engineering proceedings

Proceeding Paper

Application of Artificial Neural Networks for Signal Recovery After Chaotic Switching-Based Encryption †

Hristina Stoycheva [1,*,‡] and Georgi Mihalev [2,‡]

[1] Department of Communication Technique and Technologies, Faculty of Electronics and Engineering, Technical University of Gabrovo, 5300 Gabrovo, Bulgaria
[2] Department of Automation, Information and Control Systems, Faculty of Electronics and Engineering, Technical University of Gabrovo, 5300 Gabrovo, Bulgaria; gmihalev@tugab.bg
* Correspondence: hsstoycheva@tugab.bg
† Presented at the International Conference on Electronics, Engineering Physics and Earth Science (EEPES2026), Bandirma, Turkey, 24–27 June 2026.
‡ These authors contributed equally to this work.

Abstract

The problem of recovering an information sequence in the signal decoding process under the application of a chaotic switching scheme via synchronization is examined in the article. A classical chaotic switching scheme based on the bifurcation parameter of the Lorenz system is used, in which the two logical levels are encoded through fundamentally different system dynamics. Decoding is performed by means of chaotic synchronization, whereby the encoding system with one value of the bifurcation parameter, located in the transmitter, is synchronized with another system located in the receiver. Through the use of a pretrained nonlinear autoregressive artificial neural network (NARX), dynamic nonlinear signal reconstruction through input–output alignment (DNRS-IOA) is implemented for the recovery of the information sequence. Experiments are performed in the MATLAB environment, and graphical and numerical results are presented, showing low error levels (MSE = 0.002) and high correlation levels (R-value = 0.9998) between the output of the neural network and the reference signal.

Keywords: secure communication; chaos; chaotic switching; chaotic synchronization; NARX model

1. Introduction

One of the main reasons for the emergence of the process of protection through information encoding, and in particular signal encryption, is the response to practical problems associated with the transmission, dissemination, storage, and above all the use of one type of information or another. By definition, information is vulnerable, on the one hand because this is inherent in its nature, and on the other because it is disseminated through environments that are not under our control. With the development of communication networks and distribution channels, this problem is becoming more acute. For this reason, new and increasingly advanced approaches to encryption must be developed to ensure the required degree of protection, while remaining within certain acceptable limits defined by efficiency, processing speed (encoding and decoding), universality, and other parameters.

The introduction of chaos as a phenomenon for information protection is one of the most promising additions to the methods of data encoding in communication systems [1–3]. It finds application in the encoding of continuous or digital signals [4], images [5], text [6],

Check for updates

Academic Editors: Teodor Iliev, Ivaylo Stoyanov, Grigor Mihaylov and Selahattin Kosunalp

Published: 3 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

audio and video signals [7,8], access control [9], and others. The use of chaos in communication systems also plays a positive role in resistance to noise and interference [10], the efficient use of bandwidth [11], the improvement of interoperability between devices [12], the facilitation of signal processing [13], error detection [14], access management [15], and others.

Being characterized by high sensitivity to changes in parameters and initial conditions, nonlinear systems exhibiting chaotic dynamics are the main source for the generation of pseudorandom sequences. The independent use of chaotic and hyperchaotic systems in schemes and algorithms for information encoding leads to an unlimited number of variations and modifications in all known approaches. Despite the complexity of the implemented scheme, it has a significant drawback, consisting in the fact that decoding is possible only through the sharing of the so-called chaotic key.

A significant new impetus in the use of chaos for information protection is provided by the implementation of a synchronization scheme between two or more chaotic systems, one of which is designated as the master and is located in the transmitter, while the other is designated as the slave and is located in the receiver. In this way, once synchronization has been achieved, the two systems share common dynamics, and the recovery of the encoded information in the receiver becomes possible without the sharing of a key. This type of information encoding offers a high degree of protection, even when not particularly complex procedures are used, which is due to the enormous number of chaotic and hyperchaotic systems and their high sensitivity to changes in parameters and initial conditions.

In general terms, the implementation of chaos in an information encoding scheme has led to the distinction of three main approaches: chaotic masking, chaotic switching, and chaotic modulation. In the present study, attention will be focused only on the method of chaotic switching, as the earliest approach to the encoding of digital signals by means of chaos.

Although chaotic switching is classified in the literature as one of the fundamental methods of digital modulation, encoding itself through substitution and, respectively, switching between several attractors of different chaotic systems for the representation of the digital states “0” and “1” constitutes an entire group referred to as Chaos Shift Keying (CSK) [16]. In a broader sense, this also includes the variations involving switching between chaotic regimes and changing the system parameters during transmission.

The main modifications of CSK are grouped into two categories:

- Coherent CSK—in which, to a certain extent, the presence of synchronization between the chaotic systems in the receiver and the transmitter is required. The main representatives are standard CSK with switching between two attractors [17] and ICI-CSK, which represents a modification involving switching between different initial conditions of the system with the aim of improving spectral efficiency [18].
- Non-coherent CSK—the same switching-based encoding scheme, but without the requirement for synchronization. The basic representatives are: Differential Chaos Shift Keying (DCSK) [19], Frequency-Modulated DCSK (FM-DCSK) [20], Multi-Carrier DCSK (MC-DCSK) [21], Quadrature Chaos Shift Keying (QCSK) [22], and Reference-Modulated DCSK (RI-DCSK) [23].

Some of the latest and most recent developments and studies on the subject are mainly directed toward DCSK, with the primary aims being the reduction in decoding complexity and the improvement of reliability in multi-user communication systems [24], better noise suppression through the integration of an index modulation technique [25], the improvement of data transmission rate, energy efficiency, and spectral efficiency through the inclusion of code index modulation (CIM) and the use of quasi-orthonormal bases [26],

the increase in data transmission rate through the use of carrier phase modulation, time-slot indexing, and code index modulation [27], and others [28,29].

In [30], attention is also given to QCSK, where the use of joint time-slot, code, and energy-index modulation is proposed in order to achieve high-speed data transmission, while in [31], QCSK with hybrid modulation, including carrier-frequency index and slot index, is considered.

Coherent chaotic communication systems are less extensively represented, and hybrid variants of non-coherent methods with the possibility of synchronization realization are mainly discussed. In [31], an architecture consisting of amplified spontaneous emission noise (ASE), a phase modulator (PM), and a fiber Bragg grating (FBG) is proposed in order to achieve double masking at high transmission rates in an optical communication environment, while a common-signal-induced method is used to achieve system synchronization. A new scheme for high-speed key distribution, based on interferometry with interference-spectrum shift by mutual signal modulation under chaotic synchronization, is proposed in [30], where the proposed optimization significantly improves the entropy-source rate. A combination of QCSK with chaotic synchronization in [29] offers improved resistance to noise and eavesdropping compared with conventional CSK schemes. An experimental study of a high-speed optical communication scheme with chaotic key distribution in combination with chaotic synchronization is presented in [28].

In the present article, attention is focused on the decoding process in coherent CSK communication systems using chaotic synchronization for the transmission of digital information. In decoding, the response speed and the type of transient process play an essential role in the correct recovery of the digital signal. The use of an ANN is proposed as the final stage in the decoding process in order to solve some of the main problems arising in the application of coherent CSK schemes.

The remainder of the article is organized as follows. Section 2 discusses the problem that arises in signal decoding in coherent CSK schemes and presents the methods used to realize protected data transmission. Section 3 presents the obtained simulation results related to the use of a nonlinear ANN. The conclusion is presented in the final section.

2. Preliminaries

2.1. Problem Statement

The choice of an encoding scheme based on switching between two or more chaotic systems is determined by two reasons: compared with methods using a single chaotic system, switching between chaotic systems leads to better pseudorandom behavior; and second, switching between chaotic systems effectively increases the degree of protection.

In the literature review conducted and presented in Section 1, the relatively small share of publications focusing on coherent CSK schemes is noteworthy. A significant quantitative predominance of developments based on non-coherent DCSK can be observed. In the reviewed publications, it is clearly indicated that chaotic synchronization leads to an increased degree of protection, but creates a major problem in information recovery, especially in the presence of noise. As a main factor underlying this phenomenon, the presence of a transient process during the synchronization of the systems can definitely be identified.

To date, the specific steps or processing operations used in information recovery have not been discussed in detail in the literature. The decryption process is clear up to the synchronization stage, after which successive procedures for filtering, correlation, integration, threshold processing, decision-making, and others are applied. The impression is created that this part of the recovery process follows an ad hoc strategy. To a certain

extent, this is indeed the case, which makes the entire scheme inefficient and renders the design of the decoding module in the receiver difficult.

To illustrate more clearly what exactly happens after the signal is received at the receiver, a simulation-based implementation of digital signal encryption by means of classical chaotic switching is considered, using the well-known Lorenz chaotic system with bifurcation parameter r. Figure 1 shows the encoded information signal (Figure 1a) and the signal obtained at the receiver after synchronization (Figure 1b). In the figure, the aperiodic nature of the transient process during the time required to achieve complete synchronization can be clearly observed. Subsequently, this contributes to a large error in the recovered signal (Figure 2).

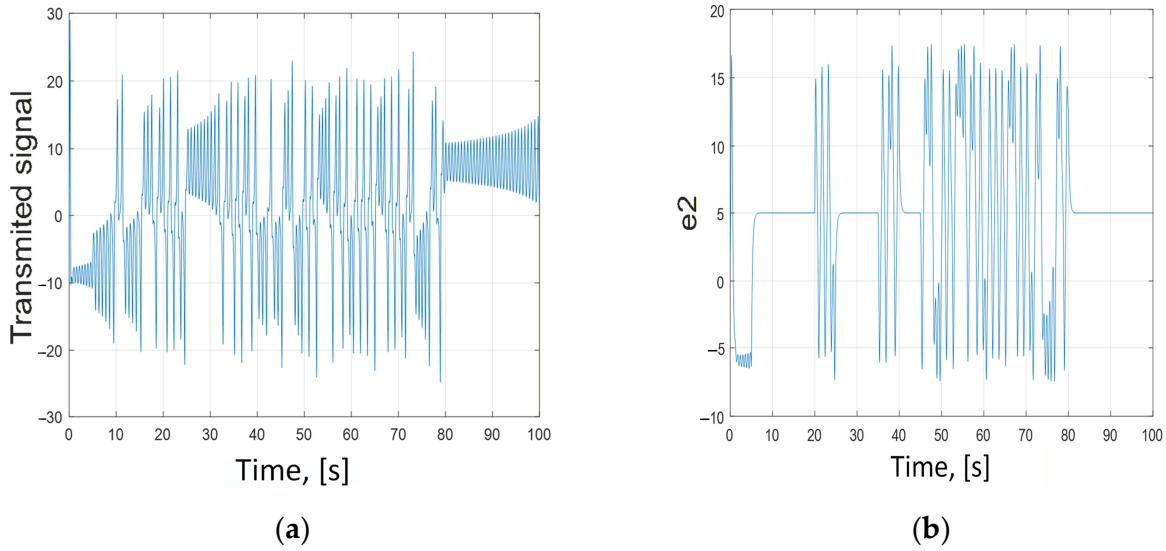


Figure 1. Encryption of a digital signal by classical chaotic switching. (**a**) Encrypted information signal; (**b**) signal in the receiver after synchronization.

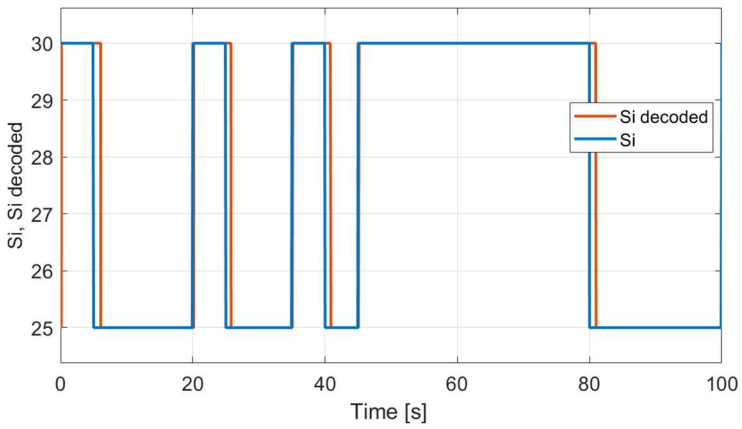


Figure 2. Information and recovered signals.

A possible approach to solving this problem is the use of a series of filters and threshold-processing operations. It should be noted in advance that this is not an optimal solution, and the coefficients used depend on the type of chaotic system.

The procedure is cumbersome, but it uses elementary building blocks. Initially, the process begins with the formation of a second delayed signal, $u_\tau(t)$, where the value of τ depends on the signal frequency. The two signals pass through a switching threshold

nonlinearity, the aim being to introduce structure and interpretability after amplification. The following relationship is used:

$$u_o(t) = u(t) + K_p H(T - u(t)), \tag{1}$$

where K_p is the gain coefficient, T is the threshold value, and H is the Heaviside function.

In the second stage, a nonlinear decision-making logic is implemented, based on the absolute difference between two input signals—the original $u(t)$ and the delayed signal $u_\tau(t)$. When the difference is very small, amplification is applied; for intermediate values, the signal is passed unchanged; and for large deviations, the output is set to zero, which is implemented by means of the formula:

$$u_o(t) = f(u(t), u_\tau(t)) = \begin{cases} |u(t) - u_\tau(t)| + K_{p2}, & for\ |u(t) - u_\tau(t)| < T_1 \\ |u(t) - u_\tau(t)|, & for\ T_1 \le |u(t) - u_\tau(t)| \le T_2, \\ 0, & for\ |u(t) - u_\tau(t)| > T_2 \end{cases} \tag{2}$$

where K_{p2} is the second gain coefficient, and T_1 and T_2 are threshold values.

In the third stage, low-pass filters are introduced depending on the noise level. A positive aspect is the use of a nonlinear compressing element that preserves the fill density at logical "1".

The final stage consists of the use of a median filter, by means of which averaging of the signal value at logical "1" is performed, which in fact represents a pulse sequence. The filter suppresses this sequence, which has the characteristics of impulse noise, by using the median while preserving the structural features of the signal. The value of the filter window is again adjusted by means of a heuristic approach.

The aim of the present study is for this entire procedure to be replaced by a nonlinear artificial neural network trained using a specific chaotic system for a given digital sequence.

2.2. Chaotic Synchronization

At its core, chaotic synchronization considers the case of unidirectional coupling between two identical chaotic systems, initialized from different initial conditions, with the aim of adjusting the dynamics of one system to those of the other. In practice, the driving system is conventionally referred to as the Master, while the system whose dynamics are adjusted to those of the driving system is referred to as the Slave.

The synthesis of an appropriate control law is a complex process, specific to each synchronization scheme, and directly dependent both on the order of the systems and on the selected type of synchronization. The common factor in every synthesized control law is the pursuit of stable synchronization. An exceptionally effective tool for the stability analysis of systems, providing not only a necessary but also a sufficient condition for stability, is the so-called second, or direct, Lyapunov method. With regard to the investigation of the time evolution of the synchronization error $e(t)$, a Lyapunov function with the following properties may be defined:

$$\begin{array}{l} V(\mathbf{e}) > 0, \forall \mathrm{e} \neq 0, \\ V(\mathbf{e}) = 0, \mathrm{e} = 0, \\ \frac{dV(\mathbf{e})}{dt} < 0, \forall \mathrm{e} \neq 0. \end{array} \tag{3}$$

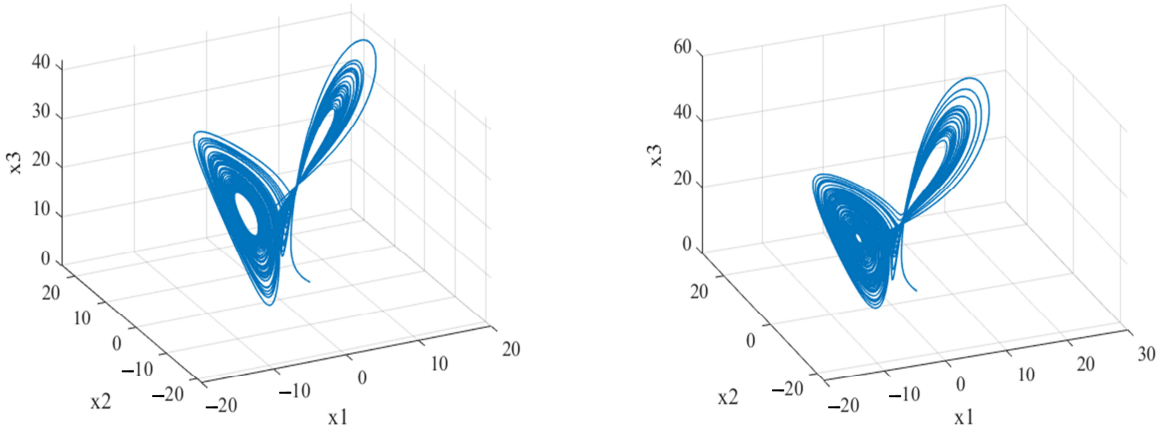
If, for a given synchronization scheme, such a function $V(\boldsymbol{e})$, for the error functions system can be found that satisfies the above conditions, then the synchronization manifold of that synchronization scheme will be stable.

When the two chaotic systems are initialized from different initial conditions and are coupled by such control functions $\mathbf{u}\left(\mathbf{x}, \widetilde{\mathbf{x}}\right)$ that $\lim_{t\to\infty} \dot{\mathbf{e}}(t) = 0$, identical synchronization occurs between the two systems.

For the construction of the synchronization scheme, the classical chaotic model of the thermal convection equations proposed by Edward Lorenz in 1963 was selected and is described by the following mathematical model:

$$\begin{aligned} \dot{x}_1 &= -\sigma x_1 + \sigma x_2 \\ \dot{x}_2 &= -x_1 x_3 + r x_1 - x_2 \\ \dot{x}_3 &= x_1 x_2 - b x_3 \end{aligned} \tag{4}$$

where, for the combination of parameter values optimal for the system, $\sigma = 10$, $b = 8/3$ and $r > 25$, chaotic oscillations arise in the system. The parameter r serves as a bifurcation parameter for the Lorenz system, since qualitative changes in the behavior of the system are observed as its value is increased. These very changes are presented graphically by means of a three-dimensional projection of the chaotic attractor in the state space in Figure 3a for $r = 25$ and in Figure 3b $r = 30$.



(**a**) $r = 25$ (**b**) $r = 30$

Figure 3. Attractors of the system for different values of r.

The slave system takes the following form:

$$\begin{aligned} \dot{\widetilde{x}}_1 &= -\sigma \widetilde{x}_1 + \sigma \widetilde{x}_2 + u_1 \\ \dot{\widetilde{x}}_2 &= -\widetilde{x}_1 \widetilde{x}_3 + r \widetilde{x}_1 - \widetilde{x}_2 + u_2 \\ \dot{\widetilde{x}}_3 &= \widetilde{x}_1 \widetilde{x}_2 - b \widetilde{x}_3 + u_3 \end{aligned} \tag{5}$$

The mismatch system is described by the equations:

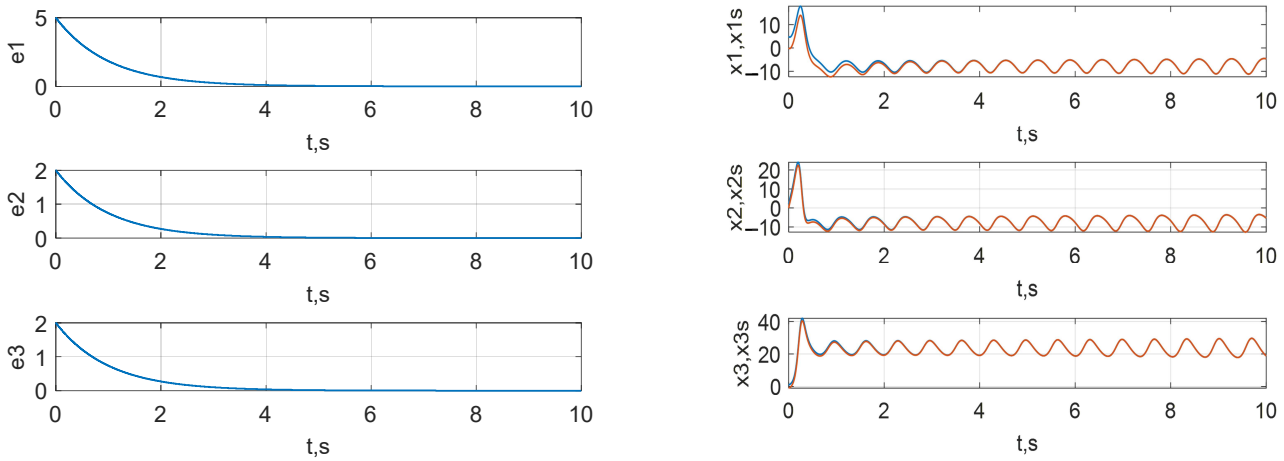
$$\begin{aligned} \dot{e}_1 &= \dot{x}_1 - \dot{\widetilde{x}}_1 + u_1, \\ \dot{e}_2 &= \dot{x}_2 - \dot{\widetilde{x}}_2 + u_2, \\ \dot{e}_3 &= \dot{x}_3 - \dot{\widetilde{x}}_3 + u_3, \end{aligned} \tag{6}$$

and, in order for identical synchronization to be achieved between the driving and the slave systems, the following control functions are synthesized:

$$
\begin{aligned}
u_1 &= -\sigma e_1 - \sigma e_2 + k_1 e_1, \\
u_2 &= -x_1 x_3 + r e_1 - e_2 + \widetilde{x}_1 \widetilde{x}_3 + k_2 e_2, \\
u_3 &= x_1 x_2 - b e_3 - \widetilde{x}_1 \widetilde{x}_2 + k_3 e_3.
\end{aligned} \tag{7}
$$

Under the control law synthesized in this manner, and for positive constants k_i, the conditions of Lyapunov's second method for stability are satisfied, as a result of which the synchronization scheme is stable.

The synchronization scheme is studied in Simulink environment, and the graphical results are displayed using MATLAB (R2023a). The positive constants $k_i = 1$, $i = 1 \div 3$, and the following random initial conditions are chosen: $\mathbf{x} = [5\ 2\ 1]^{\mathrm{T}}$ and $\widetilde{\mathbf{x}} = [0\ 0\ 1]^{\mathrm{T}}$. The error functions obtained from the simulation are presented in Figure 4a. The transient completes in 4 s, which is graphically proven from the time variables presented in Figure 4b. After the completion of the transient process, it is visible that all variables are in synchronization mode and the dynamics of the slave system are equal to those of the master system.



(**a**) error functions (**b**) time-domain characteristics

Figure 4. Identical synchronization between two Lorenz systems.

2.3. Chaotic Switching

For the implementation of the basic variant of chaotic switching, the bifurcation parameter of the Master system, β_1, is selected, and it is required that all pairs of parameters of the Master and Slave systems be approximately equal, including $\beta_1 \approx \widetilde{\beta}_1$. A second value of the bifurcation parameter is then selected, $\beta_2 = \beta_1 + \Delta$, where Δ is chosen such that, at the new value of the parameter, synchronization does not occur ($\widetilde{\beta}_1$ remains unchanged). It is assumed that β_1 corresponds to "0", while β_2—corresponds to "1". In this way, the binary sequence is encoded by switching between two different chaotic attractors of the transmitter, corresponding to the two values of the selected bifurcation parameter. Since the corresponding parameter in the receiver is not changed, the two systems become desynchronized during the transmission intervals of "1" (β_2), whereas during the transmission of "0" ($\beta_1 \approx \widetilde{\beta}_1$) they become synchronized again. A simplified block diagram of chaotic switching is presented in Figure 5.

Let the secure transmission of a binary sequence be required. Based on the presented synchronization scheme, the attractor for $r = 25$ is selected to correspond to "0", while that for $r = 30$ is selected to correspond to "1".

The states of the information sequence alter the value of the bifurcation parameter of the system in the transmitter, whereby the transmitted signal represents a combination of

two different chaotic signals. In the case of unauthorized interception of the signal in the transmission medium, they are, in practice, impossible to distinguish from one another.

In the receiver, after the synchronization process, the information signal represents a combination of a chaotic signal—where the received signal corresponds to $r = 30$—and zero—for $r = 25$, due to the achieved synchronization. The information signal thus obtained must then undergo a recovery process.

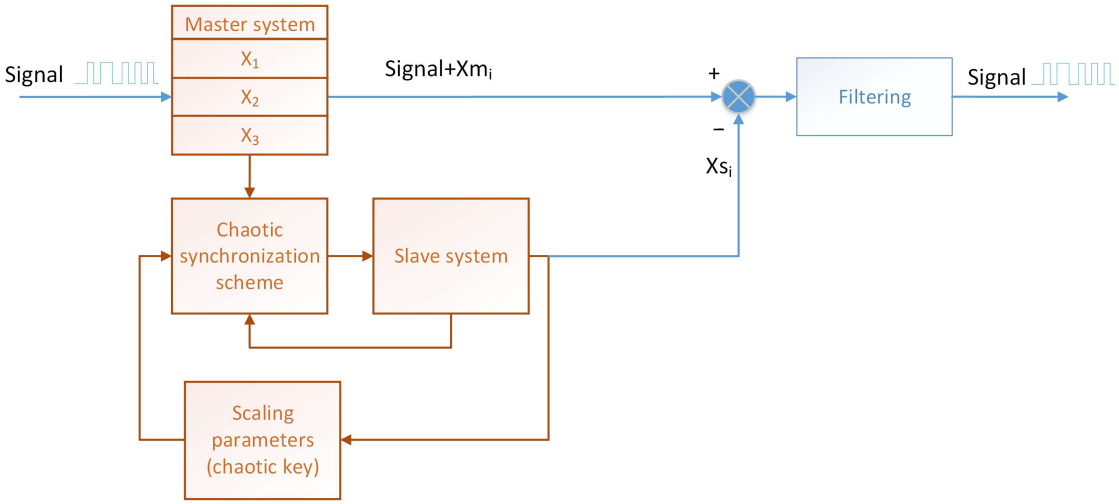


Figure 5. Simplified block diagram of chaotic switching.

2.4. Dynamic Nonlinear Signal Reconstruction via Input–Output Time Alignment

The recovery of the signal after the synchronization process is a task in which the recovered information signal must be obtained from the signal received at the receiver, representing the error function. Considering the nature of the signals (Figures 1 and 2), this type of task cannot be classified as time-series prediction, or as approximation, or as pure filtering. This type of processing is referred to as Dynamic Nonlinear Signal Reconstruction with Input–Output Alignment (DNRS-IOA). For the implementation of DNRS-IOA, nonlinear autoregressive artificial neural networks are used, as they provide particularly good results and are well suited for handling nonlinear dynamic problems, such as the present one.

There are essentially three such ANNs: the Nonlinear Autoregressive Network with Exogenous Inputs (NARX), the Nonlinear Autoregressive Network (NAR), and the Nonlinear Input–Output Network (NIO). Of these, the first is selected for use because, unlike the other two, it can be trained using target data from the receiver signal and the information signal, while the values of the variables from the state vector of the employed chaotic system can be used as an additional time series. It is precisely this ANN architecture that makes it possible to obtain the best possible results.

The neural network is composed of a single hidden layer containing 50 neurons. The training method used is the Levenberg–Marquardt method. This method generally requires more memory, but it is much faster. The training process is automatically terminated when the performance ceases to improve, which is observed when the mean squared error of the validation records begins to increase. Typically, during the training process, a percentage ratio is selected to determine what portion of the data is used for training (the data fed to the ANN during training), validation (used to measure the condition for stopping the training), and testing (used for independent testing of the ANN during and after training, without being involved in the training process). For the specific task, 70% is used for training, 15% for validation, and 15% for testing.

In many prediction tasks, a certain correlation is observed between the modeled time series of values and additional external information. This additional information may be beneficial to the reconstruction process by providing a more accurate prediction. A model of a Nonlinear Autoregressive Neural Network with Exogenous Input is presented in detail in [17].

This type of ANN predicts a series of values $y(t)$ for given p past values of the series $y(t)$ and an additional (external) series x(t), which may be one-dimensional or multidimensional. The mathematical definition of the NARX neural network is described by:

$$y(t) = h(x(t-1), x(t-2), \ldots, x(t-k), y(t-1), y(t-2), \ldots, y(t-p)) + \epsilon(t) \quad (8)$$

In the present task, one input is used for the received signal $y(t-1)$ at time $t-1$, and one additional input, again at time $t-1$, is used for the information $x(t-1)$, which is proposed to correspond to the values of the information signal. Figure 6 shows the architecture of the NARX model used.

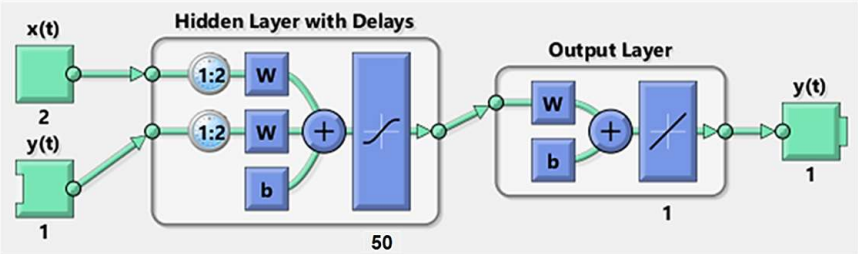


Figure 6. NARX model of ANN.

3. Simulation Results and Analysis

In the present section, graphical and numerical results from the training of the ANN for signal recovery in the receiver, the testing of the already trained model, and analyses of the obtained results are presented. The training and testing processes are carried out using simulation data in the MATLAB (R2023a) environment.

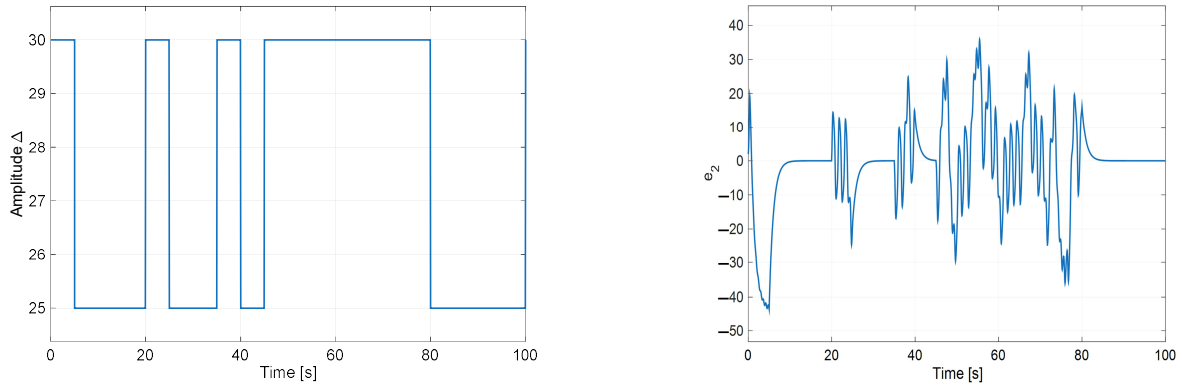
3.1. Training of NARX Model of ANN

For the training of the NARX model of the ANN, a simulation scheme has been developed in the MATLAB/Simulink environment, implementing an identical synchronization scheme between two Lorenz chaotic systems, which has already been described in detail in the preceding sections. The simulation has a duration of 100 s with a fixed step size of 0.001, whereby data sequences recorded in arrays of size 1×1.10^5 are obtained, with the entire set of values being used. As shown in Figure 6, the time delay of the NARX model is equal to 2, and the stopping criteria for the training process are as follows: reaching a gradient value of 1×10^{-7}, six out of six validation checks, or 1000 training epochs. In the present case, the stopping condition related to the validation checks is satisfied. The input data are normalized using min–max normalization. A standard value of 42 is used as the random seed in order to ensure reproducibility of both the network initialization and the training process. The training data for the ANN are taken from the variable e_2 of the mismatch vector, which is supplied as the external series $x(t)$, while the information signal is used as the main series $y(t)$.

The NARX model of the ANN used is of the form presented in Figure 6 and is created and trained in open-loop form. Open-loop (single-step) training is more efficient than closed-loop (multi-step) training. The open loop allows the correct past outputs to be fed to the network while it is being trained to produce the correct current outputs. After

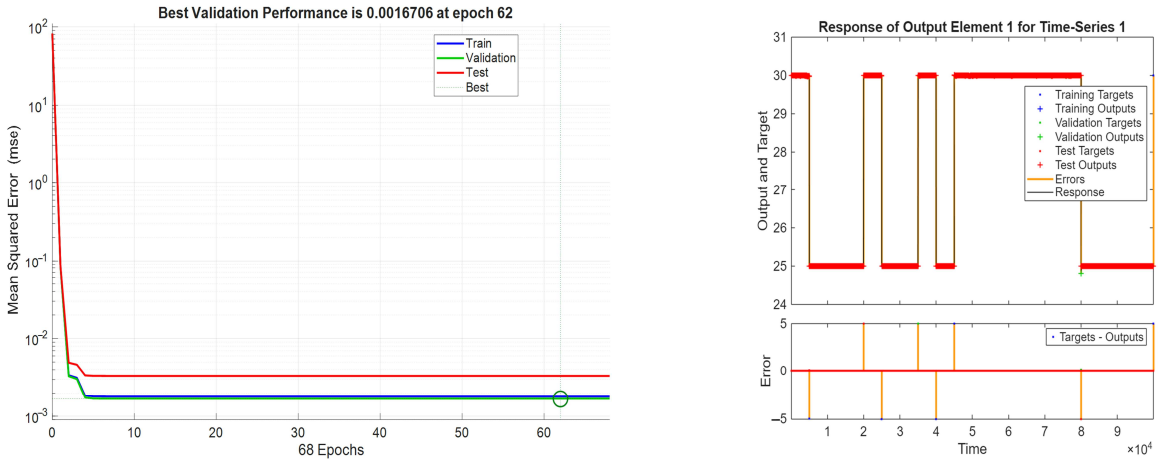
training, the network can be converted into closed-loop form or any other form required by the application.

Figure 7 presents the graphs of the signals used for the training of the ANN, while Figure 8 presents the graphical results of the training process.



(**a**) (**b**)

Figure 7. Training signals: (**a**) information signal; (**b**) signal at the receiver after synchronization.



(**a**) (**b**)

Figure 8. Graphical results from the training of the ANN: (**a**) performance; (**b**) response of the output element.

As can be seen, during training, an MSE value of 0.00167 is achieved after 62 training epochs, upon reaching the validation criterion. The achieved correlation (Regression R-value) between the output and the response for the test sample is 0.9997.

3.2. Testing of the Trained ANN

A drawback of this type of neural network is that training can be performed using a numerical sequence of arbitrary length, but not using several different sequences. The use of several different sequences increases the size of the matrix supplied to the vector $\mathbf{x}(t)$. For this reason, the ANN trained in this manner is tested with 10 other randomly generated digital information sequences and their corresponding numerical sequences for the error function e_2.

Figure 9 shows the information test sequences, which are shifted relative to one another for better visibility of the graph. Table 1 presents the numerical results for the MSE and the correlation for each digital sequence.

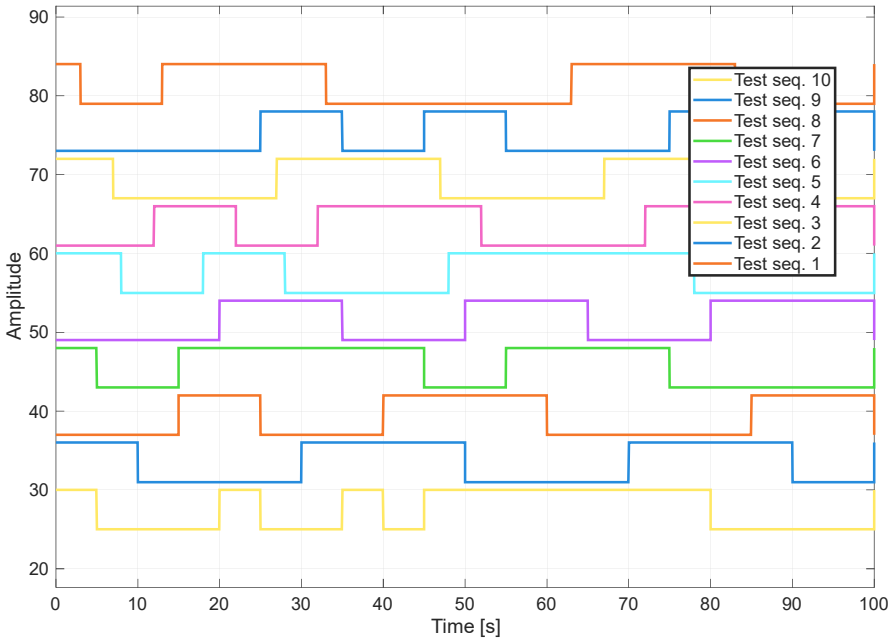


Figure 9. Test information sequences with randomly generated transitions between the levels.

Table 1. Numerical results for 10 randomly generated information sequences.

Information Sequence	MSE	Regression R-Value
Test sequence 1	0.0023	0.9998
Test sequence 2	0.0021	0.9998
Test sequence 3	0.0021	0.9998
Test sequence 4	0.0015	0.9999
Test sequence 5	0.0015	0.9999
Test sequence 6	0.0038	0.9997
Test sequence 7	0.0015	0.9999
Test sequence 8	0.0015	0.9999
Test sequence 9	0.0015	0.9999
Test sequence 10	0.0037	0.9997

3.3. Analysis

The feeding of a chaotic signal into a NARX model of an ANN leads not merely to smoothing or filtering, but to the recognition of the hidden dynamic structure of the useful signal and the suppression of components that are not compatible with that signal, owing to the context provided by past values. In this way, an estimate of the hidden (information) signal is obtained, which constitutes a form of signal reconstruction. The presence of an approximation element in fact leads to the dynamic nonlinear identification of a process from which the recovered signal is obtained. Filtering in the NARX model can compensate for slight temporal deformations or local stretching in time, such as that caused by the transient process of synchronization, something that ordinary filters would handle with difficulty, whereas NARX captures the dynamic form rather than only the frequency dependencies.

From the considerations presented above, it may be concluded that the obtained processing of the received signal is the so-called dynamic nonlinear signal reconstruction through input–output temporal alignment. The trained model captures the low-dimensional structure of the information signal and recognizes the local temporal pattern rather than individual points, thereby allowing recovery even when individual points are severely distorted. Despite the seemingly complex processes involved in this type of

encryption, the task is relatively easy to solve by means of this type of ANN, since the solutions obtained are consistent with the learned dynamics, whereas the other chaotic deviations are rejected. The differences in duration caused by the transient process of synchronization, which constitute the main problem, are absorbed, since pointwise coincidence is not sought; instead, a sequence compatible with the learned mode of behavior is sought.

The training results confirm this, as the achieved performance is sufficient for the reconstruction of such types of signals with a relatively small number of training epochs. Figure 8b clearly shows the high degree of overlap between the output of the ANN and the training sequence. The error plot shows how the transient process is almost entirely absorbed, with an error of only a single sample, comparable in amplitude, being observed when the levels of the digital signal change; moreover, the value follows the direction of the level change, which, if desired, can easily be corrected.

When the trained NARX model is tested, the same behavior is observed, with the average MSE over the ten test sequences being 0.00215 and the correlation being 0.9998, which is sufficient for the purposes of signal recovery.

4. Conclusions

The article proposes an approach to solving the problem of information recovery after the application of the chaotic switching method in the encryption of digital signals. The current state of the problem is described in detail, and the main issues arising in coherent CSK with the use of chaotic synchronization are defined. By using a NARX model of an ANN, significant advantages have been achieved, and the accuracy and precision of the recovery of the information sequence have been improved.

The designed ANN has been trained and tested using simulation data from a model implemented in the MATLAB/Simulink environment. From the tests performed, it is evident that the neural network has been well trained, while in the tests average MSE values on the order of 0.002 and R-value values of 0.9998 have been achieved. The results show that the use of an ANN in the reconstruction of the information sequence in the receiver after the application of the chaotic switching method and subsequent chaotic synchronization is an effective option providing a high degree of information protection.

Author Contributions: Conceptualization, H.S. and G.M.; methodology, H.S. and G.M.; software, H.S. and G.M.; validation, H.S. and G.M.; formal analysis, H.S. and G.M.; investigation, H.S. and G.M.; resources, H.S. and G.M.; data curation, H.S. and G.M.; writing—original draft preparation, H.S. and G.M.; writing—review and editing, H.S. and G.M.; visualization, H.S. and G.M.; supervision, H.S. and G.M.; project administration, H.S. and G.M.; funding acquisition, H.S. and G.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by University Center for Research and Technology at the Technical University of Gabrovo, project SRP 2026-22 (НИП 2026-22) "Research on intelligent methods, architectures and technologies for data protection in communication networks".

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tse, C.; Lau, F. *Chaos-Based Digital Communication Systems. Operating Principles, Analysis Methods and Performance Evaluation*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2003.

2. Gao, S.; Wu, R.; Iu, H.H.-C.; Erkan, U.; Cao, Y.; Li, Q.; Toktas, A.; Mou, J. Chaos-based video encryption techniques: A review. *Comput. Sci. Rev.* **2025**, *58*, 100816. [CrossRef]
3. He, Z.; Sayadi, H. AI in Chaos: Adaptive and Secure Communication Via Deep Reinforcement Learning and Moving Target Defense. *IEEE Access* **2025**, *13*, 199971–200000. [CrossRef]
4. Zheng, T.; Wang, K.; Yang, X.; Bian, C.; Li, W.; Yu, J. Frequency-time domain masking and digital encryption system for DSM-based fiber-wireless integrated system. *Opt. Fiber Technol.* **2024**, *88*, 104020. [CrossRef]
5. Bowen, Z.; Liu, L. Chaos-based image encryption: Review, application, and challenges. *Mathematics* **2023**, *11*, 2585. [CrossRef]
6. Lawnik, M.; Moysis, L.; Volos, C. Chaos-Based Cryptography: Text Encryption Using Image Algorithms. *Electronics* **2022**, *11*, 3156. [CrossRef]
7. El-Mowafy, M.A.; Gharghory, S.M.; Abo-Elsoud, M.A.; Obayya, M.; Allah, M.I.F. Chaos based encryption technique for compressed H264/AVC videos. *IEEE Access* **2022**, *10*, 124002–124016. [CrossRef]
8. Haridas, T.; S.D., U.; G., V.; Krishnan, M.S.; Muni, S.S. Chaos-based audio encryption: Efficacy of 2D and 3D hyperchaotic systems. *Frankl. Open* **2024**, *8*, 100158. [CrossRef]
9. BenMarak, O.; Anis, N.; Sadok, E. A security evaluation of Chaos Attribute-based Access Control (ABAC) for Cloud Computing. In *Proceeding of the International Conference on Advanced Information Networking and Applications*; Springer Nature: Cham, Switzerland, 2024.
10. Fu, Y.; Yu, Q.; Li, H. Design of a Differential Chaotic Shift Keying Communication System Based on Noise Reduction with Orthogonal Double Bit Rate. *Appl. Sci.* **2024**, *14*, 10723. [CrossRef]
11. Zhang, G.; Shun, S. A noncoherent chaotic communication system with multidimensional index modulation based on cyclic permutation grouping. *Digit. Signal Process.* **2024**, *155*, 104749. [CrossRef]
12. Yu, B.; Yang, H.; Jia, Y.; Liao, H.; Li, X. A Short Reference Differential Chaos Shift Keying Cooperative Communication System Based on Modified Code Index Modulation. *Entropy* **2025**, *27*, 562. [CrossRef] [PubMed]
13. Ma, H.; Fang, Y.; Chen, P.; Li, Y. Reconfigurable intelligent surface-aided M-ary FM-DCSK system: A new design for noncoherent chaos-based communication. *IEEE Trans. Veh. Technol.* **2022**, *72*, 4829–4843. [CrossRef]
14. Martinez-Gost, M.; Pérez-Neira, A.; Lagunas, M. Predictive Demodulation for Chaotic Communications. *arXiv* **2024**, arXiv:2409.06630.
15. Li, Z.; Wang, H.; Ji, Y. Hardware fingerprint construction of optical transmitters based on permutation entropy spectrum of chaos for secure authentication. *Opt. Laser Technol.* **2024**, *171*, 109947. [CrossRef]
16. Yang, H.; Tang, W.K.S.; Chen, G.; Jiang, G.-P. Multi-carrier chaos shift keying: System design and performance analysis. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2017**, *64*, 2182–2194. [CrossRef]
17. Tam, M.; Francis, C.; Tse Chi, K. *Digital Communications with Chaos: Multiple Access Techniques and Performance*; Elsevier: Amsterdam, The Netherlands, 2010.
18. Soujeri, E.; Kaddoum, G.; Herceg, M. Design of an initial condition-index chaos shift keying modulation. *Electron. Lett.* **2018**, *54*, 447–449. [CrossRef]
19. Ma, H.; Fang, Y.; Chen, P.; Mumtaz, S.; Li, Y. A novel differential chaos shift keying scheme with multidimensional index modulation. *IEEE Trans. Wirel. Commun.* **2022**, *22*, 237–256. [CrossRef]
20. Capligns, F.; Babajans, R.; Cirjulina, D.; Kolosovs, D.; Litvinenko, A. Frequency-Modulated Antipodal Chaos Shift Keying Chaotic Communication on Field Program Gate Array: Prototype Design and Performance Insights. *Appl. Sci.* **2025**, *15*, 1156. [CrossRef]
21. Tao, Y.; Fang, Y.; Ma, H.; Mumtaz, S.; Guizani, M. Multi-carrier DCSK with hybrid index modulation: A new perspective on frequency-index-aided chaotic communication. *IEEE Trans. Commun.* **2022**, *70*, 3760–3773. [CrossRef]
22. Chen, H.; Chen, P.; Wang, S.; Lai, S.; Chen, R. Reference-modulated PI-DCSK: A new efficient chaotic permutation index modulation scheme. *IEEE Trans. Veh. Technol.* **2022**, *71*, 9663–9673. [CrossRef]
23. Hameed, A.; Fadhil, S. A Novel Multi-Leaf Codebook Design for Reliable Sparse Code Multiple Access Differential Chaos Shift Keying System. *Phys. Commun.* **2025**, *73*, 102910. [CrossRef]
24. Zhang, G.; Yongqi, G.; Xinyu, X. A High-Reliability Dual-Mode M-ary Differential Chaos Shift Keying System with Index Modulation. *Digit. Signal Process.* **2025**, *166*, 105388. [CrossRef]
25. Hameed, A.; Fadhil, S.H. A novel code index modulation for an efficient sparse code multiple access differential chaos shift keying system. *AEU-Int. J. Electron. Commun.* **2025**, *202*, 155987. [CrossRef]
26. He, L.; Xiong, X.; Li, C. A novel differential chaos shift keying system based on joint time slot and code index of carrier phase modulation. *Digit. Signal Process.* **2025**, *156*, 104803. [CrossRef]
27. Zhang, G.; Hu, Y.; Chen, X.; Pei, Y. Denoising-enhanced differential chaos shift keying with joint dual orthogonal codes and time-frequency index modulation. *Chaos Solitons Fractals* **2025**, *197*, 116475. [CrossRef]
28. He, L.; Xiong, X.; Guo, Y. Design and analysis of a novel differential chaos shift keying system with joint three-dimensional index modulation. *Chaos Solitons Fractals* **2024**, *189*, 115609. [CrossRef]

29. He, L.; Hu, Y.; Chen, X. Design and Performance Analysis of High-Data-Rate Multi-Carrier Three-Dimensional Index Modulation Quadrature Chaos Shift Keying System. *Digit. Signal Process.* **2025**, *167*, 105429. [CrossRef]
30. Cirjulina, D.; Babajans, R.; Kolosovs, D. Design Particularities of Quadrature Chaos Shift Keying Communication System with Enhanced Noise Immunity for IoT Applications. *Entropy* **2025**, *27*, 296. [CrossRef] [PubMed]
31. Gao, Z.; Ma, Z.; Wu, S.; Gao, H.; Wang, A.; Fu, S.; Li, Z.; Qin, Y.; Wang, Y. Physical secure key distribution based on chaotic self-carrier phase modulation and time-delayed shift keying of synchronized optical chaos. *Opt. Express* **2022**, *30*, 23953–23966. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.