Secure Data Transmission Approach with Two-stage Chaotic Protection

Dragomir Chantov[1]

***Abstract* – In this paper an approach for chaotic data protection, applicable to different types of secure communication systems, is proposed. The essence of the proposed method is in combining two independent principles of chaotic data protection – chaotic masking and chaotic parameter modulation, together in order to obtain a higher security level. The method implies the usage of two different pairs of synchronized chaotic systems, integrated in the transmitter and in the receiver of the communication system. The binary information signal modulates a particular parameter of the first system in the transmitter in such way, that the system switches between two different chaotic attractors. The synchronizing chaotic signal, containing and hiding the information signal, is then not directly fed to the identical chaotic system in the receiver as by the standard chaotic parameter modulation approach, but is added to the synchronizing chaotic signal of the second synchronization scheme. In such way the chaotic masking technique is applied, but the masked signal is not the information signal, but the synchronizing signal of the first synchronization scheme. By masking a chaotic signal with another chaotic signal, produced from two different systems, a higher degree of information protection is achieved.**

***Keywords* – Chaotic synchronization, Chaotic masking, Chaotic sswitching**

I. Introduction

Chaotic systems are a specific class of nonlinear systems, characterized with high sensitivity to the initial conditions and a positive Lyapunov exponent(s), which determines the exponential setting apart of the nearby trajectories and the forming of a strange attractor in the phase space. Due to their properties, which put the chaotic systems neither in the class of the determined nor in that of the stochastic systems, they are used in communication systems with chaotic data protection, where the specific features of the chaotic signal are used to hide the transmitted information signal.

These communication systems are based on a phenomenon, called chaotic synchronization. To synchronize two or more chaotic systems means to design a proper coupling between them in such way that the motion of the systems to be in some aspect synchronized. After achieving stable synchronization between two chaotic systems, the coupling chaotic signal between them can be used to bear and hide some kind of useful signal, for example the information signal of a communication system. Different approaches of chaotic data protection are offered so far, the most popular are the chaotic masking technique [1] and the chaotic parameter modulation [2]. However, some research works have shown, that not always these techniques can guarantee the desired level of security.

The chaotic synchronization data protection method, proposed in this paper, implies a two-level structure with synchronized chaotic systems in the transmitter and in the receiver of the communication system. The chaotic parameter modulation technique is used in the first pair of systems to encode a binary information signal. Instead of directly transmitting the chaotic coupling signal through the transmission channel, as with the basic method, it is added to the synchronization chaotic signal of the second pair of completely different chaotic systems. In this way a chaotic signal is masked with another chaotic signal, enhancing the security level of the whole system.

The remaining sections of the paper are organized as follows. In Section II the basic chaotic synchronization definitions are given. In Section III the proposed technique for secure data transmission with two-stage chaotic protection is defined. In Section IV the numerical results with the Van der Poll - Duffing and Rossler chaotic systems, used for the two levels of data protection, are presented.

II. Chaotic Synchronization with Combined Decomposition-type and Feedback Coupling

The main task of chaotic synchronization is to design a coupling scheme between two or more chaotic systems in such way, that their dynamics to be synchronized. Two uni-directionally coupled continuous chaotic systems, called *Master* system and *Slave* system, defined with:

$$\textit{Master}\ \ \dot{\mathbf{x}} = \mathbf{f}(\mathbf{x},t),\ \ \textit{Slave}\ \ \dot{\tilde{\mathbf{x}}} = \tilde{\mathbf{f}}(\tilde{\mathbf{x}},\mathbf{x},t) \qquad (1)$$

where $\mathbf{x} \in \Re^n$ and $\tilde{\mathbf{x}} \in \Re^n$, are called *synchronized* in terms of a given function $Q_t = Q_t[\mathbf{x}(t), \tilde{\mathbf{x}}(t)]$, if $\lim\limits_{t\to\infty} Q_t = 0$. By the most common case of two identical chaotic systems, subjected to synchronization, this function usually is $Q_t = \|\mathbf{e}(t)\|$, where $\mathbf{e}(t)$ is the difference (the error) between the states of the two systems:

$$\mathbf{e}(t) = \mathbf{x}(t, \mathbf{x}(t_0)) - \tilde{\mathbf{x}}(t, \tilde{\mathbf{x}}(t_0)). \qquad (2)$$

The Master and Slave systems are *identically synchronized*, if:

$$\lim_{t\to\infty} \mathbf{e}(t) = 0. \qquad (3)$$

Different approaches to design the coupling are proposed so far. In this paper the combined synchronization approach, proposed in [3], is used. This approach is a combination of the well-known *Partial Replacement* (PR) and *Feedback-coupling* (FB) synchronization methods and implies a double connection between the systems of the type:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, x_i) \rightarrow \dot{\tilde{\mathbf{x}}} = \mathbf{f}(\tilde{\mathbf{x}}, x_i) + \alpha\mathbf{E}(\mathbf{x} - \tilde{\mathbf{x}}). \qquad (4)$$

[1] Dragomir Chantov is with the Department of Automation, Technical University of Gabrovo, Hadji Dimitar 4, 5300 Gabrovo, Bulgaria, E-mail: dchantov@yahoo.com.

This technique gives the possibility to design a far greater number of coupling variants than the basic PR and the FB methods.

III. Method for Secure Data Transmission with Two-stage Chaotic Protection

Two of the most popular methods for chaotic data protection in communication systems are the chaotic masking and the chaotic parameter modulation (chaotic switching) techniques.

By the first one, the data signal is simply added to the chaotic synchronization signal, generated from the master chaotic system at the transmitter. If the amplitude of the data signal is significantly lower than that of the chaotic signal, the synchronization scheme remains stable and the re-construction of the system's variables in the Slave system in the receiver (after achieving stable synchronization) allows the extraction of the data signal.

The chaotic parameter modulation method is characterized with the coding of a binary information signal by different chaotic attractors, obtained for different values of a system parameter at the transmitter. Although more reliable than the chaotic masking technique, this approach also has some limitations and in some cases the desired security level can not be achieved.

The proposed two-stage chaotic data protection method, which implies the consecutive application of the afore-mentioned principles, is illustrated on Fig. 1. The system consists of two synchronization schemes – Master 1 – Slave 1 and Master 2 – Slave 2, which are based on *different chaotic systems*. The chaotic parameter modulation is applied to the Master 1 system at the transmitter. Instead of transmitting the chaotic coupling signal x_i directly to the Slave 1 system at the receiver, it is then masked with a second chaotic signal y_l, generated from a completely different chaotic system at the transmitter. In such way the transmitted signal through the transmission channel is $s(t) = y_l(t) + x_i(t)$, which is a combination of two different chaotic signals. If the level of $x_i(t)$ is sufficiently lower than that of the bearing signal $y_l(t)$ and if a stable synchronization scheme is designed for the pair Master 2 – Slave 2, the signal $x_i(t)$ can be recovered at the receiver - $x_{ir}(t)$. If the level of $x_i(t)$ is such, that it hampers the synchronization of the second pair of systems, it can be scaled down to $x_{isc}(t)$ by the gain k and after extracting the recovered signal $x_{iscr}(t)$ at the receiver it is re-scaled to its original level.

The recovered chaotic signal $x_{ir}(t)$ drives the Slave 1 system at the receiver. according to the preliminarily designed coupling scheme with stable synchronization. After detecting the moments of synchronized and de-synchronized behavior of the pair Master 1 – Slave 1 by the accessible error functions, the original information signal is recovered at the receiver - i_r.

Both synchronization schemes can be designed using the combined method, defined in Section II, to take advantage of the great variety of coupling variants, offered by this approach. The Master 1 – Slave 1 scheme is then defined with:

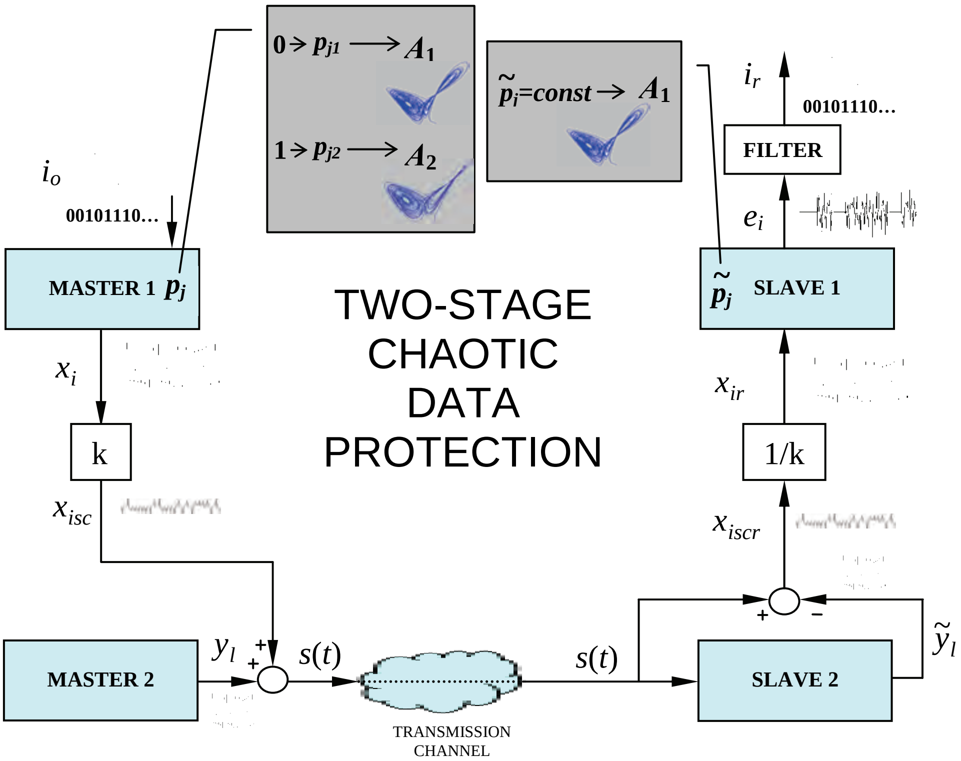


Fig. 1. Two-stage data protection technique with chaotic parameter modulation and chaotic masking

$$\dot{\mathbf{x}} = \mathbf{f}\left(\mathbf{x}, x_i, p_j\right) \to \dot{\tilde{\mathbf{x}}} = \mathbf{f}\left(\tilde{\mathbf{x}}, x_{ir}\right) + \alpha_x \mathbf{E}_x \left(\mathbf{x} - \tilde{\mathbf{x}}\right), \qquad (5)$$

where p_j is the parameter, modulated by the information signal $i_o(t)$.

The Master 2 – Slave 2 scheme is defined with:

$$\dot{\mathbf{y}} = \mathbf{g}\left(\mathbf{y}, y_l\right) \to \dot{\tilde{\mathbf{y}}} = \mathbf{g}\left(\mathbf{y}, s(t)\right) + \alpha_y \mathbf{E}_y \left(\mathbf{y} - \tilde{\mathbf{y}}\right), \qquad (6)$$

where $s(t) = y_l(t) + x_{isc}(t)$ is the signal, transmitted through the channel.

The recovered scaled synchronizing signal of the first pair at the receiver is:

$$x_{iscr}(t) = s(t) - \tilde{y}_l(t). \qquad (7)$$

Apparently, the reconstruction of this signal can be achieved after the second pair of chaotic systems synchronizes, i.e. after $y_l(t) = \tilde{y}_l(t)$.

The main advantage of the proposed approach is that in fact one chaotic signal is masked by another one, produced from different system, and the combined chaotic signal is the only signal, transmitted through the channel of the communication system. In such way, by combining the advantages of two known approaches for secure data transmission with chaotic protection, the security level of the system is enhanced.

IV. Numerical Experiments

To test the proposed two-stage chaotic data protection approach, two well-known chaotic models are chosen for designing the two separate synchronization schemes.

The Master 1 – Slave 1 synchronization scheme is designed on the basis of the Van der Pol – Duffing (VPD) third-order continuous chaotic model [4], which is described by the equations:

$$\begin{aligned} \dot{x}_1 &= -\nu(x_1^3 - \sigma x_1 - x_2), \\ \dot{x}_2 &= x_1 - x_2 - x_3, \\ \dot{x}_3 &= \beta x_2, \end{aligned} \qquad (8)$$

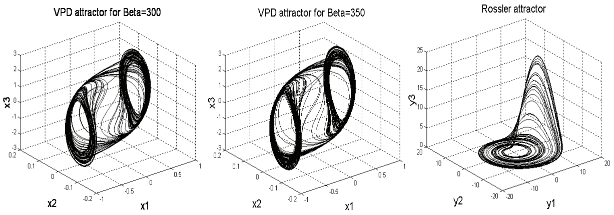
where the nominal parameter values are: $\nu = 100,\ \sigma = 0.35,\ \beta = 300$. The VPD attractor, obtained by computer simulation with Matlab, is shown on Fig. 2(a).

As the first synchronization scheme is used for the parameter modulation data transmission technique, one of its parameters has to be selected for the modulating procedure. The experiments with the three parameters of the VPD system show, that the parameter β is an appropriate candidate for this task. The p_{j1} value, used to code the zeros of the information signal, can be the nominal value $\beta = 300$. After some simulations, the p_{j2} value, used to code the ones, is set to $\beta = 350$. The VPD attractor for $\beta = 350$ is shown on Fig. 2(b). Obviously, it occupies the same area of the state space as the basic attractor, but is slightly different. In such way the switching moments between the two attractors will be unidentifiable by observation of the time-series of the state variables, as the transitions between the two attractors are commensurable with the transitions between the unstable periodic orbits within the basic attractor. On the other hand, as it will be shown further, the difference between the two attractors is enough the two systems to de-synchronize when the ones of the information signal are transmitted.

The Master 2 – Slave 2 scheme is designed on the basis of the Rossler third-order continuous chaotic model [5], which is described by the equations:

$$\begin{aligned} \dot{y}_1 &= -y_2 - y_3, \\ \dot{y}_2 &= y_1 + a y_2, \\ \dot{y}_3 &= b + y_1 y_3 - c y_3, \end{aligned} \qquad (9)$$

where the nominal parameter values are: $a = 0.2,\ b = 1,\ c = 9$. The Rossler attractor is shown on Fig. 2(c).



(a) (b) (c)

Fig. 2. (a) - VPD attractor for $\beta = 300$; (b) - VPD attractor for $\beta = 350$; (c) - Rossler attractor

At first, both synchronization schemes are designed and simulated independently to find the most appropriate type of the couplings. After testing the different possible variants of the combined synchronization approach over the Van der Pol – Duffing model and assuming only a one-variable coupling, the Slave 1 system is designed in the following way:

$$\begin{aligned} \dot{\tilde{x}}_1 &= -\nu(\tilde{x}_1^3 - \sigma \tilde{x}_1 - \underline{x_2}), \\ \dot{\tilde{x}}_2 &= \tilde{x}_1 - \tilde{x}_2 - \tilde{x}_3 + \underline{\alpha_x (x_2 - \tilde{x}_2)}, \\ \dot{\tilde{x}}_3 &= \beta \tilde{x}_2, \end{aligned} \qquad (10)$$

where the coupling gain is $\alpha_x = 20$.

The Slave 2 Rossler system is designed according to the same principles as the previous one. The most appropriate variant of the combined synchronization approach, again implying the self-imposed limitation of one-variable coupling to get the most “economic” coupling, is defined with the equations:

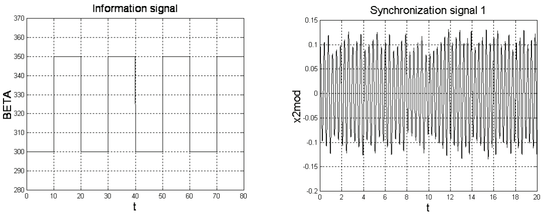
$$\begin{aligned} \dot{\tilde{y}}_1 &= -\tilde{y}_2 - \tilde{y}_3, \\ \dot{\tilde{y}}_2 &= \tilde{y}_1 + a\underline{y_2} + \underline{\alpha_y (y_2 - \tilde{y}_2)}, \\ \dot{\tilde{y}}_3 &= b + \tilde{y}_1 \tilde{y}_3 - c\tilde{y}_3, \end{aligned} \qquad (11)$$

where the coupling gain is $\alpha_y = 2$.

After designing the two stable synchronization schemes, the two-stage chaotic data protection system can be built according to the scheme, shown on Fig. 1. To imitate the information signal i_o in the simulation scheme, a pulse generator with period of 20*s* and 50% duty cycle is used. It modulates the β parameter of the Master 1 VPD system at the transmitter between the values $\beta = 300$ and $\beta = 350$.

The time series of the modulated parameter $\beta(t)$ is shown on Fig. 3(a).

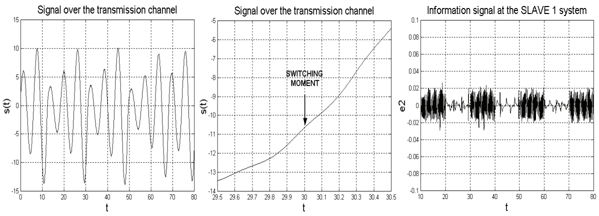
The experiments have shown that no additional scaling of the synchronization signal of the first synchronization scheme is necessary as the level of the VPD x_2 coupling variable is significantly lower than the y_2 Rossler synchronization signal. The time series of the modulated by the information signal VPD coupling variable x_{2MOD} is shown on Fig. 3(b).



(a) (b)

Fig. 3. (a) – Information signal; (b) – Synchronization signal of the first synchronization scheme

The combined chaotic signal $s(t) = y_2(t) + x_{2MOD}(t)$, transmitted over the channel, is shown on Fig. 4(a). One of the zero-to-one transition moments of the information signal is magnified on Fig. 4(b). It is obvious that the switching remains undetectable by observing the time series of $s(t)$. After the two Rossler systems are synchronized, the recovered VPD synchronization signal $x_{2rMOD}(t)$ at the receiver is approximately equal to the original signal $x_{2MOD}(t)$ at the transmitter. Consequently, $x_{2rMOD}(t)$ can be used to synchronize the Slave 1 VPD system with the MASTER 1 system at the transmitter. Then the observation of the second error function $e_2(t) = x_{2MOD}(t) - \tilde{x}_2(t)$ at the receiver, shown on Fig. 4(c), allows to restore the original information signal after the initial synchronization of the two Rossler systems.



(a) (b) (c)

Fig. 4. (a) – Signal over the transmission channel $s(t)$; (b) – One of the switching moments over $s(t)$; (c) – Error function $e_2(t) = x_{2MOD}(t) - \tilde{x}_2(t)$

The de-synchronization moments (the ones of the information signal) are clearly visible on the figure. The experiments show that the variance of $e_2(t)$ is about $1.2e-4$ in the de-synchronization windows (a "one" transmission) and about $1.7e-5$ in the synchronization ones (a "zero" transmission). A simple filter can then be designed in the receiver module to track the changes in the variance of the error function in order to restore the original information signal.

V. Conclusion

A method for secure data transmission with chaotic protection of the information signal was presented in this paper. The proposed method combines the advantages of chaotic masking and chaotic parameter modulation techniques and at the same time it ensures a higher rate of data security by transmitting only a chaotic signal, generated by one chaotic system, masked with another chaotic signal, generated by completely different chaotic system, over the transmission channel. The reconstruction of the information signal at the receiver is achieved by application of a simple algorithm, assuming stable synchronization schemes are designed for the chaotic parameter modulation and chaotic masking procedures. To facilitate the design of such schemes, a synchronization approach implying a combination of partial replacement and feedback coupling synchronization methods is used. It allows to design a large number of coupling schemes for any particular pair of chaotic systems and it was proven empirically, that some of these schemes achieve faster synchronization than the fastest variant of the basic synchronization methods. This permits a faster rate of data transmission if a chaotic data protection system is designed on the basis of the given synchronization scheme.

References

[1] U. Parlitz, *et all*, "Encoding messages using chaotic synchronization", Physical Review E, Vol.53, No.5, pp.4351-4361, 1996.

[2] M. Ogorzalek, "Taming chaos – part I: Synchronization", IEEE Transactions on Circuits and Systems-I, Vol.40, No.10, pp.693-699, 1993.

[3] R. Radev, D. Chantov, "Control of chaotic system by combined synchronization", Proc. of International Scientific Conference ICEST 2005, 29 June - 1 July 2005, Nis, Serbia, pp.490-493.

[4] G. King and T. Saito, "Bistable chaos. I. Unfolding the cusp", Physical Review A, Vol.46, No.6, pp.3092-3099, 1992.

[5] O. Rossler, "An equation for continuous chaos", Physics Letters, Vol.57A, No.5, pp.397-398, 1976.