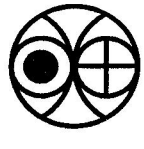
PRL TN-80-2001

PRL Technical Note

Application of Chaotic Dynamics to Communications through Synchronization

R.E. AMRITKAR AND D.R. KULKARNI

JULY 2001



Physical Research Laboratory
Navrangpura, Ahmedabad 380009

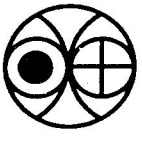
PRL TN-80-2001

PRL Technical Note

Application of Chaotic Dynamics to Communications through Synchronization

R.E. AMRITKAR AND D.R. KULKARNI

JULY 2001



Physical Research Laboratory
Navrangpura, Ahmedabad 380009

Application of Chaotic Dynamics to Communications through Synchronization

R. E. Amritkar and D. R. Kulkarni

Physical Research Laboratory, Navarangpura, Ahmedabad 380 009

ABSTRACT

Various methods of communications based on synchronization of two identical chaotic systems are briefly discussed. The method that uses the synchronization of active-passive decomposition of a chaotic system is found to be good. In this feasibility report we have applied the method to communicate three computer generated and two experimental time series signals using different chaotic systems and their combinations. The merits of communication using this method are studied in terms of shape of the transmitted signal, extent of the masking of the signal, errors in the recovered signal and spectra of original and recovered signals. In general it is found that masking of the signal is quite effective and the accuracy of the recovered signal is very high. It is, however, observed that the signal of short length consisting of sharp kinks in the data requires additional smoothing to be masked effectively. Combinations of chaotic systems are used to generate hyperchaotic transmitted signal to carry the information signal. It is expected that they would be difficult to decode and hence would lead to more secure communications but unfortunately they also have relatively low accuracy of the recovered signal. We have also examined the effect of additive noise and variation of parameters of chaotic systems on the accuracy of the recovered signal.

1 Introduction

It is now well established [1, 2, 3, 4, 5] that chaotic signals generated by dissipitive nonlinear system have potential applications to communications. Since chaotic signals are typically broadband, noise-like, and difficult to predict, they are particularly suitable for secure communication (cryptography). Chaotic signals can be specially useful as carriers for information bearing waveforms to be transmitted.

In methods of communication based on the property of synchronization [1] the actual communication of desired signal is implemented in two ways. The first approach [2, 3] is based on signal masking in which a small amplitude analog message is just added to a relatively large amplitude chaotic signal at the transmitter. Such systems are known as chaotic signal masking systems. In the second approach [2, 4] the digital signal in the form of bit sequence is used to modulate one of the transmitter parameters as the chaotic system evolves in time. These systems are known as chaotic modulation systems. In both the cases one of the variables of the transmitter system is used to drive the chaotic system at the receiver end. The actual information bearing waveform can be recovered at the receiver using the principle of synchronization. The process of synchronization essentially enables us to remove the carrier signal from the transmitted signal so that the information signal can be extracted at the receiver end. It can be shown [1] that two identical low dimensional chaotic systems would, under certain condition, synchronize if one of the variables from the first system is used to drive the other. It may thus be noted that the chaotic systems employed at the transmitter and the receiver need to have identical dynamics with almost same parameters.

Another method of secure communication which is not based on the property of synchronization has been suggested by Abarbanel and Linsay [5]. It has been demonstrated that one can modulate the phase of a selected unstable periodic orbit (UPO) using the binary information signal so that it can be transmitted in an encoded fashion along the transmission channel. In general using UPOs for communications have number of advantages. Unfortunately, the coded message is easily cracked using local linear approximation to chaotic flows. Hence this method may not be very useful for secure communications and is not covered in this report.

The purpose of the present feasibility report is to briefly review some of the recent developments relating to the use of chaos in communications based mainly on synchronization. In Section 2 we review in brief some important methods of synchronization available in the literature. However, we do not cover all the methods of synchronization. Section 3 describes how these methods can be applied to communications and how they compare in terms of security and accuracy of the recovered signal. Amongst the methods of communications discussed above we have found that the one based on the active-passive decomposition gives better numerical results. We

have encoded various types of signals such as sinosidal, triangular, rectangular, electroencephalegraph (EEG) signal, annual sunspot numbers etc using this method and the results are presented in section 4. Section 5 details the study of how the recovered signal is affected due to introduction of noise in the transmitted signal as well as the variation of parameters of receiver chaotic systems. Some attempts to decode the signal using different methods are broadly discussed in section 6. Section 7 describes in brief some considerations about implementing the system in hardware. In the concluding section 8 we summarize the pros and cons of various methods and chaotic systems related to secure communications in the light of numerical results.

2 Methods of synchronization

Two chaotic signals are said to synchronize if they show identical values as a function of time. In general, the two signals will synchronize only asymptotically. Several methods of synchronization of two chaotic systems have been proposed. Here, we briefly outline three methods of synchronization of two identical systems.

2.1 Self-synchronizing chaotic systems

Pecora and Carrol (PC) [1] were the first to report that chaotic systems can possess self synchronizing property. A chaotic system is self synchronizing if it can be decomposed into two subsystems: drive system and a stable response subsystem and when drive signal from one system is fed into another identical system then the response subsystem of the second system synchronizes with that of the first system. Pecora and Carrol have shown that synchronization occurs if all the lyapunov exponents of the response subsystem are negative. The property of synchronization would be robust if any initial condition of response subsystem and/or any perturbation in the drive signal almost always lead to synchronization.

Consider the well known Lorenz system, A, as given below.

$$\begin{aligned} \dot{X} &= \sigma(Y - X) \\ \dot{Y} &= \rho X - Y - XZ \\ \dot{Z} &= -\beta Z + XY \end{aligned} \tag{1}$$

where σ, ρ and β are the parameters.

Divide Lorenz system into two subsystems, Y as the drive subsystem and (X, Z) as the response subsystem. Consider a system B, identical to system A, defined by (X_1, Y_1, Z_1). To drive this system by Y we set $Y_1 = Y$. The evolution of the response sybsystem of B is given by

$$\dot{X}_1 = \sigma(Y - X_1)$$

$$\dot{Z}_1 = -\beta Z_1 + X_1 Y \tag{2}$$

When the Lyapunov exponents of the response subsystem (X, Z) are all negative then the response subsystem (2) converges and asymptotically synchronizes with the system A, i.e.

$$|X_1 - X| \text{ and } |Z_1 - Z| \to 0 \text{ as } t \to \infty$$

The Lyapunov exponents are determined by using the Jacobian matrix corresponding to the differences ($\Delta X = X_1 - X, \Delta Z = Z_1 - Z$).

$$J = \begin{pmatrix} -\sigma & 0 \\ Y & -\beta \end{pmatrix}. \tag{3}$$

There is another way of dividing Lorenz system, namely system $C = (X_2, Y_2, Z_2)$ with $X_2 = X$ as the drive and (Y_2, Z_2) as the stable response subsystems. The response subsystem obeys the equations,

$$\begin{aligned} \dot{Y}_2 &= \rho X - Y_2 - X Z_2 \\ \dot{Z}_2 &= -\beta Z_2 + X Y_2 \end{aligned} \tag{4}$$

The variables (Y_2, Z_2) synchronize with (Y, Z) when driven by X.

The remaining way of dividing Lorenz system, namely Z as the drive and (X, Y) as the response subsystems does not lead to a stable response system since one of the response subsystem Lyapunov exponent turns out to be almost zero.

It is interesting to recognize that the two response subsystems, B and C, defined above (Eqs. (2) and (4)) can be combined to produce a full dimensional response system that is structurally similar to the drive system (1). Specifically the input signal $X(t)$ from the drive system (1) drives the response subsystem (Y_2, Z_2) to produce the output $Y_2(t)$. The signal $Y_2(t)$ is subsequently used to drive the response subsystem (X_1, Z_1) to generate $X_1(t)$. Now the subsystem (Y_2, Z_2) synchronizes to drive the system to produce $Y_2(t)$ equal to $Y(t)$. This implies that the subsystem (X_1, Z_1) is actually driven by the signal $Y(t)$ and hence eventually synchronizes with the drive system (1) producing $X_1(t)$ equal to $X(t)$. Thus we get a single three-dimensional response system which is similar to the drive system (1). We will make use of this fact while applying the method to communication in Section 3.

2.2 Synchronization using adaptive control

John and Amritkar (JA) [4] have introduced another method for synchronizing the evolution of a non-linear and chaotic system to a desired unstable trajectory through adaptive control. The desired unstable trajectory may be a chaotic orbit or an unstable periodic orbit. For the implementation of this method it is assumed that one or more of the system parameters are available for control.

The chaotic system that generates the desired unstable orbit is called a target system or a response system. One of the variables of the drive system is used to vary a selected parameter of the system which then drives the response system. When synchronization takes place, all the variables of the response system as well as the selected conrolled parameter synchronize to those of the drive system. The response system consists of equations of the drive system supplemented by the additional equation governing the time evolution of the selected control parameter.

The method is illustrated using the Lorenz system given by Eq. (1) as a drive system. The response system is controlled by the parameter ρ of the Lorenz system and the drive variable Y. The evolution of the response system is given by

$$\begin{aligned} \dot{X}_1 &= \sigma(Y_1 - X_1) \\ \dot{Y}_1 &= \rho X_1 - Y_1 - X_1 Z_1 \\ \dot{Z}_1 &= -\beta Z_1 + X_1 Y_1 \\ \dot{\rho} &= -\epsilon(Y_1 - Y)\ \mathrm{sgn}(\frac{d\dot{Y}_1}{d\rho}) - \delta(\rho - \rho^*) \end{aligned} \tag{5}$$

where ϵ is the stiffness constant, δ is the damping constant and the function $\mathrm{sgn}(x)$ denotes the sign of x.

It can be seen from Eq. (5) that the parameter ρ changes depending on

- The difference between the system output variable $Y_1(t)$ and the corresponding variable $Y(t)$ of the desired orbit.
- The difference between the evolving parameter ρ and its value ρ^* for the desired orbit.

The range of values of constants ϵ and δ for which synchronization is possible are determined by studying the Lyapunov exponents of the response system. The condition for synchronization with the desired trajectory is that all Lyapunov exponents of the response system (5) are negative. The critical values of the stiffness constant ϵ and damping constants δ can be determined by the condition that the largrest Lyapunov exponent is zero. The synchronization is found to be quite robust as per the criterion given in the previous section.

2.3 Synchronization by active-passive decomposition

In this method [3] of synchronization we consider an arbitrary N-dimensional chaotic autonomous dynamical system

$$\dot{\mathbf{Z}} = \mathbf{F}(\mathbf{Z}) \tag{6}$$

The goal is to rewrite this system as a non-autonomous system that possesses certain synchronization properties. We thus write

$$\dot{\mathbf{X}} = \mathbf{f}(\mathbf{X}, \mathbf{S}) \tag{7}$$

where $\mathbf{X}$ is the new state vector corresponding to $\mathbf{Z}$ and $\mathbf{S}$ is some vector value function of time given by

$$\mathbf{S} = \mathbf{h}(\mathbf{X}) \text{ or } \dot{\mathbf{S}} = \mathbf{h}(\mathbf{X}, \mathbf{S}) \tag{8}$$

The pair of functions $\mathbf{f}$ and $\mathbf{h}$ constitute a decomposition of the original vector $\mathbf{F}$. The crucial point of this decomposition is that for suitable choice of the function $\mathbf{h}$ any system

$$\dot{\mathbf{Y}} = \mathbf{f}(\mathbf{Y}, \mathbf{S}) \tag{9}$$

which is given by the same non-autonomous vector field $\mathbf{f}$, the same driving $\mathbf{S}$, but different variables $\mathbf{Y}$ synchronizes with original system (7). In other words, the components of the vectors $\mathbf{X}$ and $\mathbf{Y}$ asymptotically approach each other;

$$|X_i - Y_i| \to 0 \text{ as } T \to \infty$$

The synchronization of the pair of identical systems (7) and (9) occurs if all conditional lyapunov exponents of non-autonomous system (7) are negative. In this case the system (7) is a passive system and the decomposition is called active-passive decomposition (APD) of the original dynamical system (6). Though $\mathbf{S}$ is assumed to be vector valued in the above formulation for the sake of generality, in practice for the application to communications, it is often considered as a scalar valued function. As an illustration we give below the APD of well known Rossler system given by

$$\begin{aligned} \dot{Z}_1 &= 2 + Z_1(Z_2 - 4) \\ \dot{Z}_2 &= -Z_1 - Z_3 \\ \dot{Z}_3 &= Z_2 + 0.45 Z_3 \end{aligned} \tag{10}$$

The passive part of the APD is

$$\begin{aligned} \dot{X}_1 &= 2 - 4X_1 + X_2^2 - sX_2 \\ \dot{X}_2 &= -X_2 - X_3 + s \\ \dot{X}_3 &= X_2 + 0.45 X_3 \end{aligned} \tag{11}$$

where the transmitted signal s can be written as

$$s = X_2 - X_1 \tag{12}$$

and the component corresponding to Eqn. (9) is given by

$$\begin{aligned} \dot{Y}_1 &= 2 - 4Y_1 + Y_2^2 - sY_2 \\ \dot{Y}_2 &= -Y_2 - Y_3 + s \\ \dot{Y}_3 &= Y_2 + 0.45 Y_3. \end{aligned} \tag{13}$$

It is worth pointing out that in the APD method the system (11) is actually driven by the transmitted signal s which is a function of the variables of the original system. Further according to the PC method [1] the Rossler system (10) can have only one response subsystem (X_2, X_3) for synchronization, while in the APD method there can be number of different functional forms of $\mathbf{h}$ for which synchronization can be possible. Thus the APD method can be considered to provide a more general framework compared to the PC method.

3 Application to communications

We will now see how the synchronization techniques described in the previous section can be applied to communications.

3.1 Communication using PC method

Cuoma and Oppenheim [2] have shown that the PC method of synchronization can be used in a communication system which may be either a chaotic signal masking system or a chaotic modulation system. They have implemented these systems in analog circuitry based on the Lorenz equations.

3.1.1 Signal masking system

In signal masking scheme the transmitter generates a chaotic signal $X(t)$. The message bearing signal $m(t)$ is then added to $X(t)$. The actual signal that is transmitted is

$$s(t) = X(t) + m(t). \tag{14}$$

It is assumed that for masking, the power level of $m(t)$ should be significantly lower than that of $X(t)$. The dynamical system implemented at the receiver is also a full three dimensional Lorenz system given by

$$\begin{aligned} \dot{X}_r &= \sigma(Y_r - X_r) \\ \dot{Y}_r &= \rho s(t) - Y_r - s(t)Z_r \\ \dot{Z}_r &= s(t)Y_r - \beta Z_r \end{aligned} \tag{15}$$

The transmitted signal $s(t)$ drives the subsystem (Y_r, Z_r), while Y_r drives X_r. The receiver tries to synchronizes with the transmitter, and thus $X_r(t)$ tries to synchronize with $X(t)$ and consequently the message signal $m(t)$ can be recovered as

$$\hat{m}(t) = s(t) - X_r(t). \tag{16}$$

It may noted that the message signal $m(t)$ is not a part of the dynamics of the transmitter system. It is also obvious that for large power of the message signal $m(t)$, the transmitted signal $s(t)$ considerably deviates from the original Lorenz signal $X(t)$ leading to poor synchronization and thereby proportionately inexact recovery of the message signal $m(t)$.

3.1.2 Chaotic modulation system

In chaotic modulation system Cuoma and Oppenheim have again used the Lorenz system both at the transmitter and the receiver ends as before. The idea is to modulate a transmitter parameter dynamically using the message bearing digital signal $m(t)$ in the form of bits and to transmit the chaotic drive signal. For example a binary signal which looks like a square wave can produce variation in the transmitter parameter say β such that for zero bit $\beta(0) = 4.0$ and for one bit $\beta(1) = 4.4$. At the receiver the parameter modulation will produce a synchronization error between the received drive signal $X(t)$ and the receiver's regenerated drive signal $X_r(t)$. In fact the parameter modulation produces significant synchronization error during one-bit transmission and very little error during zeto-bit transmission. Using the synchronization error the modulation can be detected and the message signal $m(t)$ can be recovered. In this method also the synchronization depends on the extent of modulation of the transmitter parameter. For large modulation the method is likely to fail as the modulated parameter is not a part of the receiver dynamic system which works only with the unmodulated parameter β.

3.2 Communication using JA method

In the JA method [4] of synchronization applied to communications the parameter of the transmitter is again modulated by the binary information signal. In the specific case described by them the modulation of the transmitter parameter is produced by varying the parameter ρ of the Lorenz system between the values 28 and 28.5 corresponding to the bits 0 and 1 of the binary signal respectively. The drive signal is the variable Y of the Lorenz system. The response system at the receiver is the controlled chaotic system described by eq.(4) and is controlled by using the parameter $\rho = 28.0$. It may be noticed that unlike the PC method of chaotic modulation the time evolution of the parameter is embedded in the dynamics of the response system. As a result when the transmitter and the receiver synchronize, the controlled parameter ρ of the response system also gets synchronized with that of the transmitter along with other variables of the system. The plot of the deviation of the parameter ρ from its controlled value 28 against time clearly shows spike corresponding to binary 1. It is observed that the beginning of the spike precisely corresponds to the beginning of the binary 1 of the information signal, but the end of the binary 1 transmission can not be determined accurately. Though this method is better than the PC method

of chaotic modulation, it also tends to perform better only within a limited range of parameter variation.

3.3 Communication using APD method

Parlitz et al [3] have shown that the APD method of synchronization can be used to design a chaotic signal masking system. There are two methods to do so. The first one enables us to reconstruct the information exactly while the second one, called autosynchronization method, offers new features to design more robust communication system.

3.3.1 Exact reconstruction method

In this method the information signal m is included in the function h (see Eqs. (8) and (12)) describing the scalar signal s. If h is invertible with respect to m

$$m = h^{-1}(\mathbf{X}, s) \tag{17}$$

then the information recovered at the receiver

$$m_r = h^{-1}(\mathbf{Y}, s) \tag{18}$$

converges to the original information m if the transmitter ($\mathbf{X}$ system) and the receiver ($\mathbf{Y}$ system) synchronize. To demonstrate the method they have implemented the following decomposition of the Rossler system. The transmitter system (passive component) is

$$\begin{aligned} \dot{X}_1 &= 2 + X_1(X_2 - 4) \\ \dot{X}_2 &= -X_1 - X_3 \\ \dot{X}_3 &= X_2 - X_3 + s \end{aligned} \tag{19}$$

The transmitted signal is

$$s = 1.45X_3 + m \tag{20}$$

The receiver system is

$$\begin{aligned} \dot{Y}_1 &= 2 + Y_1(Y_2 - 4) \\ \dot{Y}_2 &= -Y_1 - Y_3 \\ \dot{Y}_3 &= Y_2 - Y_3 + s \end{aligned} \tag{21}$$

The recovered signal m_r can be obtained by

$$m_r = s - 1.45Y_3 \tag{22}$$

when the transmitter and the receiver synchronize.

3.3.2 Autosynchronization method of APD

In contrast to the above method the information signal m in this method is not included in the function h in this method. As a result the transmitted signal does not contain the information signal leading to more secure communication. The resulting communication system based on Rossler system would have following components. The transmitter system is

$$\begin{aligned} \dot{X}_1 &= 2 - 4X_1 + X_2^2 - sX_2 + m \\ \dot{X}_2 &= -X_2 - X_3 + s \\ \dot{X}_3 &= X_2 + 0.45X_3 \end{aligned} \tag{23}$$

The transmitted signal is

$$s = X_2 - X_1 \tag{24}$$

and the receiver system is

$$\begin{aligned} \dot{Y}_1 &= 2 - 4Y_1 + Y_2^2 - sY_2 + Y_4 \\ \dot{Y}_2 &= -Y_2 - Y_3 + s \\ \dot{Y}_3 &= Y_2 + 0.45Y_3 \end{aligned} \tag{25}$$

$$\dot{Y}_4 = a(s_r - s) \tag{26}$$

where $s_r = Y_2 - Y_1$, $m_r = Y_4$ and a is a free convergence parameter. It can be shown that the error $e_4 = Y_4 - m$ will be small if the information signal m changes slowly compared to the time scale of the error dynamics.

3.3.3 Cascading in the APD method

For secure communications it is desirable to use high dimensional chaotic carrier in order to make the decoding as difficult as possible. The transmitted signal in such systems would be hyperchaotic. In order to construct [3] systematically the high dimensional synchronizing systems the standard low dimensional systems with well-known dynamics are used as building blocks. These blocks which may consist of different systems or identical systems can be arranged in series (cascaded) or in parallel. The synchronization of the transmitter and the receiver is based on the mutual synchronization of low dimensional systems that constitute the building blocks.

If we want to construct say a 9-dimensional communication system one way is to have three identical Rossler systems in cascade both in the transmitter and the receiver systems. The transmitter system may look as follows.

$$\mathbf{f}_A(\mathbf{X}_A, \mathbf{S}_A) \rightarrow \mathbf{f}_B(\mathbf{X}_B, \mathbf{S}_B) \rightarrow \mathbf{f}_C(\mathbf{X}_C, \mathbf{S}_C), \tag{27}$$

where A, B and C are three systems used for cascading. The corresponding cascaded receiver system would be

$$\mathbf{f}_A(\mathbf{Y}_A, \hat{\mathbf{S}}_A) \leftarrow \mathbf{f}_B(\mathbf{Y}_B, \hat{\mathbf{S}}_B) \leftarrow \mathbf{f}_C(\mathbf{Y}_C, \mathbf{S}_C) \tag{28}$$

In order to have total synchronization all the pairs of the system

$$\begin{aligned} \mathbf{f}_A(\mathbf{Y}_A, \hat{\mathbf{S}}_A) &\rightarrow \mathbf{f_A}(\mathbf{X_A}, \mathbf{S_A}) \\ \mathbf{f}_B(\mathbf{Y}_B, \hat{\mathbf{S}}_B) &\rightarrow \mathbf{f_B}(\mathbf{X_B}, \mathbf{S_B}) \\ \mathbf{f}_C(\mathbf{Y}_C, \mathbf{S}_C) &\rightarrow \mathbf{f_C}(\mathbf{X_C}, \mathbf{S_C}) \end{aligned} \tag{29}$$

should synchronize so that the information signal could be recovered. It is also possible to have two different (non-identical) systems such as Lorenz and Rossler systems to form a six simensional parallel system [6].

The APD-based communication system is much superior to other methods dicussed earlier. In the communication system based on PC method the information is just added to a chaotic carrier but not injected into the dynamical system constituting the transmitter. In other words the receiver is driven by the sum of the chaotic signal and the information signal whereas the transmitter is just driven by the pure chaotic signal. Because of this slightly different drive signal the transmitter and the receiver systems do not synchronize exactly and the information signal can only be recovered with some error which vanishes in the limit $|m| \rightarrow 0$. Thus if one uses an information signal with small amplitude, the error will be reduced to that extent. However, if the information signal is too small in amplitude it is likely to be destroyed by noise in the transmission channel. Furthermore the method with too small signal amplitude is not very secure. It is possible to fit a nonlinear model to time series given by the transmitted signal s that now consists of low dimensional chaotic carrier (as m is very small). Using this model the information may then be extracted from s by method of nonlinear noise reduction.

In contrast it may be emphasized that in the APD-based communication the information signal is not just added to a chaotic carrier but also drives the dynamical system constituting the transmitter. It is thus difficult to decode the transmitted signal. Further with exact reconstruction the information signal can be exactly recovered without any error.The provision to build high dimensional system makes the method ideal for secure communications. In this report we have, therefore, focussed our attention on this method and employed it for communicating different types of signals. The details are presented in the next section.

4 Results

In this section we present the results of application of synchronization methods to communicate different types of signals. To be specific we have used five types of signals. The three of them are computer generated signals viz. i) sine waveform ii) triangular waveform and iii) rectangular waveform. The other two are real signals viz. i) annual sunspot series and ii) electroenceplalograph (EEG) signal of a normal human being. The relevant statistics of these signals is given in Table 1 to get the

quantitative feel for the data. It may be noted that both the real signals have high

Signal Type	Sample Size	Mean	St.Dev.	Minimum	Maximum
Sine	1000	0.0	0.7075	-1.0	1.0
Triangular	5000	0.5	0.2887	0.0	1.0
Rectangular	5000	0.5	0.5	0.0	1.0
Annual Sunspot Series	247	51.9421	41.6018	0.0	190.2
Human EEG	1024	-0.0048	4.7051	-13.3042	14.0773

Table 1: Statistics of Signals used in the Study

frequency sharp peaks in the data. As stated earlier we have used the APD method of synchronization for all calculations. The study is carried out using the following schemes.

1. Using the low-dimensional chaotic systems such as Rossler and Lorenz.
2. Examining the effect of smoothing the signal.
3. Using the hyper-chaotic system obtained by cascading identical Rossler systems.
4. Using the hyper-chaotic system obtained by combining the heterogeneous systems such as Rossler and Lorenz systems.
5. Studying the effect of noise on signal recovery.
6. Studying the effect of parameter variation on signal recovery.

The process of obtaining the transmitted signal for a given information signal is sometimes loosely termed as encoding the information signal and that of recovering the signal from the transmitted signal as decoding the signal. We use this terminology intermittantly in this section.

4.1 APD using Rossler and Lorenz systems

In this exercise we follow the method of exact reconstruction of the information signal in the framework of APD. We have noted earlier that this method enables us to recover the information signal i using Eqs. (22) or (33). bearing signal almost exactly from

the chaotic transmitted carrier waveform. For the Rossler system we use the active-passive decomposition as described by Eqs. (19) to (21). Similarly the APD scheme used for the Lorenz system is as follows. The transmitter is given by

$$\begin{aligned} \dot{X}_1 &= -10X_1 + s(t) \\ \dot{X}_2 &= 28X_1 - X_2 - X_1X_3 \\ \dot{X}_3 &= X_1X_2 - 2.6667X_3 \end{aligned} \tag{30}$$

The transmitted signal is

$$s(t) = 10X_2 + iX_3, \tag{31}$$

where i the information signal to be transmitted. The receiver is given by

$$\begin{aligned} \dot{Y}_1 &= -10Y_1 + s(t) \\ \dot{Y}_2 &= 28Y_1 - Y_2 - Y_1Y_2 \\ \dot{Y}_3 &= Y_1Y_2 - 2.6667Y_3 \end{aligned} \tag{32}$$

The recovered information signal is obtained as

$$i_R = (s(t) - 10Y_2)/Y_3. \tag{33}$$

In order to transmit the information signal i, we now solve Eqs. (19) or (30) numerically using some arbitrary initial initial condition $X(0) = V_1$. This gives us the signal $s(t)$ which is transmitted to the receiver. At the receiver end Eqs. (21) or (32) are solved numerically using some other arbitrary initial condition $Y(0) = V_2$. This allows us to recover the information signal using Eqs. (22) or (33). In general the initial conditions V_1 and V_2 are different and hence it takes some time before the transmitter and receiver systems get synchronized. During this time the recovered signal does not match with the corresponding segment of the information signal. In order to solve this problem it is necessary to pad the actual information signal with leading zeros or some random signal. It is worth mentioning here that in all our calculations we have used the padding signal to be zero. The length of this padding signal depends on the synchronization time. Let T_p denote the duration of this padding signal. This procedure ensures that before the information signal is recovered the transmitter and receiver systems are completely synchronized. However, due to this procedure the transmitted signal is often much longer than the actual information bearing signal.

Another important point worth noting for secure communication is that the amplitude range of the information signal should be much smaller (10% or less) than the range of the chaotic signal so as to mask the signal effectively. We, therefore, scale down the amplitude of the information signal keeping in view the amplitude range of the selected chaotic carrier. If the information signal is not sufficiently masked by the

chaotic carrier the spectral analysis of the transmitted signal may reveal the characteristic spectral features of the information signal which may be used to identify the same. We therefore compare the spectral contents of the actual signal, the corresponding transmitted signal and the recovered signal in all five types of signal studied here. Otherwise also it is often necessary, in practice, to scale down the amplitude of the information signal so as to make the system numerically stable. Too large an amplitude may set numerical instability in the solution of differential equation.

In our calculations we obtain the transmitted and the recovered signals for each type of information signal discussed above. We also evaluate the frequency contents of these signals. The goodness of the recovered signal is tested by calculating the error statistics for different synchronization timings. We present these results for the Rössler system. For Lorenz system the results are similar and hence only those pertaining to annual sunspot series are presented. It may be noted that for all the information signals the amplitude range used was one.

In Table 2 we give the error analysis of the recovered sine signal as the padding time T_p increases.

Padding Time,T_p	$\bar{e}$	σ_e	e_{min}	e_{max}
0	3.606	2.835	$0.381 * 10^{-2}$	9.597
5	0.253	$0.180 * 10^{-1}$	0.209	0.270
10	$0.366 * 10^{-2}$	$0.215 * 10^{-2}$	$0.267 * 10^{-5}$	$0.880 * 10^{-2}$
15	$0.298 * 10^{-3}$	$0.732 * 10^{-4}$	$0.170 * 10^{-3}$	$0.418 * 10^{-3}$
20	$0.406 * 10^{-4}$	$0.768 * 10^{-5}$	$0.263 * 10^{-4}$	$0.519 * 10^{-4}$
30	$0.113 * 10^{-6}$	$0.588 * 10^{-7}$	$0.253 * 10^{-9}$	$0.223 * 10^{-6}$

Table 2: Error Analysis of Recovered Sine Signal

It can be seen that the error in the recovered signal reduces as the padding time increases. Fig. 1 gives the plots of the actual sine signal, the corresponding transmitted signal and the recovered signal when the error is minimum (after the padding time $\approx$ 30 seconds in this case). The transmitted and the recovered signal are obtained by solving Eqs. 19, 20 and 21. Fig. 2 gives the spectral contents of the signals presented in Fig. 1.

It can be noted that the original sine signal could be recovered with great accuracy. Further the transmitted signal masks the sine wave and does not provide any clue to the identity of the signal. This can also be confirmed from Fig. 2. Similar results are

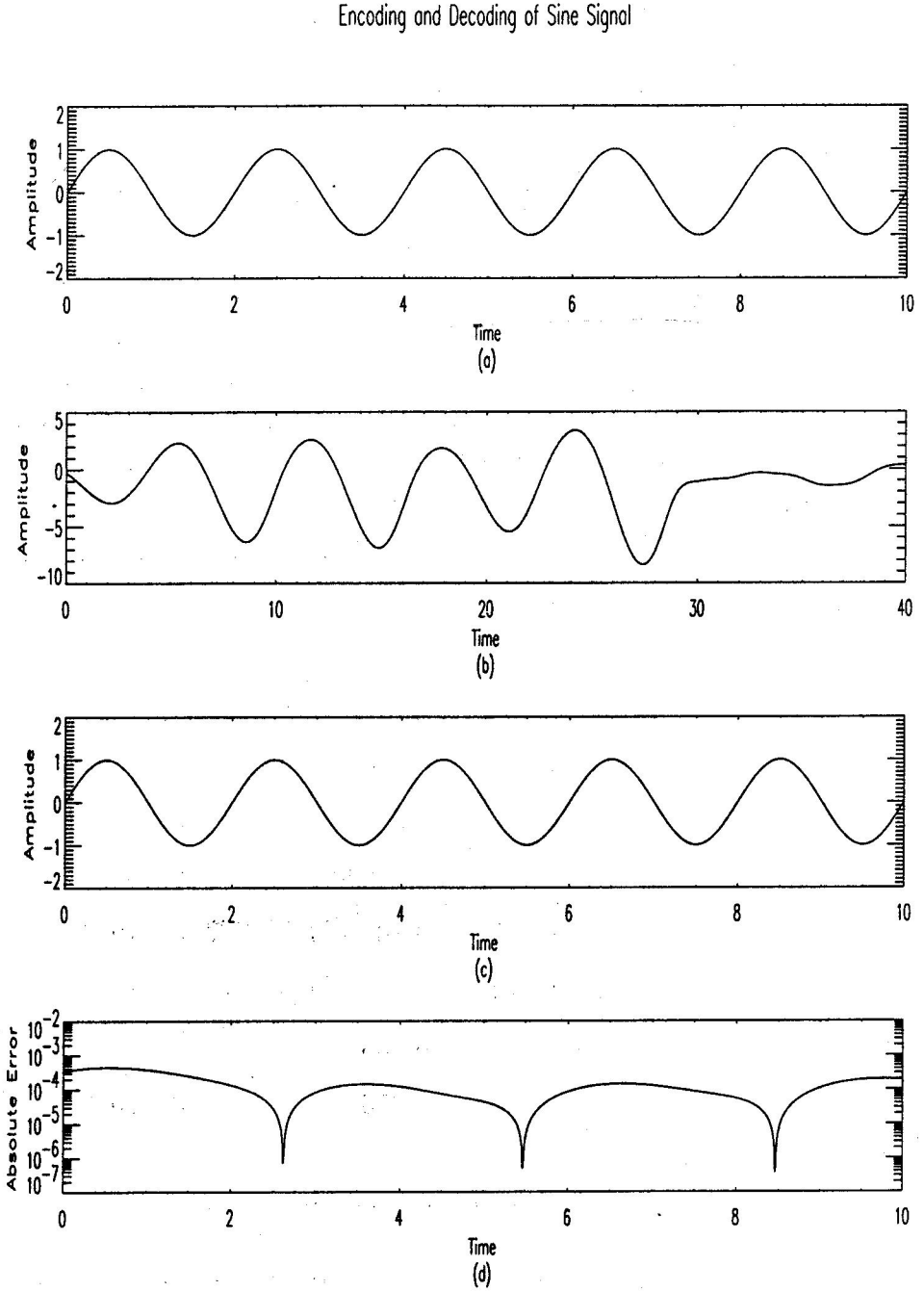


Figure 1: Encoding and decoding of Sine signal obtained using APD method with Rossler system. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padding part of the signal is not shown except in (b). One can notice change in behaviour of transmitted signal after the information signal is added (time 30 to 40 units in Fig.(b) above). This change can be made homegeneous by padding with identical copies of the same signal (or some other signal) from $t = 0$.

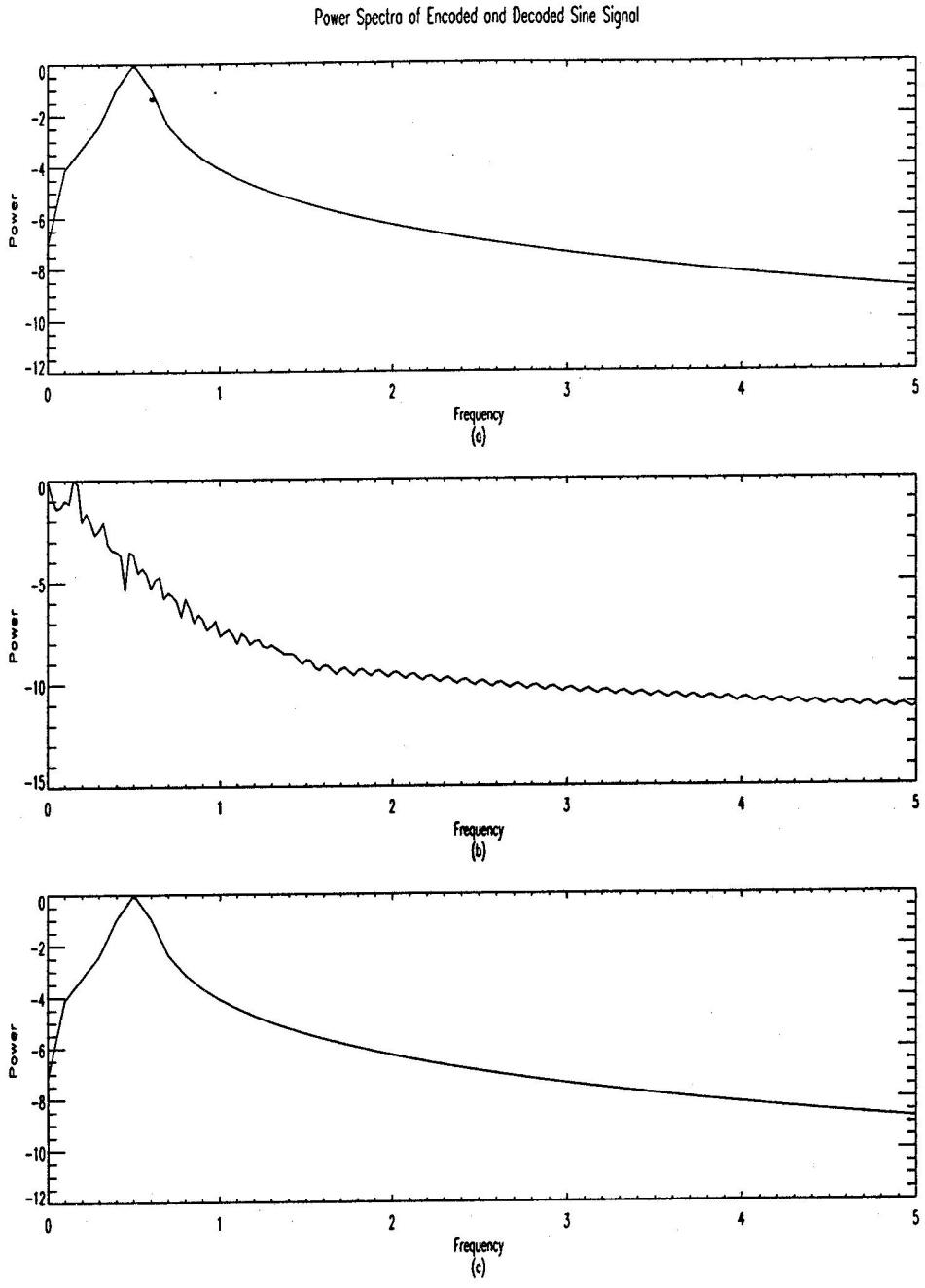


Figure 2: Power spectra of encoded and decoded sine signal obtained using APD method with Rossler system. a) the spectrum of original sine signal. b) the spectrum of transmitted sine signal. c) the spectrum of recovered sine signal.

obtained for the other computer generated signals viz. triangular signal (Fig. 3) and rectangular signal (see Fig. 4).

The results for the annual sunspot series are given in Fig. 5 and Fig. 6

and those for the EEG signal in Fig. 7 and Fig. 8. For these signals the accuracy of the recovered signals is not as high as those in the computer generated signals.

Similar results are obtained using Lorenz system [6] for all the information signals. The results for the annual sunspot series and EEG using the Lorenz system are given in Fig. 9 and Fig. 10 respectively.

4.2 Effect of smoothing the signal

We note that the annual sunspot series and EEG signals have sharp high frequency peaks in the data. Even after scaling down the amplitude the identity of the signal can not be completely masked in the transmitted signal. If we look at the transmitted signal one clearly finds the variation similar to the structure of the information signal. The effect is quite pronounced if the length of the signal is short. We, therefore, suggest that the signal be sampled with much higher frequency so that the transmitted signal is quite smooth. Additional points required for high frequency sampling can be obtained using cubic spline interpolation. We refer to this procedure as 'smoothing' in this report. The process of smoothing essentially increases the length of the signal which, in turn, gets superimposed on a much larger segment of the carrier chaotic signal. As the length of the signal increases, the sharp variations in the signal are merged in the oscillation of the chaotic signal. Consequently one finds the transmitted signal is smooth and does not show the identity of the information signal. In Fig. 11 we present the transmiited signal for annual sunspot series for different lengths. It can be seen that for the length 2000 one gets smooth transmitted signal.

4.3 Cascading identical Rossler systems

We have seen [3] earlier that cascading number of identical, low-dimensional systems gives rise to a high-dimensional chaotic carrier. The communication based on the high-dimensional chaotic system would be desirable as it would be more secure. Making use of cascading of three identical Rossler systems we have encoded and decoded the five information signals in the framework of APD. The APD scheme has the following components.

The transmitter is

$$\begin{aligned} \dot{X_1} &= 2 + X_1(X_2 - 4) \\ \dot{X_2} &= -X_1 - X_3 \\ \dot{X_3} &= X_2 + 0.45s \end{aligned} \tag{34}$$

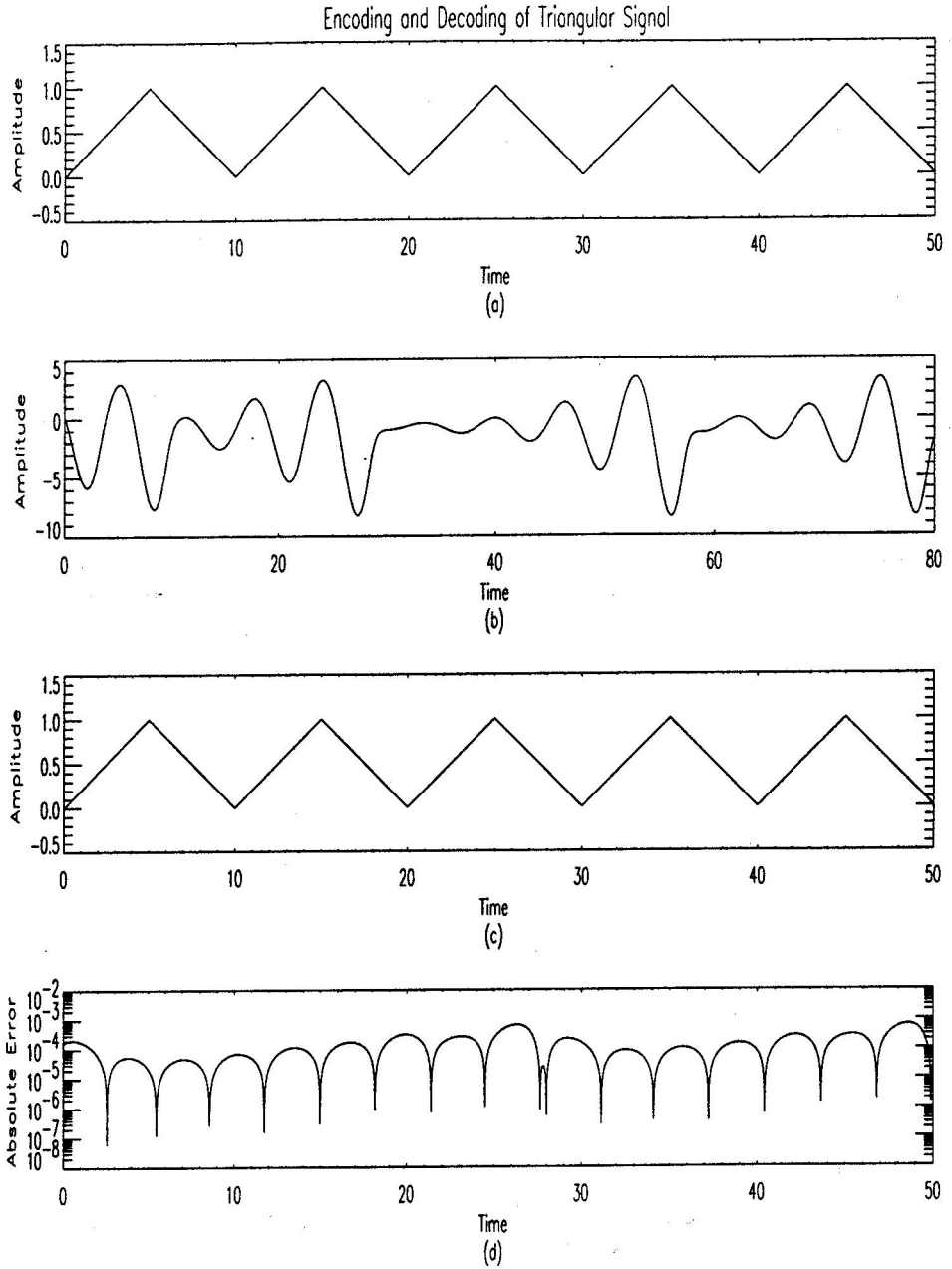


Figure 3: Encoding and decoding of triangular signal obtained using APD method with Rossler system. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padded part of the signal is not shown except in (b).

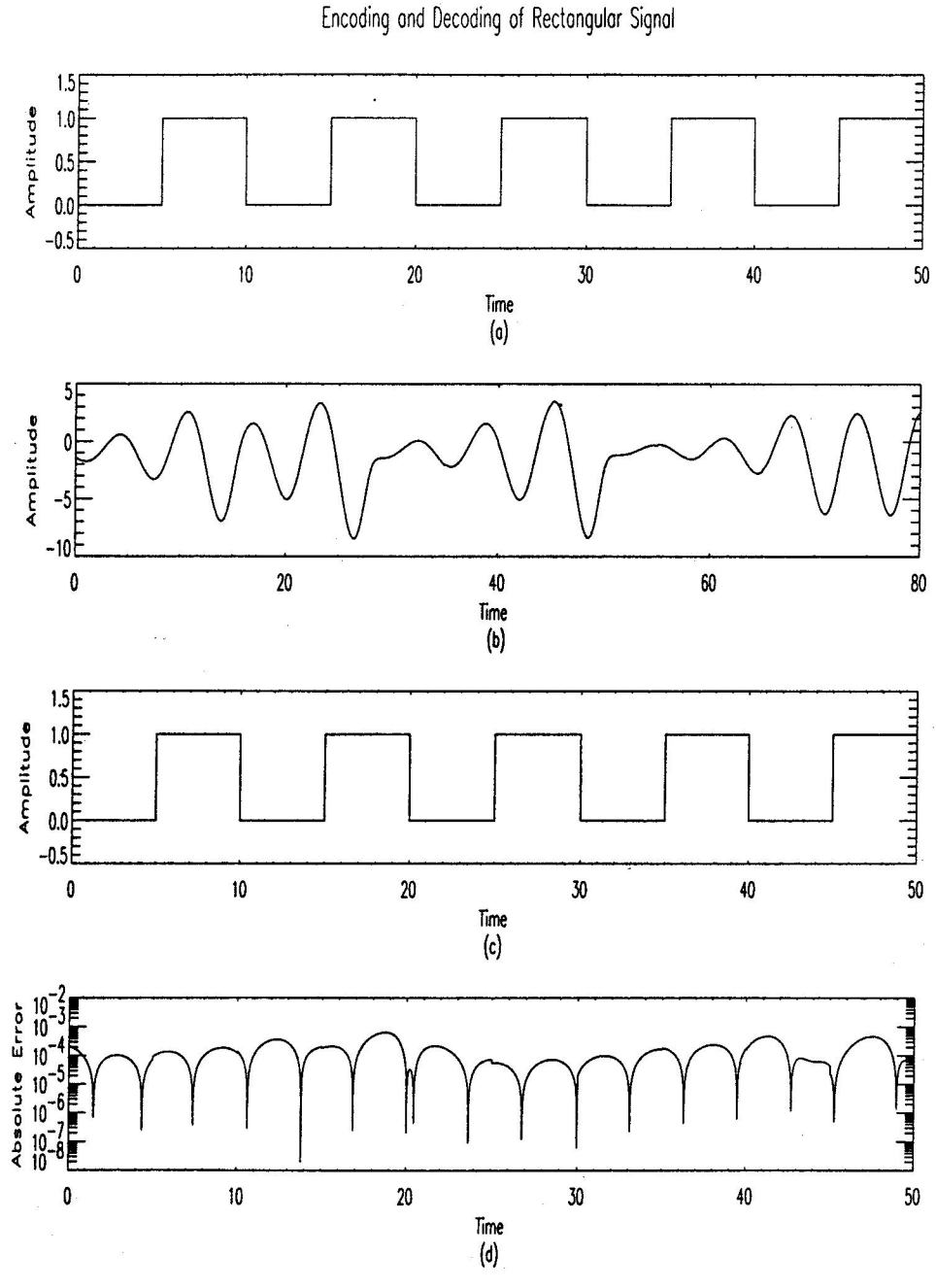


Figure 4: Encoding and decoding of rectangular signal obtained using the APD method with Rossler system. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padded part of the signal is not shown except in (b).

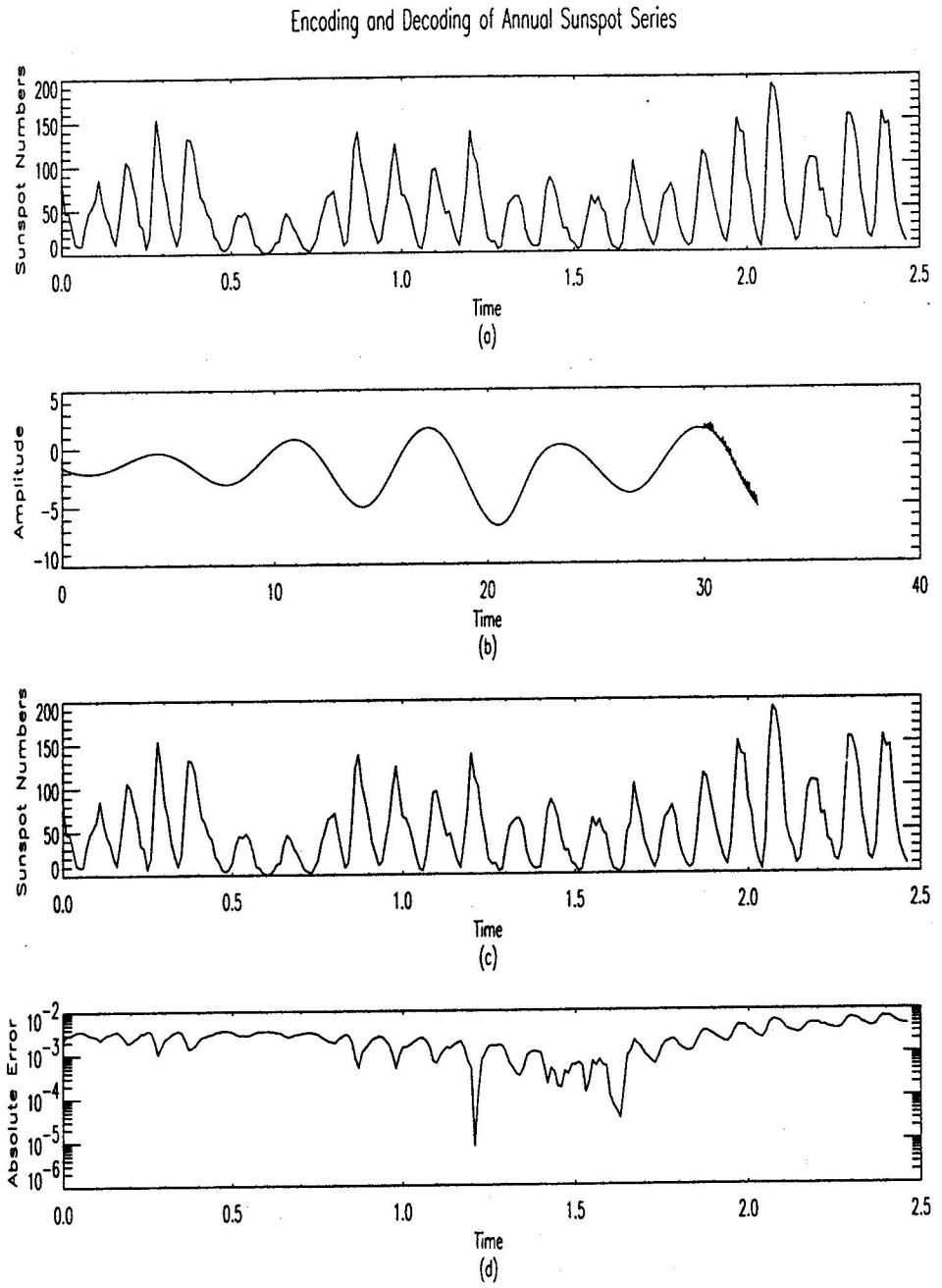


Figure 5: Encoding and Decoding of annual sunspot series using Rossler system in the APD method of communications. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padded part of the signal is not shown except in (b).

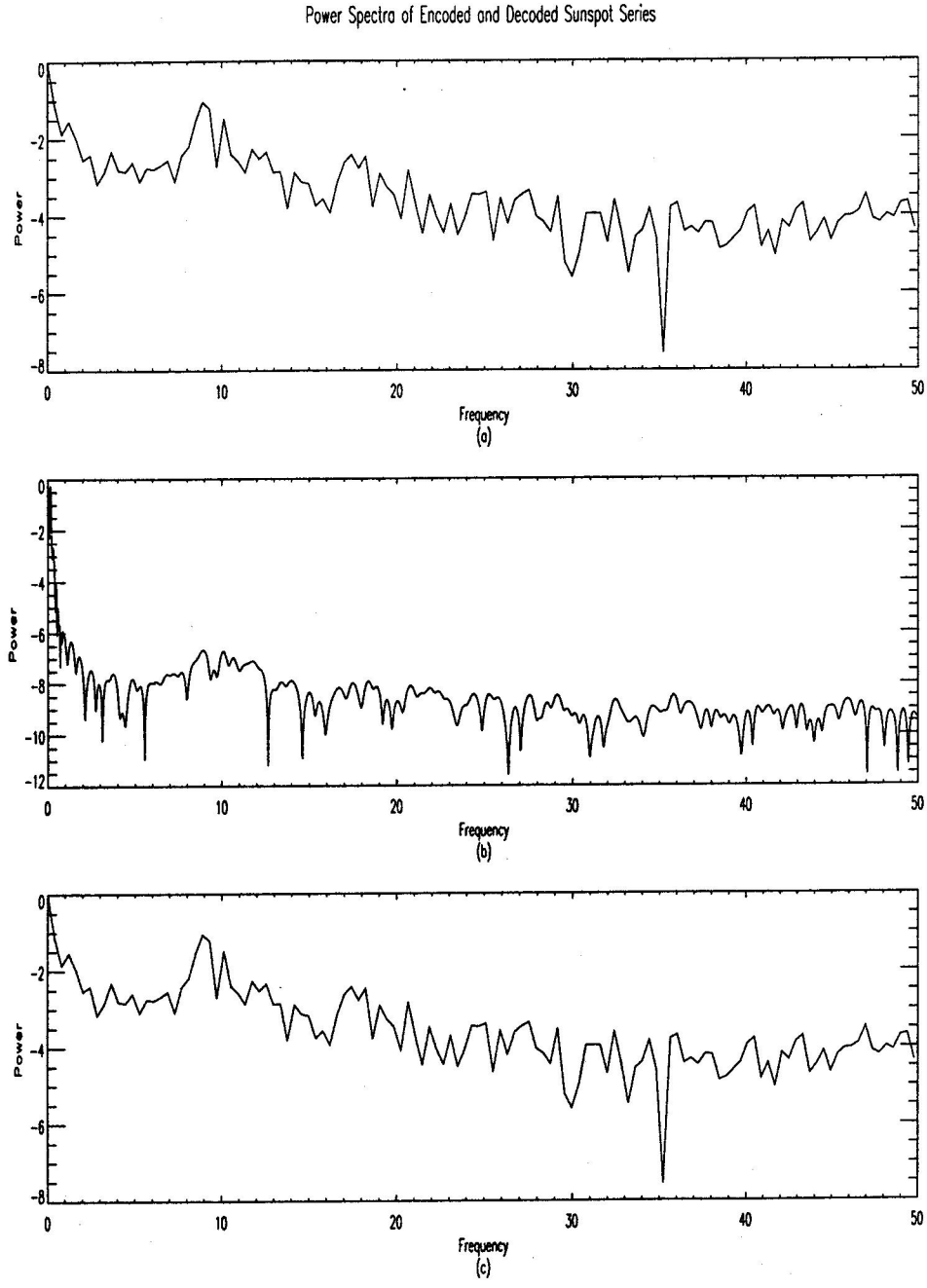


Figure 6: Power spectra of encoded and decoded annual sunspot series using Rossler system in the APD method of communications. a) the spectrum of the original series b) the spectrum of the transmitted signal c) the spectrum of the recovered signal.

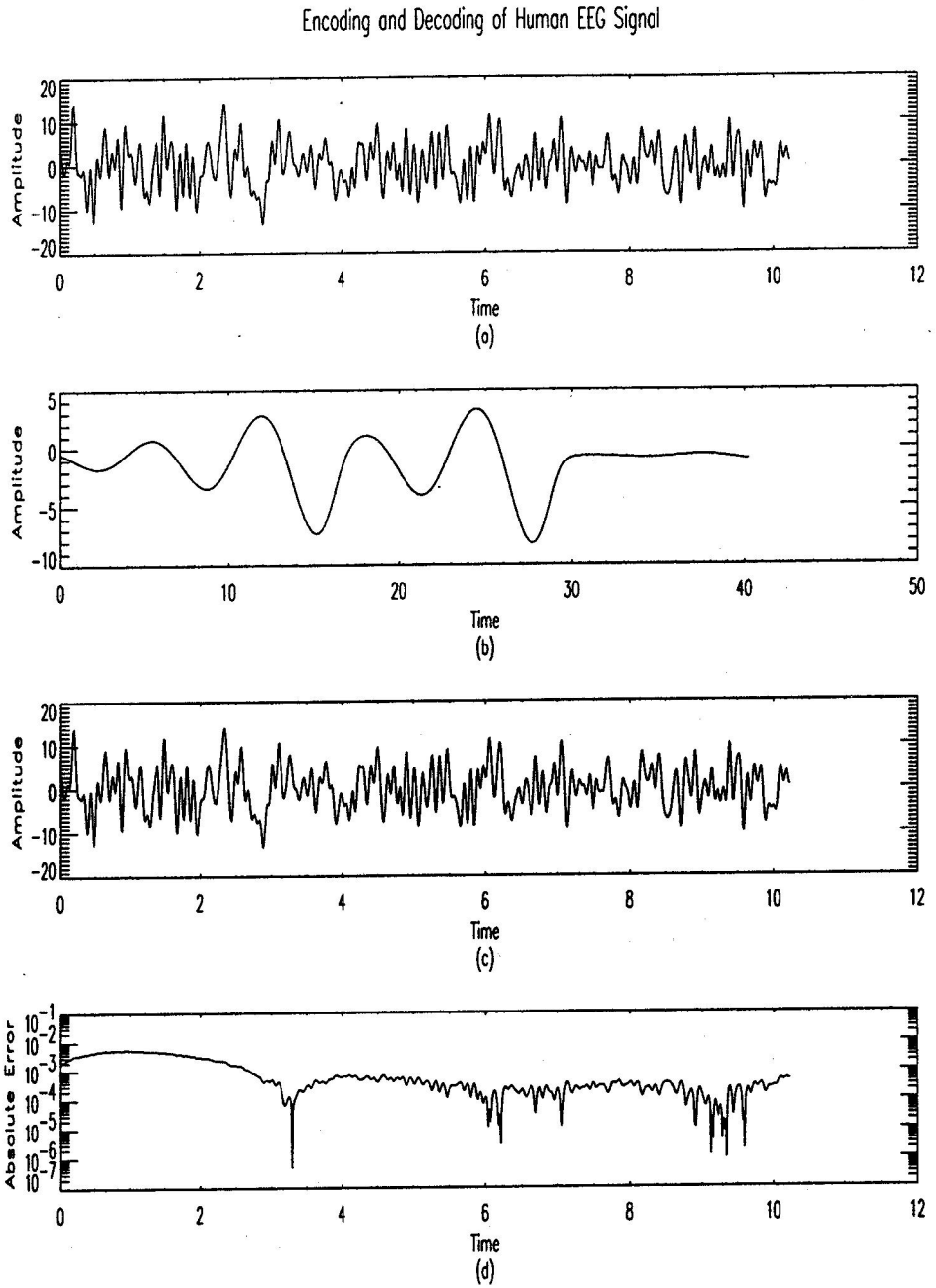


Figure 7: Encoding and Decoding of human EEG signal using Rossler system in the APD method of communications. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padded part of the signal is not shown except in (b).

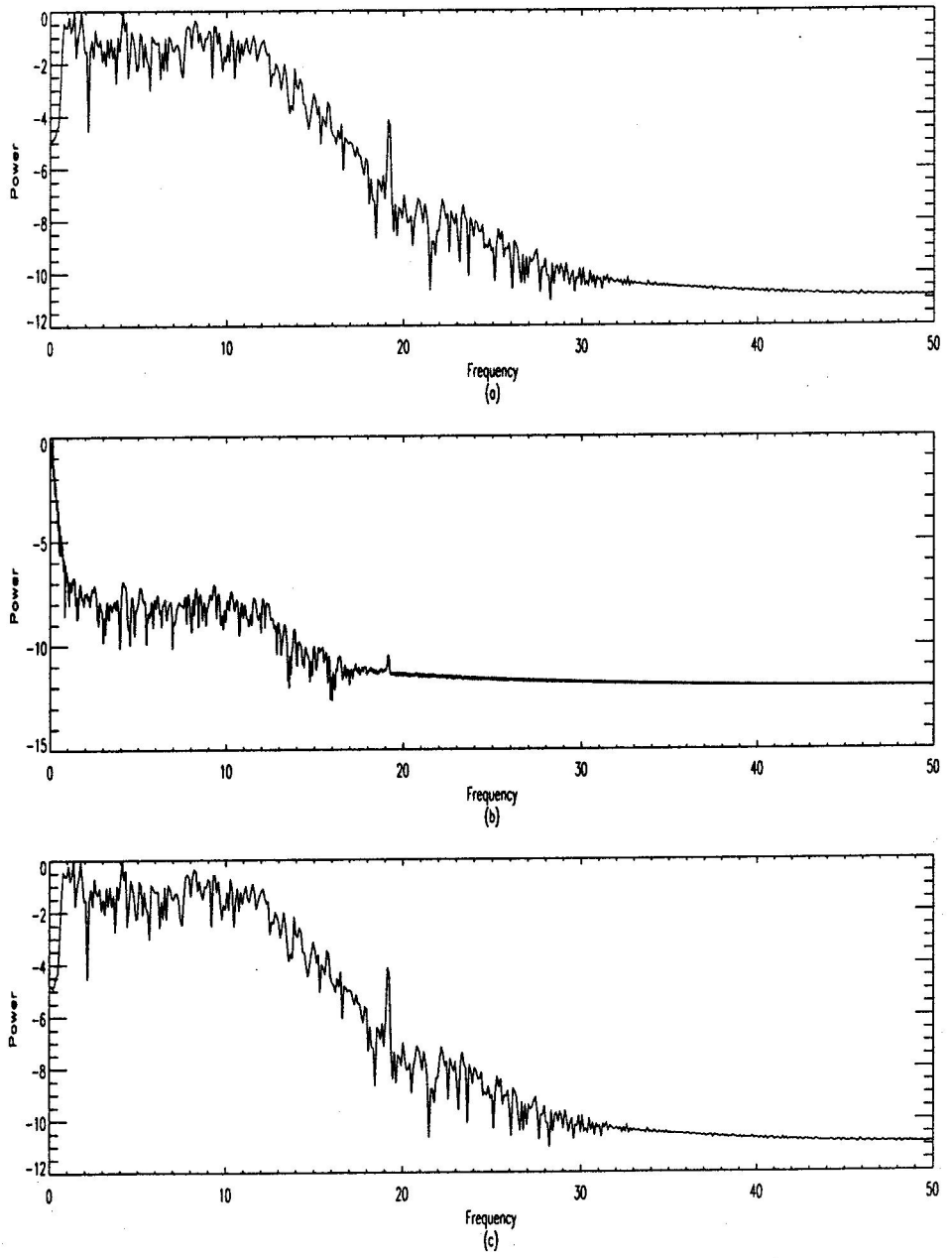


Figure 8: Power spectra of encoded and decoded human EEG signal using Rossler system in the APD method of communications. a) the spectrum of the original signal b) the spectrum of the transmitted signal c) the spectrum of the recovered signal.

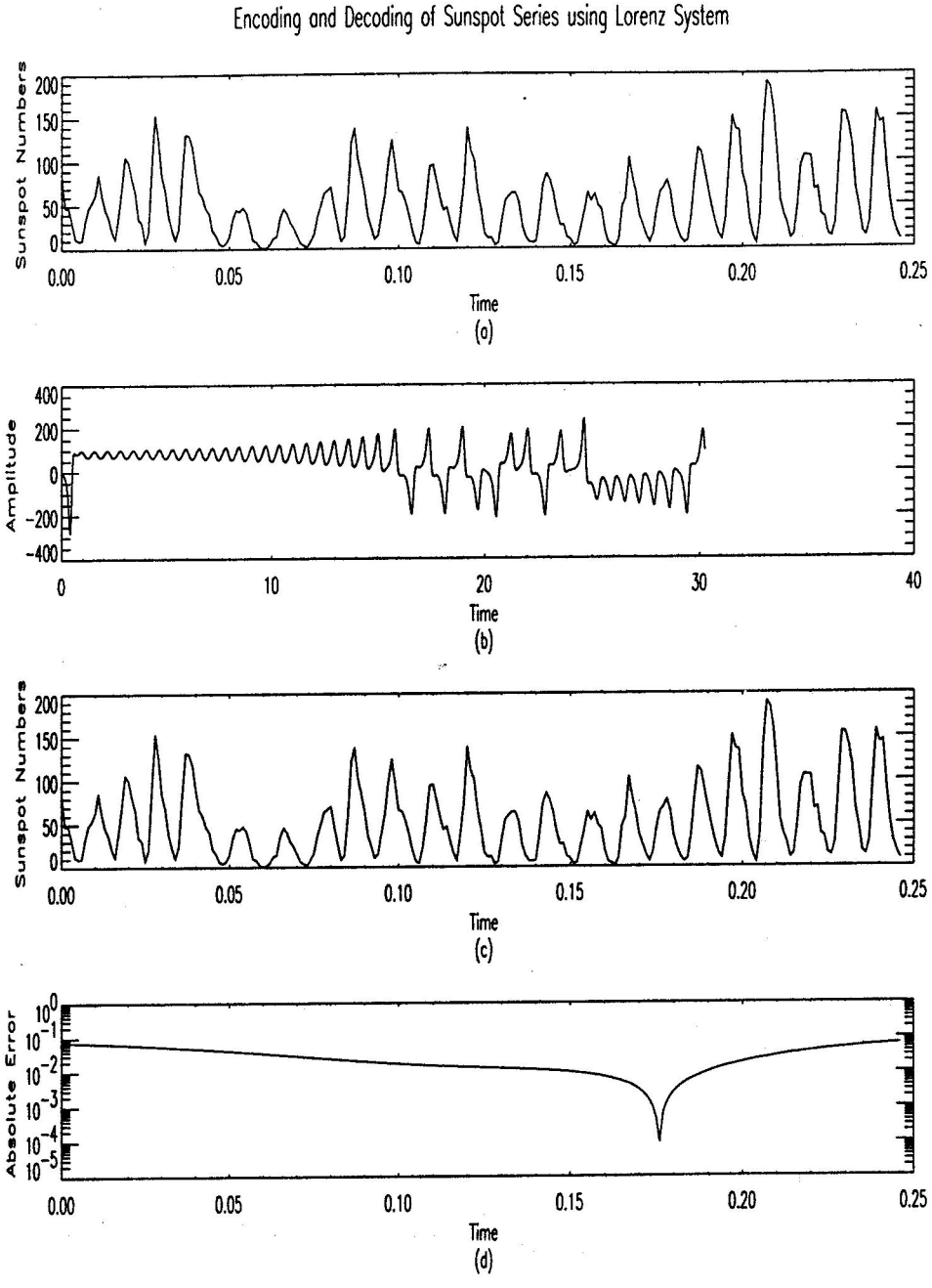


Figure 9: Encoding and Decoding of sunspot signal using Lorenz system in the APD method of communications. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padded part of the signal is not shown except in (b).

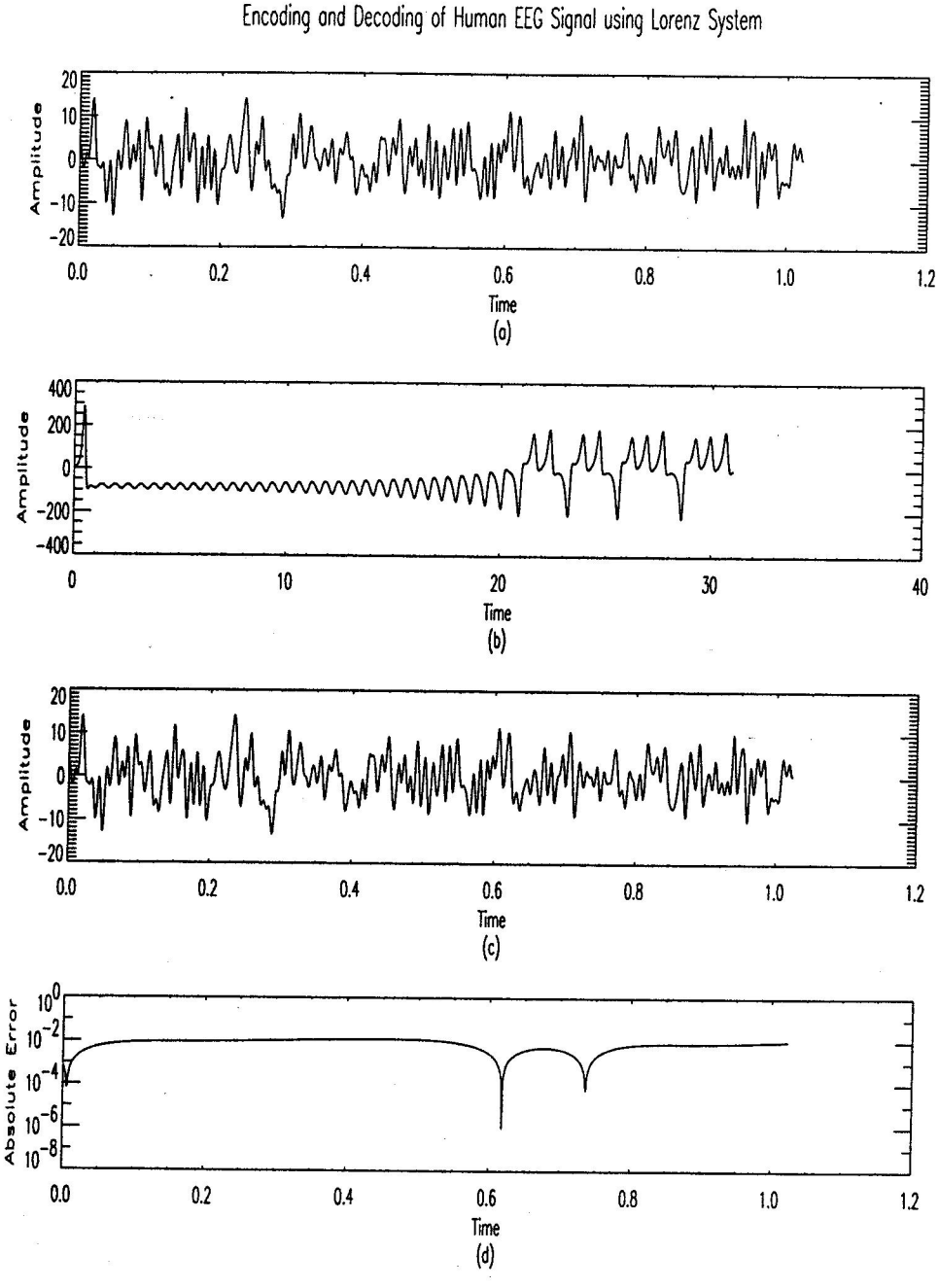


Figure 10: Encoding and Decoding of human EEG signal using Lorenz system in the APD method of communications. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padded part of the signal is not shown except in (b).

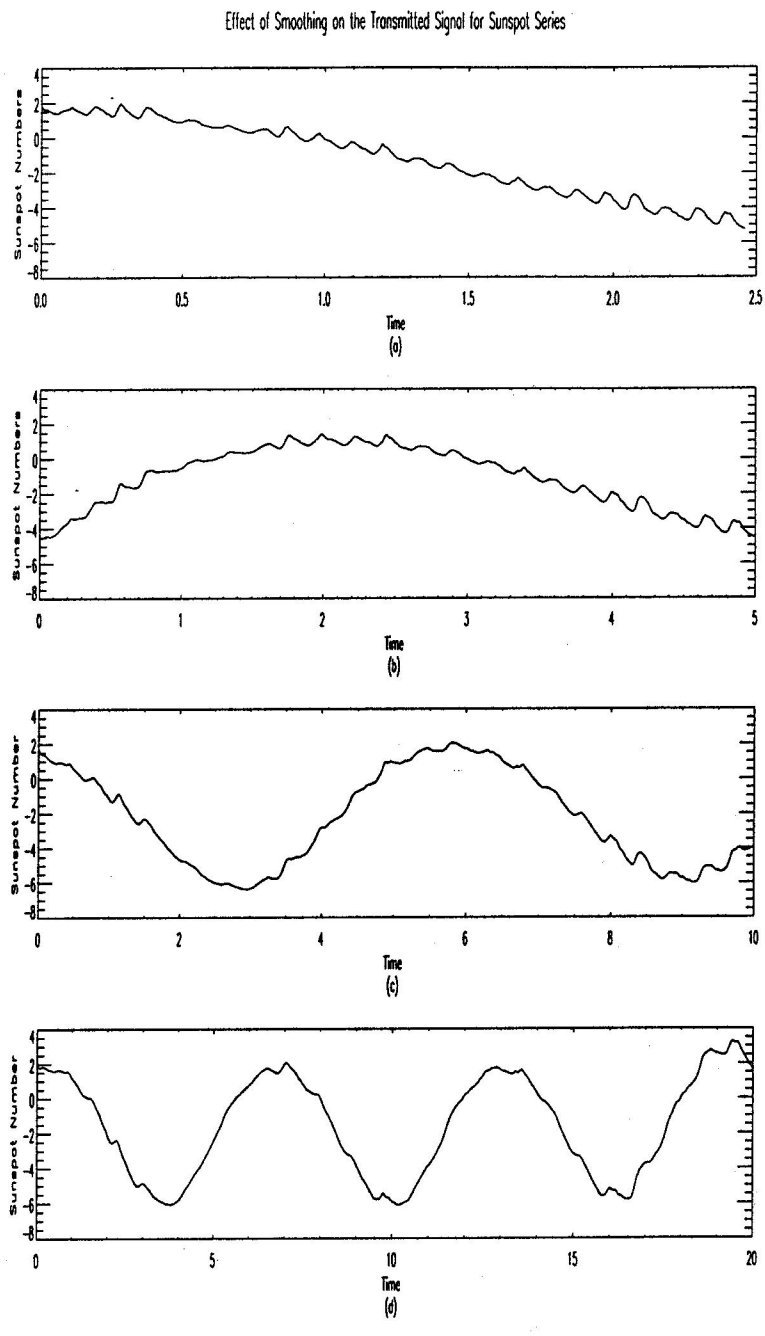


Figure 11: The Effect of smoothing on the transmitted sunspot series as the number of samples in the series is increased using interpolation. a) the original sample size 247 b) the sample size 500 c) the sample size 1000 d) the sample size 2000.

The transmitted signal for each stage of cascading is given by

$$s_{out} = X_3 + 0.25 s_{in}, \tag{35}$$

where s_{in} for the first stage is the actual information signal to be transmitted.

The receiver is

$$\begin{aligned} \dot{Y_1} &= 2 + Y_1(Y_2 - 4) \\ \dot{Y_2} &= -Y_1 - Y_3 \\ \dot{Y_3} &= Y_2 + 0.45s \end{aligned} \tag{36}$$

The recovered signal at the final stage of decoding would be

$$i_r = (s_{out} - Y_3)/0.25. \tag{37}$$

It may be noted that the input s_{in} at each stage is multiplied by a suitable factor (0.25 in this case) so as to keep its amplitude small enough so that the numerical instability in the solution is avoided.

The three stage cascading in the APD framework using the Rossler systems works very well for all the signals. Therefore we report here only the encoding and decoding of annual sunspot series to highlight some features of the scheme.

Since the message passes through number of stages while it is encoded, the synchronization time required is much higher than the one with single stage. Also the accuracy of the recovered signal decreases as the number of stages in the cascading increases. This is expected as the errors in one stage propagate to the next stage and thus, tend to be amplified. Fig. 12 shows results for annual sunspot series using three-stage APD with Rössler system.

It is observed that the procedure of smoothing usually required for a short signal containing sharp peaks for a single stage scheme is not necessary in cascading. As the signal passes through succesive stages it gets completely masked by the high-dimensional chaotic carrier. This is shown in Fig. 13. in which the transmitted signals for each stage are plotted omitting the padding time. The transmitted signal for the third stage does the masking reasonably well than the others.

4.4 Combining Heterogeneous Systems

It is also possible to combine two heterogeneous systems [6] in parallel to form a high-dimensional chaotic system to be used for communications. Here, we combine the Rossler system and the Lorenz system to produce a six-dimensional hyperchaotic system. The system can be used in the APD framework for a more secure communication.

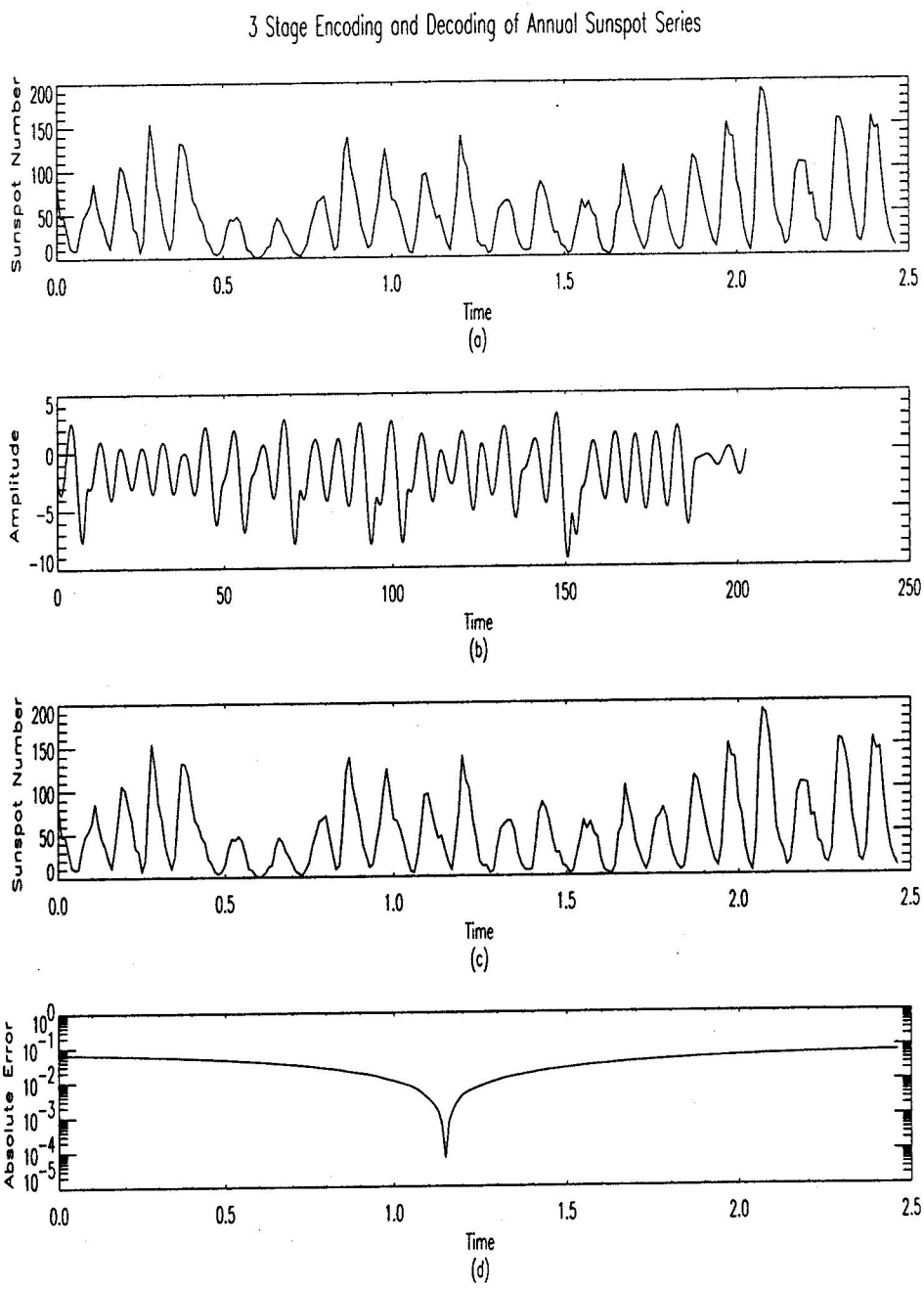


Figure 12: Encoding and Decoding of Sunspot Signal by cascading three Rossler systems in series in the APD method of communications. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padded part of the signal is not shown except in (b).

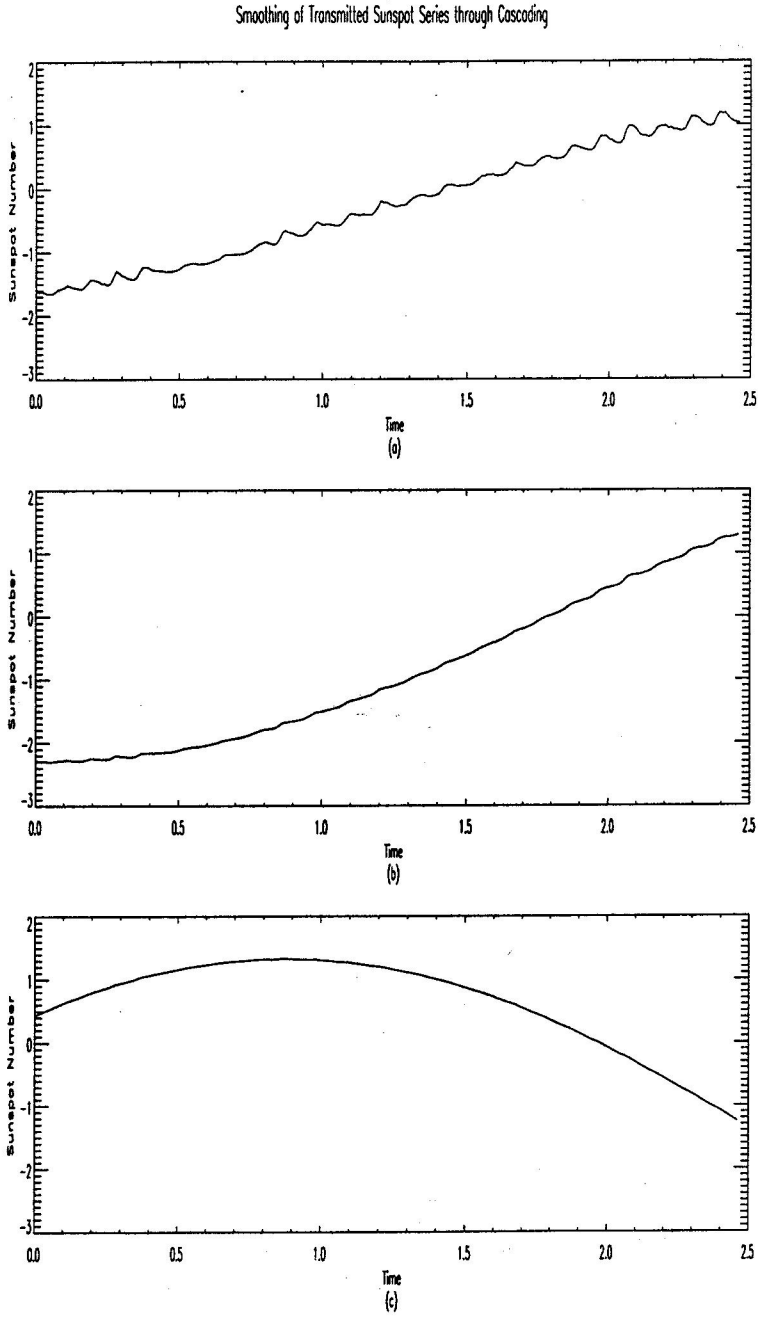


Figure 13: Smoothing of the transmitted sunspot series (without increasing its sample size by interpolation) as it passes through different stages of cascading. a) after stage one b) after stage two c) after stage three.

The transmitter of our communication model is given by

$$\begin{aligned}
\dot{X}_1 &= 2 + X_1(X_2 - 4) \\
\dot{X}_2 &= -X_1 - X_3 \\
\dot{X}_3 &= X_2 - 2.45X_3 + s_{aux} \\
\dot{X}_4 &= -10X_4 + s \\
\dot{X}_5 &= 28X_4 - X_5 - X_4X_6 \\
\dot{X}_6 &= X_4X_5 - 2.6667X_6
\end{aligned} \tag{38}$$

where $s_{aux} = i + 3X_3$ and

$$s = 10X_5 + 30s_{aux}/X_6 \tag{39}$$

inwhich i is the signal to be transmitted.

The receiver system is given by

$$\begin{aligned}
\dot{Y}_1 &= 2 + Y_1(Y_2 - 4) \\
\dot{Y}_2 &= -Y_1 - y_2 \\
\dot{Y}_3 &= Y_2 - 2.45Y_3 + S_{aux} \\
\dot{Y}_4 &= -10Y_4 + s \\
\dot{Y}_5 &= 28Y_4 - Y_5 - Y_4Y_6 \\
\dot{Y}_6 &= Y_4Y_5 - 2.6667Y_6
\end{aligned} \tag{40}$$

where $S_{aux} = (s - 10Y_5)Y_6/30$ and the recovered signal

$$i_R = S_{aux} - 3Y_3 \tag{41}$$

A few remarks regarding this scheme may be mentioned at this stage. It is observed that the transmitted signal is quite hyperchaotic. Further, as in the case of cascading identical systems, the synchronization time needed is quite large. The time step Δt to be used in the scheme to obtain the solution corresponds to that component system which, if solved independently, needs the smallest time step dt to get reasonably accurate solution. In fact we have observed that it is desirable to have the time step Δt smaller than dt. We also note that the transmitted signal of the parallel system does show the structure of the information signal and hence the signal needs to undergo the smoothing procedure.

The encoding and decoding of all the information signals are carried out using this scheme and the results are found to be very good. The typical results for the annual sunspot series are reported here. Fig. 14 displays the transmitted, recovered and error signals for the sunspot series.

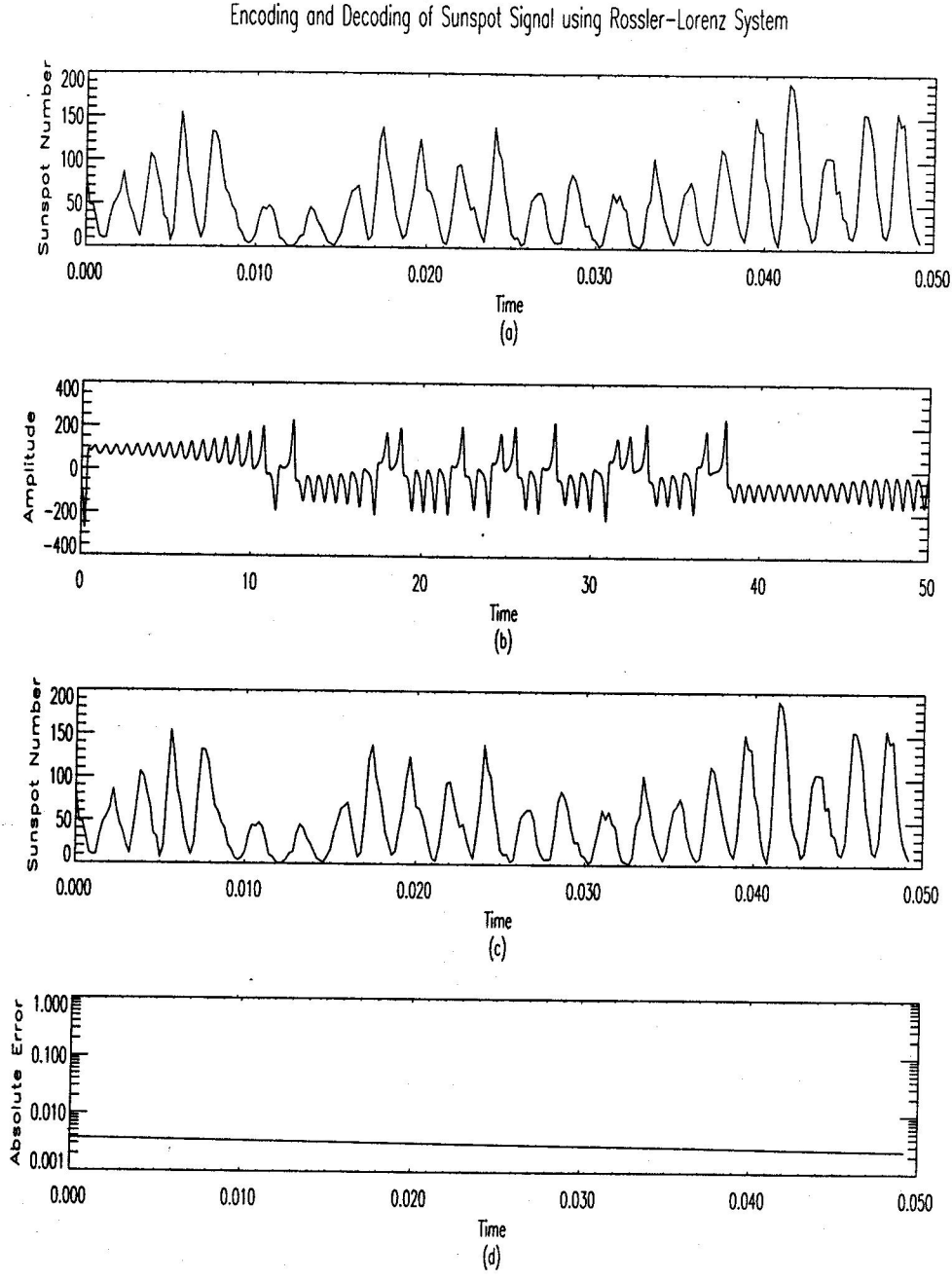


Figure 14: Encoding and Decoding of Sunspot signal using heterogenous Rossler and Lorenz systems in the APD method of communications. a) the original signal b) the transmitted signal c) the recovered signal d) the absolute error in the recovered signal in log scale. The padded part of the signal is not shown except in (b).

5 Effect of noise and parameter variation on recovered signal

In this section we study how the accuracy of the recovered signal is affected by the addition of noise in the transmitted signal as well as by the variation of parameters of the chaotic receiver system.

5.1 Effect of noise on signal recovery

In the recovery procedure so far, we have assumed that the transmitted signal generated by the transmitter system is directly received by the receiver system without any contamination. However in a typical communication application the tramsmitter site and the receiver site are geographically at a long distance from each other. Consequently the transmitted signal, as it traverses through long distance, is likely to get contaminated by some noise. Here we study the robustness of the recovery procedure at the receiver against the noisy signal. To be specific we are interested in knowing how the amount of noise in the transmitted signal affects the accuracy of the recovered signal. We assume that the nature of the noise is an additive gaussian noise with mean equal to zero. The strength of the noise, as indicated by its standard deviation (σ_n), is taken as some percentage of the σ_s of the transmitted signal. The goodness of the recovered signal is measured by evaluating the quantity known as normalized mean square error (NMSE). The term NMSE is defined as the ratio of the mean square deviation of the recovered signal from the original signal and the variance of the original signal.

In our study the σ_n of the noise is varied from 1% to 10% of the σ_s of the transmitted signal. The calculations are performed in the APD framework using the Rössler system as given by Eqs. (34) and (36) but without cascading. It is observed that the behaviour of the NMSE with respect to the percentage of noise is fairly smooth for all the signals only upto 5% noise. For higher percentage of the noise, however, the NMSE shows wild fluctuations especially in the real signals. We can, thus, conclude that the maximum percentage of noise tolerated by the recovery procedure is 5%. Within the 5% of noise the NMSE for all signals increases as the noise increases. The rate of increase is found to be much lower in the computer generated signals that that in the real signals. Also the increase in not exactly linear. The NMSE in the recovered sunspot series as a function of percentage of noise added in the transmitted signal is shown in Fig. 15.

The goodness of the recovered signal depends on how close the value of NMSE is to zero. We presume that the value of NMSE to be less than 0.05 as an indicator of good match between the recovered and the original signal. Keeping this criterion we can say that the computer generated signals can tolerate noise upto 5% while the real signals have tolerence only upto 3%.

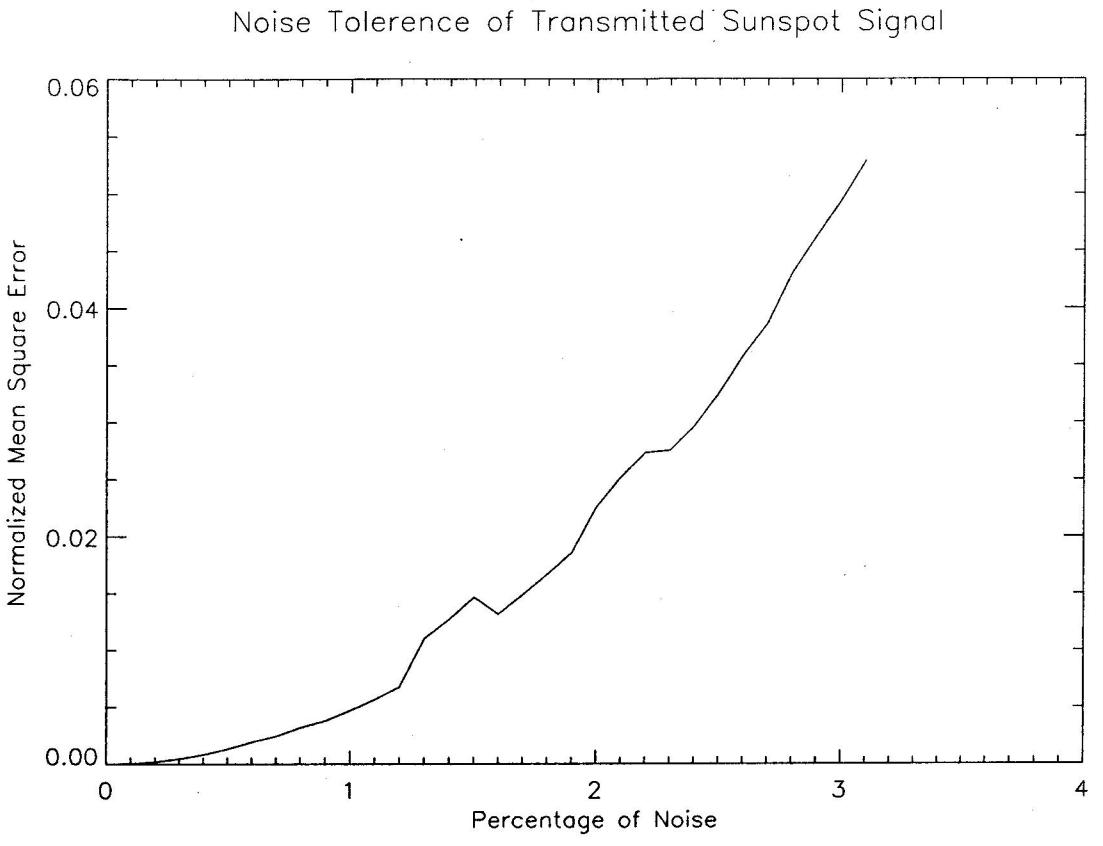


Figure 15: The normalized mean square error in the recovered sunspot signal is shown as a function of percentage of noise added in the transmitted signal.

The robustness of the receiver system against the limited noise level in the transmitted signal can be considered as a desirable attribute of any communication system. Unfortunately for the communication system based on the synchronization of two chaotic systems the noise tolerence level is not very high.

5.2 Effect of parameter variations

In the communication application based on synchronization the inherent requirement is that the parameters of the transmitter system should be same as those of the receiver system. In computer simulations this requirement can be easily satisfied for obvious reasons. However, in actual implementation, it implies that we would need to build two identical hardware units, one for the transmitter system and other for the receiver system. In practice two hardware units, though designed with the same specification, would not be exactly identical due to the fact that the components that go into the systems might not be identical. Therefore, we examine how the parameter variations in the two systems affects the accuracy of the recovered signal.

We have studied various signals in the APD framework using the Rossler system. We rewrite the Rössler system (10) in the following form.

$$\begin{aligned} \dot{X}_1 &= b + X_1(X_2 - c) \\ \dot{X}_2 &= -X_1 - X_3 \\ \dot{X}_3 &= X_2 + aX_3 \end{aligned} \tag{42}$$

where a, b, c are the parameters whose normal values will be taken as (0.45, 2, 4) respectively.

Again the calculations are performed in the APD framework using the Rossler system as given by Eqs. (34) and (36) but without cascading. The parameters a, b, and c are varied systematically about their normal values in the receiver system. The transmitted signal is generated by the transmitter system using the normal values of the parameters. The plots of NMSE in the recovered signal against the percentage variation in different parameters of the receiver system are obtained using different signals. These plots have similar behaviour to those obtained for noise variation discussed previously. It is observed that the parameters a and c are more critical than the parameter b. The parameters a and c tolerate the variation of about 5%, while the parameter b tolerates a variation of about 10%. In general the EEG signal has less tolerence against parameter variations compared to other signals. Fig. 16 shows the NMSE in the recovered sunspot signal as a function of percentage of variation in parameter a.

Finally it may be noted that the parameters of the transmitter system do provide the key to decode the message. Hence the robustness of the receiver system against parameter variations may not be a desirable feature. However, for the hardware implementation the tolerence against small variations would be necessary. From this point of view our results seem to be encouraging.

6 Some attempts of decoding the messages

It may be noted that the communication based on chaotic synchronization has two desirable features for secure and private communication. The first one is that the actual transmitted signal, being a chaotic carrier masking the information signal, is broadband and hence look like some type of noise. Secondly it is not possible to decode the signal at the receiver end without the full knowledge of the transmitter system. In other words it implies that it may be, in general, difficult for a third party to extract the message easily. However number of attempts have been made to decode message even in the absence of any knowledge of the transmitter system. We describe some of these efforts in this section.

Perez and Cerdeira [7] have reported that it is possible to extract messages masked by chaotic carriers in the PC method using the Lorenz system without resorting to a

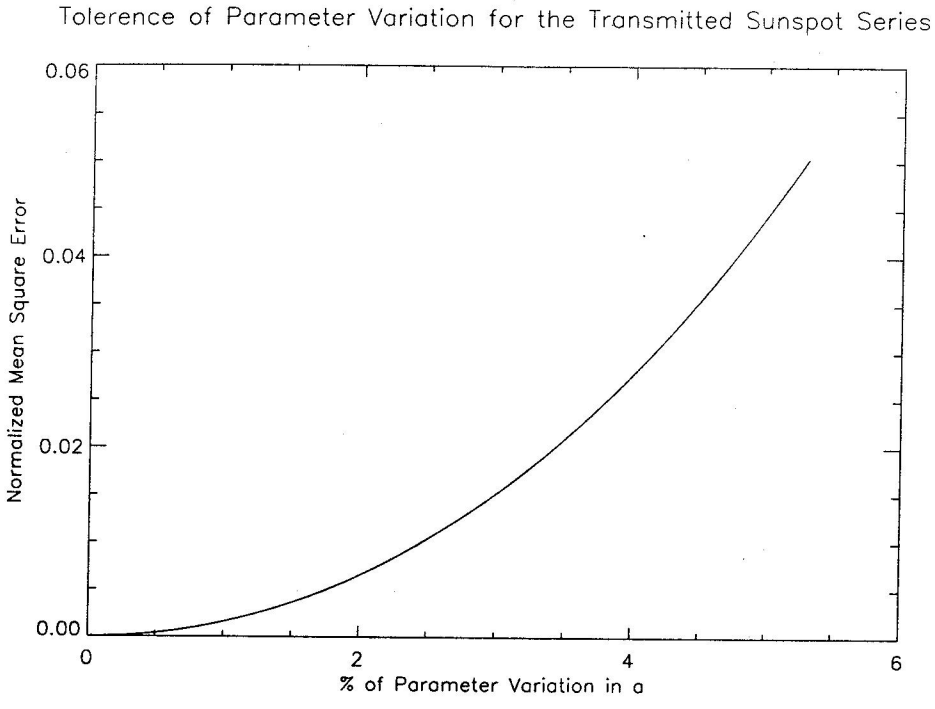


Figure 16: The normalized mean square error in the recovered sunspot signal is shown as a function of the percentage of variation in Rossler parameter a.

non-linear receiving system. The method is based on the partial reconstruction of the dynamics using some return maps. By analyzing the evolution of the signal on the attracting sets of these maps, the message can be extracted. The method is specific to Lorenz oscillator case and can not be generalized.

The other method by Short [8] is more general and is based on the complete reconstruction of the dynamics. In this approach the amplitude of the modulating signal is assumed to be small and the phase-space of the chaotic carrier is reconstructed from the transmitted time-series using the standard embedding technique. The chaotic time-series is predicted by noting the flow of nearby trajectories in the embedded space. Then the fourier transform of the difference between the predicted series and the actual transmitted series is taken and a comb filter is applied. This fourier spectrum now reveals the modulating signal. The technique works well when the modulating signal amplitude is small. If the amplitude of the modulating signal is large, the phase-space structure of the carrier gets greatly altered and it is not be possible to get a good delay embedding of the carrier dynamics.

Next we try to decode the sunspot signal from the corresponding transmitter signal of the APD method of communication using the local linear approximation [8] for the state space reconstruction applying the standard embedding technique. We find that the single step predictions (with prediction step $S = 1$) for all the points within the

transmitted signal are very accurate. In other words the error signal does not reveal the identity of the message signal. The error signal is also found to be almost zero even for other prediction steps $S = 2$ and $S = 3$. Similar results are obtained for other signals. It thus suggests that the local linear approximation method may not work for decoding the message signal in the APD method. It may be worth remembering that the most important way the APD method of communication differs from other methods is that the message signal is not just externally added to the chaotic carrier signal but it forms the part of the transmitter system and is dynamically embedded in the transmitted signal.

7 Some considerations of hardware implementation

In order to build the operational communication system in real time it is essential that the process of encoding the message at the transmitter as well as the process of decoding the same at the receiver should be performed as fast as possible. This can be achieved by implementing the system in hardware [2, 9, 10] (A note-book PC may also work equally well.) One would, thus, design an appropriate analog circuit implementing the chaotic system equations used in the transmitter and the receiver systems of the communication system. However the implementation of these equations with an electronic circuit is not always straightforward. The foremost difficulty is often caused due to wide dynamic range of values assumed by the state variables in the equations. These values, in turn, exceed the reasonable power supply limits. This difficulty can be eliminated by transforming the state variables into a set of new variables whose values are now confined to suitably small and similar range. The set of equations using the new variables can be easily implemented with an electronic circuits.

The circuit implementation typically has some widely used standard components. It would invariably contain operational amplifiers and associated circuitry to perform the operations of addition, subtraction and integration. The non-linear terms would be generally implemented using analog multipliers. The parameters of the system could be varied by adjusting the corresponding resistors so that any parameter can be varied independently. The circuit time scale also can be adjusted by changing the values of the associated capacitors.

In order to verify the chaotic behaviour of the circuit, there would be an analog-to-digital (AD) data recorder system which can be used to sample the appropriate circuit output. If the properties of the sample are similar to those for the signal obtained by the numerical simulation one can then say that the performance of the circuit and the simulation are consistent.

8 Summary and conclusions

Application of chaotic dynamics to communications has been studied mainly using the property of synchronization. It is known that two identical low-dimensional chaotic systems would, under certain conditions, sunchronize if one of the variables from the transmitter system is used to drive the receiver system. In a typical application, a large amplitude chaotic signal at the transmitter is used as a carrier which masks the relatively low amplitude information bearing signal added to it. The actual information bearing signal can be recovered at the receiver by removing the carrier signal generated by the synchronized receiver system. Various methods of synchronizations and their application to communications have been briefly discussed. It has been found that the method of communication based on the synchronization of active-passive decomposition (APD) of the chaotic system is very accurate.

We have focussed on the APD method of communications using different chaotic systems and their combinations viz. i) Rossler system ii) Lorenz system iii) Cascaded identical Rossler systems in series and iv) Parallel heterogenous system consisting of Rossler and Lorenz system. The idea is to study the relative merits of the systems in terms of shape of the transmitted signal, extent of masking of information signal, errors in recovered signal and power spectra of original and recovered signals. In our exercise of computer simulation we have used these systems to communicate three computer generated and two experimental time series signals. In general we have found that the transmitted chaotic signal very well masks the message signal and the accuracy of the recovered signal is quite high. However short signals such as annual sunspot series consisting of sharp peaks and valleys requires additional smoothing before it can be masked completely in the transmitted signal. The objective of using the cascaded identical systems and parallel heterogenous systems is to generate hyperchaotic transmitted signal for carrying the information signal. It is expected that such signals would be difficult to decode and hence are desirable for secure communications but at the same time they would have relatively low accuracy of the recovered signal. We have also studied the effect of additive noise in the transmitted signal and variation of parameters of the chaotic systems on the accuracy of the recovered signal. It is found that the tolerence for the noise is about 3% and that for the parameter variation is about 5%.

References

[1] L.M. Pecora and T.L. Carroll, "Synchronization in chaotic systems", *Phys. Rev. Lett.*, **64**, pp. 821-824, 1990.

[2] K.M. Cuomo and A.V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications", *Phys. Rev. Lett.*, **71**, pp. 65-68, 1993.

[3] U. Parlitz, L. Kocarev, T. Stojanovski and H. Preckel, "Encoding messages using chaotic synchronization", *Phys. Rev.*, **E 53**, pp. 4351-4361, 1996.

[4] J.K. John and R.E. Amritkar, "Synchronization of unstable orbits using adaptive control", *Phys. Rev.*, **E 49**, pp. 4843-4848, 1994.

[5] H.D. Abarbanel and P.S. Linsay, "Secure communications and unstable periodic orbits of strange attractors", *IEEE Trans. Circuits and Systems II*, **40**, pp. 643-645, 1993.

[6] L. Kocarev and U. Partiltz, "General Approach for chaotic synchronization with applications to communications", *Phys. Rev. Lett.*, **74**, pp. 5028-5031, 1995.

[7] G. Perez and H.A. Cardeira, "Extracting messages masked by chaos", *Phys. Rev. Lett.*, **74**, pp. 1970-1973, 1995.

[8] K.M. Short, *Int. Jrnl. Bifurc. Chaos*, **4**, pp. 959, 1994.

[9] K.M. Cuomo, A.V. Oppenheim and S.H. Strogatz, *IEEE Trans. Circuits and Systems II*, **40**, pp. 626, 1993.

[10] T.L. Carroll and L.M. Pecora, "Synchronizing nonautonomous chaotic circuits", *IEEE Trans. Circiuts and Systems II*, **40**, pp. 642, 1993.