}}(0)$.

In order to achieve hybrid synchronization between systems (1) and (2), such control $u(\mathbf{x}, \tilde{\mathbf{x}})$is needed, to fulfill the condition:

$$\lim_{t\to\infty} e_i(t) = 0, \tag{3}$$

where for identical synchronization, the error function between the systems $e_i(t)$ has the following form $e_i(t) = x_i(t) - \tilde{x}_i(t)$, as a result, the Controlled system will have identical behavior as the Controlling system. In the case of anti-synchronization, $e_i(t) = x_i(t) + \tilde{x}_i(t)$ and the Slave system has a behavior - opposite to the Master system. Hybrid synchronization is a combination of both methods, ie. the error function will take the following form:

$$e_i(t) = x_i(t) \pm \tilde{x}_i(t), \tag{4}$$

Respectively:

$$\dot{e}_i(t) = f(\boldsymbol{x}) \pm f(\tilde{\boldsymbol{x}}) \pm u(\boldsymbol{x}, \tilde{\boldsymbol{x}}) = h(\boldsymbol{x}, \tilde{\boldsymbol{x}}) \pm u(\boldsymbol{x}, \tilde{\boldsymbol{x}}), \tag{5}$$

where $h(\mathbf{x}, \tilde{\mathbf{x}}) = f(\mathbf{x}) \pm f(\tilde{\mathrm{x}})$.

A control based on the Lyapunov second stability method, is synthesized, where such function $V(e)$, corresponding to the conditions is needed:

$$V(e) > 0, \forall e \neq 0, \tag{6}$$

$$V(e) = 0, e = 0, \tag{7}$$

$$\frac{dV(e)}{dt} < 0, \forall e \neq 0, \tag{8}$$

In order to fulfill the three conditions, the selected Lyapunov function most often is a quadratic function of the individual components of the vector e, and the fulfillment of the third condition will be sought by appropriate synthesis of the control functions to the Slave system $u(\mathbf{x}, \tilde{\mathbf{x}})$.

The control function $u(\mathbf{x}, \tilde{\mathbf{x}})$ is chosen of the following type:

$$u(\boldsymbol{x}, \tilde{\boldsymbol{x}}) = h(\boldsymbol{x}, \tilde{\boldsymbol{x}}) \mp k(e_i), \tag{9}$$

Where the first part of the equation $h(\mathbf{x}, \tilde{\mathbf{x}})$ aims to eliminate the first component of the error system (5) and the second part aims to ensure that condition (8) is fulfilled.

With two-component control synthesized as such (9), the error system (5) will be stabilized at the point $e_i = 0$, which corresponds to the selected form of hybrid synchronization.

The Master (1) and the Slave (2) systems, are marginally synchronized when:

$$\lim_{t\to\infty} e_i(t) \to const \neq 0. \tag{10}$$

This condition can be achieved through the so-called marginal coefficients c_i.

In the case of projective synchronization, the slave system (2) will have the same quality behavior as the control system (1), but the attractors of the two systems will have a different scale and sometimes different symmetry. In order to achieve this type of synchronization, it is necessary for the error system to acquire the following type:

$$\dot{e}_i(t) = f(\boldsymbol{x}) \pm \alpha_i f(\tilde{\boldsymbol{x}}) \pm u(\boldsymbol{x}, \tilde{\boldsymbol{x}}), \tag{11}$$

where α_i are scaling coefficients. The cases of identical, anti- and hybrid synchronization can be considered as a special case of projective synchronization with a scaling coefficient $\alpha_i = 1$.

To achieve the combined synchronization [sai19], it is necessary to add to the slave system not only a control function, but also the corresponding scaling coefficients α_i, as well as the marginal coefficients c_i. In this case, the error system acquires the following generalized form:

$$\dot{e}_i(t) = f(\boldsymbol{x}) \pm \alpha_i f(\tilde{\boldsymbol{x}}) \pm u(\boldsymbol{x}, \tilde{\boldsymbol{x}}) + c_i. \quad (12)$$

By synthesizing appropriate control, the error functions will be established not at zero, but at constants that can be freely determined by selecting c_i.

III. Synchronization of two chaotic Zhou - Li system

In 2019 a new mathematical model of a novel three-dimensional autonomous chaotic system is proposed and described by the following equations [18]:

$$\dot{x}_1 = -ax_1 + cx_2x_3 - hx_3^2,$$
$$\dot{x}_2 = bx_2 - x_1x_3,$$
$$\dot{x}_3 = x_1x_2 - dx_3. \quad (13)$$

The system is hyperchaotic for the following parameter values $a = 7$, $b = 3$, $c = 8$, $d = 0.8$ and $h = 0{,}5$. Despite its relative simplicity, the system has many unique and interesting behaviors.

A synchronization scheme of the type (1) - (2), is synthesized, with Controlling system (13) and Slave system as follows:

$$\dot{\tilde{x}}_1 = -a\tilde{x}_1 + c\tilde{x}_2\tilde{x}_3 - h\tilde{x}_3^2 + u_1,$$
$$\dot{\tilde{x}}_2 = b\tilde{x}_2 - \tilde{x}_1\tilde{x}_3 + u_2,$$
$$\dot{\tilde{x}}_3 = \tilde{x}_1\tilde{x}_2 - d\tilde{x}_3 + u_3. \quad (14)$$

Error functions are selected, such as the first pair of variables are in marginal anti-synchronization mode and the second and third are in marginal synchronization mode. Then the error system will have the following form:

$$\dot{e}_1 = \dot{x}_1 + \alpha_1\dot{\tilde{x}}_1 + c_1,$$
$$\dot{e}_2 = \dot{x}_2 - \alpha_2\dot{\tilde{x}}_2 + c_2,$$
$$\dot{e}_3 = \dot{x}_3 - \alpha_3\dot{\tilde{x}}_3 + c_3. \quad (15)$$

By substituting (13) and (14) in (15) and after a few simple mathematical transformations, the following dependences are obtained:

$$\dot{e}_1 = -ae_1 + cx_2x_3 - hx_3^2 + \alpha_1 c\tilde{x}_2\tilde{x}_3 - \alpha_1 h\tilde{x}_3^2 + \alpha_1 u_1,$$
$$\dot{e}_2 = be_2 - x_1x_3 + \alpha_2\tilde{x}_1\tilde{x}_3 - \alpha_2 u_2,$$
$$\dot{e}_3 = -de_3 + x_1x_2 + \alpha_2\tilde{x}_1\tilde{x}_2 + \alpha_3 u_3. \quad (16)$$

Taking into consideration (12) and (16), the control functions are obtained as follows:

$$u_1 = \frac{ae_1 - cx_2x_3 + hx_3^2 - \alpha_1 c\tilde{x}_2\tilde{x}_3 + \alpha_1 h\tilde{x}_3^2}{\alpha_1} + c_1 - k_1e_1,$$
$$u_2 = \frac{be_2 - x_1x_3 + \alpha_2\tilde{x}_1\tilde{x}_3}{\alpha_2} - c_2 + k_2e_2,$$
$$u_3 = \frac{-de_3 + x_1x_2 + \alpha_2\tilde{x}_1\tilde{x}_2}{\alpha_3} + c_3 - k_3e_3. \quad (17)$$

When the control functions (17), are substitute in the error system (15) a record of the following type is obtained:

$$\dot{e}_1 = -k_1e_1,$$
$$\dot{e}_2 = -k_2e_2,$$
$$\dot{e}_3 = -k_3e_3, \quad (18)$$

for which, as stated above, for positive constants k_i, condition (8) is fulfilled.

The synchronization scheme between the control system (13) and the slave system (14) with control functions (17) with coefficients $k_i = 1$, $i = 1 \div 3$ is simulated in Simulink environment. Graphical interpretations of the synchronization processes were obtained in a Matlab environment. The initial conditions of the control system are $\mathbf{x} = [0.1\ 0.1\ 0.1]^T$, and of the slave system - $\tilde{\mathbf{x}} = [0\ 0\ 1]^T$, and both sets are chosen arbitrarily. The marginal and projective factors are also randomly selected as follows: $\alpha_1 = 1$, $\alpha_1 = 2$, $\alpha_2 = 4$, $\alpha_3 = 6$, $c_1 = 3$, $c_2 = 5$ и $c_3 = 9$.

Fig. 1 presents the obtained error functions, which are not established in zero, but in the respective marginal coefficients, which graphically confirms the occurrence of a marginal chaotic synchronization around the second second of the transient process.

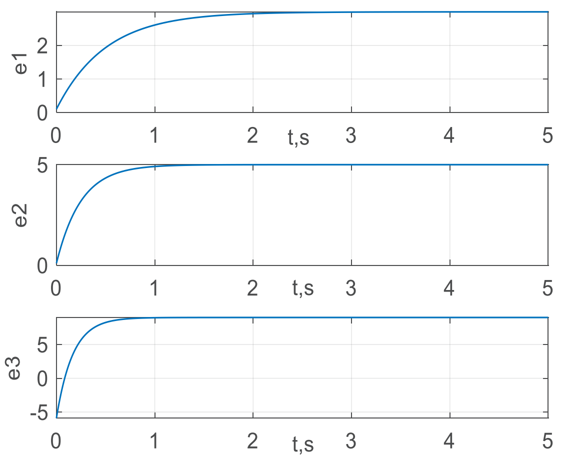

Fig. 1. Time evolution of the error functions

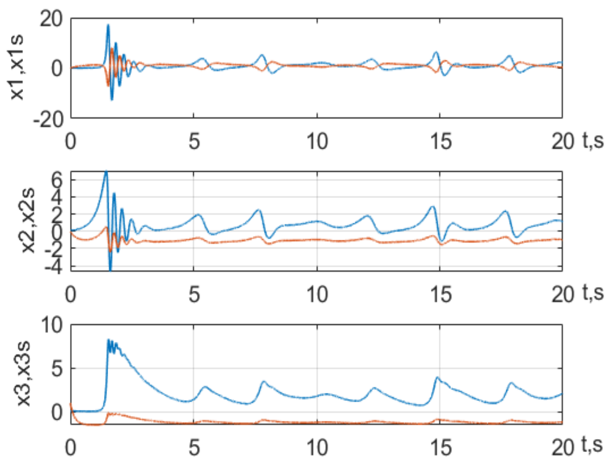

Fig. 2. Time series of the pairs of state variables

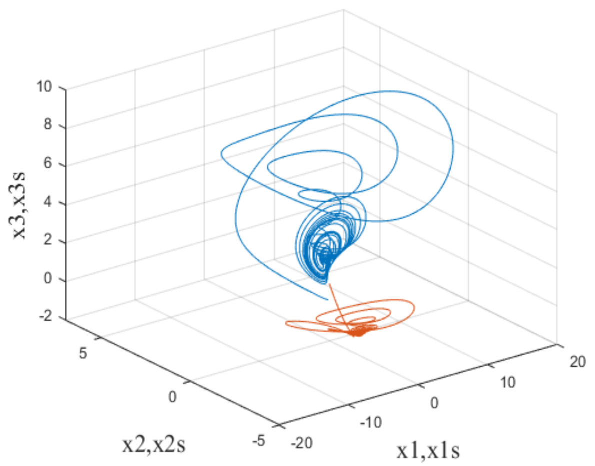

Fig. 3. Chaotic atractors of the Master and Slave systems

Time series of the pairs of state variables for the Master and Slave systems $x_i(t), \tilde{x}_i(t), i = 1 \div 3$ is presented in Fig. 2. The graph shows that after the transient process, the pairs of variables $x_1, \tilde{x}_1$ are in anti-synchronization mode and the dynamics of the Slave system is a mirrored image, relative to the abscissa, of the dynamics of the Master. In addition, the amplitude of $\tilde{x}_1$ is α_1 times lower, ie. the dynamics of the Slave system is scaled by the corresponding coefficient, according to the behavior of the control system. In the pairs of variables $x_2, \tilde{x}_2$ and $x_3, \tilde{x}_3$ an identical synchronization is observed, and the amplitude of the Slave system signal is scaled respectively by α_2 and α_3 times in relation to the Master. Fig. 2 graphically confirms the occurrence of a hybrid projective synchronization mode after the end of the transient process.

The complex synchronization dynamics of the two chaotic systems can be observed by constructing their chaotic attractors in the state space (Fig. 3). The slave system, which before synchronization had a chaotic attractor identical to that of the control system, now has an attractor that is smaller in scale α_i, shifted and definitely different from the original.

IV. Application of the Synchronization Scheme in Chaotic Switching

Chaotic switching is one of the fundamental approaches for secure information transmission public communication channel. The essence of this approach is in encoding a binary information signal in terms of different chaotic attractors of the master system at the transmitter [19]. The binary sequence of the information signal modulates one of the system's parameters in such way, that the system "switches" between two attractors, the first corresponding to the zeros and the second – to the ones of the information signal. The values of the switching parameter p_j have to be chosen carefully in such way, that both attractors A_1 (for p_{j1}) and A_2 (for p_{j2}) to be chaotic ones and to occupy the same area of the state space to impede the identification of the switching moments and at the same time to allow the systems to desynchronize when the parameter value is switched to p_{j2}. The rate of transmission is limited from the length of the transient of the synchronization scheme, so the fastest possible scheme for a given chaotic model has to be used.

№ 4 (2), 2020 ISSN: 2682 – 9517 (print) ISSN: 2683 – 0930 (online)

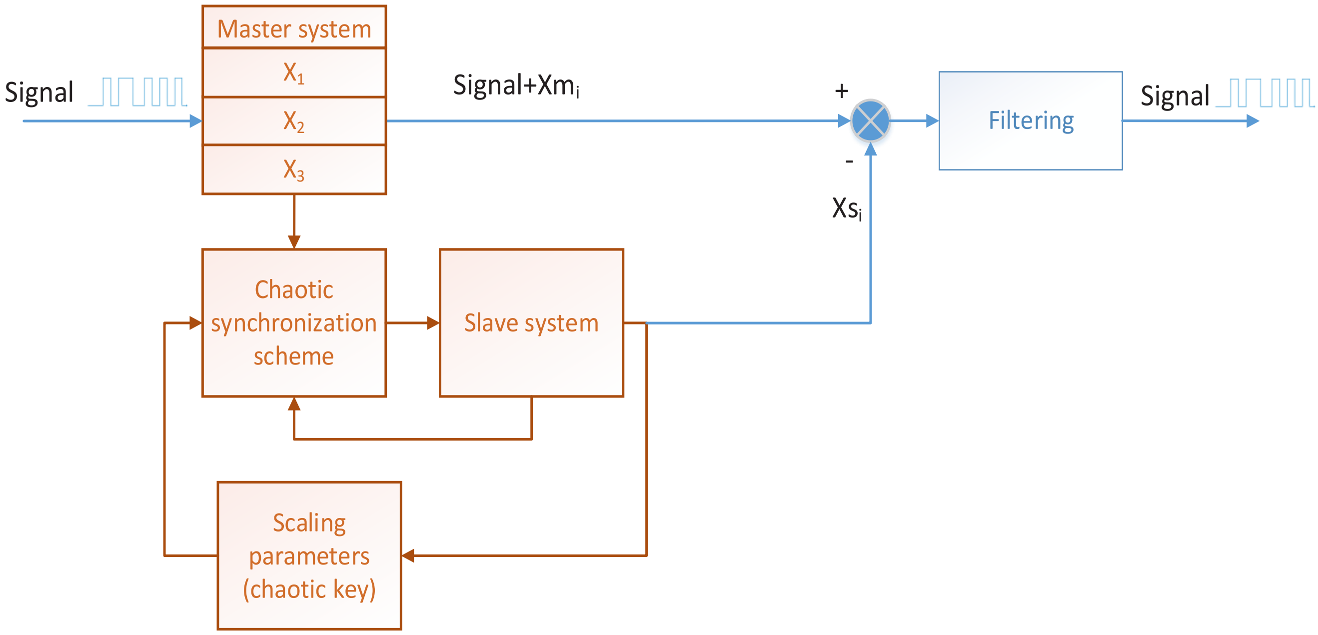

Fig. 4. Generalized block diagram for secure communication by chaotic switching

From the parameters of the Zhou - Li system, the most suitable for p_j is parameter a. One value of the parameter coincides with the nominal one - $p_{j1} = a = 7$, and when choosing Δ = 3 the second value of the parameter is $p_{j2} = p_{j1} - \Delta = 4$. At this value, the system moves on another, also chaotic attractor. Since the parameter $p_{j1} = \tilde{p}_{j1} = 7$ of the Slave system does not change, in the periods when the Master system is switched on the attractor for $a = 4$, the systems will go out of synchronization.

A generalized block diagram of the method for secure communication by chaotic switching is shown in fig. 4. The blocks and connections concerning the chaotic synchronization are marked in red, and the blocks and connections related to the communication scheme are marked in blue.

In the presented generalized block diagram of chaotic switching, the digital information signal replaces a single parameter in the Master system. The chaotic signal of this variable from the state vector is transmitted along the communication line, to the equation of which the information signal replaces the parameter. When restoring, in case of an associated "zero" of the information signal, there is no synchronization between the two systems, and in case of "one" - synchronization is performed. The subsequent signal goes through a filtering process, which is realized through a set of low-frequency, median and functional filters and threshold processing.

The combined type of synchronization increases the degree of protection by increasing the set of variations for the chaotic switching scheme, by means of the so-called a chaotic key consisting of the scaling and displacement coefficients $(\alpha_i, c_i, i = 1 \div 3)$.

For the secure transmission of the binary sequence shown in fig. 5 a). The attractor for $a = 7$ is chosen to correspond to "1", and the one for r = 4 - to "0". It is necessary to pre-select the transmission duration of each bit according to the time to achieve synchronization. For a clearer illustration of the communication method, a longer duration was chosen - 2.5s/bit. In reality, the synchronization scheme realized on the basis of a combined type of synchronization between two identical Zhou - Li systems, allows several times shorter duration. By means of a corresponding modulator in the transmitter (Master system) the parameter a is alternately changed between 7 and 4, according to the specific binary sequence and the selected bit duration. Fig. 5 a) shows the binary sequence by the values of the parameter a; on fig. 5 b) - the connecting signal x_1 in the modulation of the parameter, denoted as Transmited signal; at 5.3 c) - the connecting signal x_1 at standard synchronization; in fig. 5 d) - error $e_1(t)$.

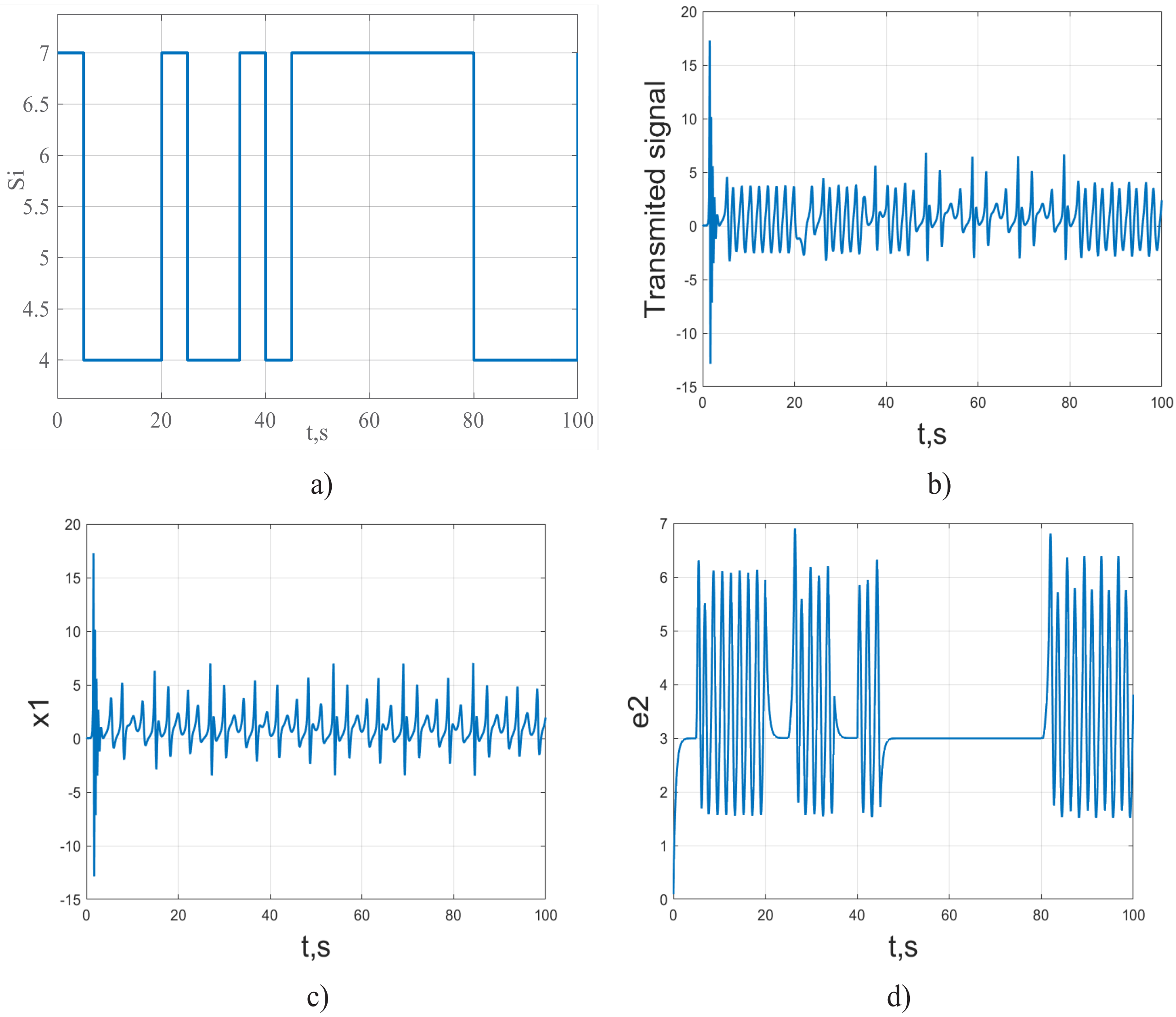

Fig. 5. Communication through chaotic switching

As shown on fig. 5, the signal transmitted along the route between the transmitter and the receiver (x_2 - Transmited signal) has a sufficiently complex dynamics and the information signal mixed in it cannot be distinguished, therefore the transmitted information is protected from unauthorized access. If the pair of attractors on which the transmitter switches are located in different areas of space, the switching would be noticeable. For the Zhou - Li system, the two attractors largely overlap and in the event of unauthorized interception of the signal x_2 - Transmited signal, it is not easy to identify the switching moments.

Since only x_2 is transmitted on the communication channel, the extraction of the useful signal in the receiver is performed by $e_2(t)$, based on a special filter, monitoring when the corresponding error is approximately zero and when it is different or oscillates with much more large amplitude around zero. Considering the previously known bit transmission duration, for the selected scheme the first case will correspond to "1" and the second - to "0".

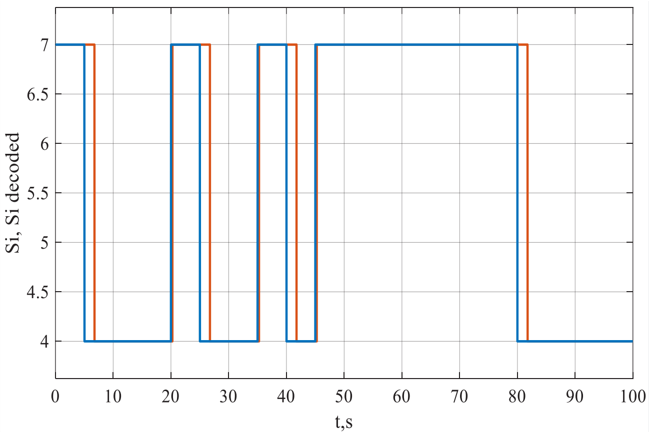

Fig. 6. Transmitted and restored information sequences

Figure 6 shows the information sequence transmitted and restored to the receiver. There is a discrepancy in the impulse duration due to the duration of the transient during synchronization. Given the bit transmission duration and the fact that the impulses can be recovered on the leading edge, this discrepancy is insignificant.

V. Conclusion

This article presents a chaotic synchronization schemes for secure transmission of digital information signal, through chaotic switching. Synchronous behavior between two identical chaotic systems, is obtained by the synthesized synchronization scheme, based on the second Lyapunov stability law. Emphasis is placed on the proposed combined type of synchronization for nonlinear systems, combining projective, marginal and hybrid chaotic synchronization. The implemented chaotic switching corresponds very well with the combined type of synchronization, as the degree of protection is increased significantly. The biggest advantage of this coding scheme is the ability to select different parameters of the control system to be replaced by the information signal, thus in practice increasing the complexity of the formed chaotic key. Without much difference, the proposed digital signal encryption system can be modified and applied to encrypt other types of information.

References

[1] J. Guemez, C. Martin, M. Matias, Approach to the chaotic synchronized state of some driving methods, Physical Review E, Vol.55, No.1, 1997, pp.124-134.

[2] Q. Wang, Signatures of quantum chaos in the dynamics of bipartite fluctuations, Physica A: Statistical Mechanics and its Applications, 2020, pp 554.

[3] A. Ganesh, B. Zhang, R. J. Chalaturnyk, V. Prasad, Uncertainty quantification of the factor of safety in a steam-assisted gravity drainage process through polynomial chaos expansion, Computers & Chemical Engineering, 2020, pp 133.

[4] E. E. Mahmoud, P. Trikha, L. S. Jahanzaib, O. A. Almaghrabi, Dynamical analysis and chaos control of the fractional chaotic ecological model, Chaos, Solitons & Fractals, 2020, pp 141.

[5] Q. Wang, Signatures of quantum chaos in the dynamics of bipartite fluctuations, Physica A: Statistical Mechanics and its Applications, 2020, pp 554.

[6] F. Zhu, F. Wang, L. Ye, Artificial switched chaotic system used as transmitter in chaos-based secure communication, Journal of the Franklin Institute, 2020, pp 10997-11020.

[7] L. Pecora, T. Carroll, Synchronization in chaotic systems, Physical Review Letters, 1990, vol. 64, pp. 821-824.

[8] X. Guo, G. Wen, Z. Peng, Y. Zhang, Global fixed-time synchronization of chaotic systems with different dimensions, Journal of the Franklin Institute, 2020 1155-1173.

[9] W. Zhang, J. Cao, R. Wu, F. E. Alsaadi , A. Alsaedi, Lag projective synchronization of fractional-order delayed chaotic systems, Journal of the Franklin Institute, 2019, pp 1522-1534.

[10] M. Chen, S. Y. Shao, P. Shi, Y. Shi, Disturbance-observer-based robust synchronization control for a class of fractional-order chaotic systems, IEEE Transactions on Circuits and Systems II: Express Briefs, 2016, Vol 64(4), pp 417-421.

[11] S. Y. Li, M. A. B. Hernández, Robust synchronization of chaotic systems with novel fuzzy rule-based controllers, Information Sciences, 2019, pp 604-615.

[12] Y. Wang, H. Yu, Fuzzy synchronization of chaotic systems via intermittent control, Chaos, Solitons & Fractals, 2018, pp 154-160.

[13] D. Zhang, A. Zhao, X. Yang, Y. Sun, J. Xiao, Generalized synchronization between chen system and rucklidge system, IEEE Access, 2019, pp 8519-8526.

[14] E. E. Mahmoud, S. M. Abo-Dahab, Dynamical properties and complex anti synchronization with applications to secure communications for a novel chaotic complex nonlinear model, Chaos, Solitons & Fractals, 2018, pp 273-284.

[15] J. Chen, F. Min, Y. Lv, B. Ye, Projective Synchronization for Heterogeneous Active Magnetic Controlled Memristor-Based Chaotic Systems, 2018 17th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), IEEE, 2018, pp. 64-67.

[16] P. Mareca, B. Bordel, A Chaotic Cryptographic Solution for Low-Range Wireless Communications in Industry 4.0, World Conference on Information Systems and Technologies, Springer, 2019, pp. 134-144.

[17] H. Stoycheva, D. Chantov, Design of chaotic synchronization system combining projective, marginal and hybrid synchronization, International Conference, Automatics and Informatics'2019, 2019, pp 39-42.

[18] C. Zhou, Z. Li, Y. Zeng, S. Zhang, A novel 3D fractional-order chaotic system with multifarious coexisting attractors, International Journal of Bifurcation and Chaos, 2019.

[19] D. Chantov, A chaos – based two level secure communication system on the basis of two different pairs of synchronized chaotic systems, International Journal on Information Technologies & Security, 2012.