Tomas Bata University in Zlín
Faculty of Applied Informatics

Nguyễn Thanh Dũng

Secure Encryption Via Deterministic Chaos

Doctoral Thesis

Supervisor: Prof. Ivan Zelinka, *PhD*.

Study-branch: Technical Cybernetics

Zlin, Czech Republic, 2012

ACKNOWLEDGEMENTS

First of all, I am deeply grateful to my supervisor **Prof. Ivan Zelinka** for his excellent guidance and valuable support during the work. He got me interested in this puzzling area of chaos and artificial intelligent. His insight and knowledge have made this work a reality.

I am indebted to **Prof. Karel Vlček, Assoc**. **Prof. Milan Matejdes** and **Assoc**. **Prof. Roman Jasek** for their conducts through my subjects. Their contributions, detailed comments have been of great value to me.

I wish to extend my thanks to **Dr. Roman Šenkeřík** for his practical help on many occasions in the simulations. Also, I warmly thank all my colleagues for their co-operation and support during the work.

I am thankful to **Ms. Jana Doleželová**, **Ms. Monika Krištofová** of Faculty of Applied Informatics, and **Ing. Michaela Bláhová** of International Affairs Department for the priceless support and advices on the never-ending problems in many things.

Last but not least, I would like to express my deepest love, respect and gratitude to my wife, my family and my friends for encouraging me to effectively complete my study.

The work was supported by the Ministry of Education, Youth and Sports of the Czech Republic under grant No. MSM 7088352101, and research project Control Algorithm Design by Means of Evolutionary Approach under grant No. GACR 102/09/1680.

ABSTRACT

The evolutionary algorithms are applied to enhance the quality of recovered signal in chaotic secure communication system that is the core objective of this dissertation. The synchronization error between the transmitter and the receiver in communication systems is used to design the cost function.

The parameters of chaotic dynamic model are estimated by evolutionary algorithms via minimizing the synchronization errors. By this way, the quality of recovered signal is increased when the synchronization error approaches to minimum value.

The Pecora and Carroll method (PC method), Active-Passive Decomposition method (APD method) and Feedback method-three synchronization methods are used to achieve the synchronization of chaos communication.

Differential evolution algorithm (DE) and Self-Organising Migrating Algorithm (SOMA) are used as the evolutionary algorithms to find the unknown parameters of receiver chaotic systems.

The synchronizations of identical chaos are executed: Synchronization of three dimensional Lotka-Volterra systems via PC method, synchronization of four dimensional Qi systems via APD method, synchronization of four dimensional Liu systems via Feedback method.

The powerful of EA on this problem are also proven via the synchronization of 5 and 6 dimensional chaotic systems.

The application of EA is used for designing the control function in the synchronization between two difference chaotic systems.

Based on the optimum results from evolutionary algorithms, the estimated values are used to reconstruct the receiver chaotic systems. The optimal quality of synchronization is achieved by using the estimated parameters.

The synchronization between the transmitter and the receiver chaotic system is used to retrieve the transmitted information in Chaotic Masking Scheme (CMS). The quality of chaotic secure communication is enhanced with estimated parameters.

It is possible to state that all simulations gave satisfactory results and thus evolutionary algorithms are successful in solving this difficult problem.

RESUME

Evoluční algoritmy jsou použity ke zvýšení kvality obnovení signálu v chaosem zabezpečeném komunikačním systému, který je klíčovým objektem této disertační práce. Chyba synchronizace mezi vysílačem a přijímačem v komunikačním systému je použita k návrhu účelovou funkci.

Parametry chaotického dynamického modelu jsou odhadovány evolučními algoritmy pomocí minimalizace chyby synchronizace. Tímto způsobem je kvalita obnoveného signálu zvýšena pokud se chyba synchronizace blíží minimální hodnotě.

K synchronizaci komunikačního chaosu jsou požity tři metody metoda Pecora-Carroll (PC), metoda Active-Passive Decomposition (APD) a zpětnovazební metoda.

Diferenciální evoluční algoritmus (DE) a Self-Organising Migrating algoritmus (SOMA) jsou evoluční algoritmy použité k nalezení optimálních parametrů chaotického přijímacího systému.

Jsou prováděny synchronizace identického chaosu: synchronizace tří-dimenzionálního Lotka-Volterra systemu pomocí PC metody, synchronizace čtyř-dimenzionálního Qi systemu pomocí APD metody a synchronizace čtyř-dimenzionálního Liu systemu pomocí zpětnovazební metody.

Výkonnost EA je potom ověřena pomocí synchronizace pěti a šesti-dimenzionálního chaotického systému.

EA je použit pro navržení řídící funkce při synchronizaci mezi dvěma rozdílnými chaotickými systémy.

Na základě optimálních výsledků z evolučních algoritmů jsou odhadované hodnoty použity k rekonstruování přijímacího chaotického systému. Pomocí odhadnutých parametrů je dosahováno optimální kvality synchronizace.

Synchronizace mezi vysílacím a přijímacím chaotickým systémem je použita k znovuzískání vysílané informace v Chaotic-Masking Scheme (CMS). Kvalita chaosem zabezpečené komunikace je zvýšena pomocí odhadovaných parametrů.

Můžeme říci, že všechny simulace dávají uspokojivé výsledky a tak evoluční algoritmy jsou úspěšné při řešení tohoto složitého problému.

CONTENTS:

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

EA	Evolutionary Algorithm
CF	Cost Function
CF_{1D}	Cost Function of 1-dimensional simulation
CF_{2D}	Cost Function of 2-dimensional simulation
CF_{3D}	Cost Function of 3-dimensional simulation
CF_{4D}	Cost Function of 4-dimensional simulation
CF_{5D}	Cost Function of 5-dimensional simulation
CF_{6D}	Cost Function of 6-dimensional simulation
CFE	Cost Function Evaluation
SOMA	Self Organizing Migrating Algorithm
ATO	All To One strategy of SOMA, all individuals search in the direction to Leader
ATR	All To One Rand strategy of SOMA, all individuals search in the direction to one randomly selected
ATA	All To All strategy of SOMA, all individuals search in the direction to all individuals
ATAA	All To All Adaptive strategy of SOMA, all individuals search in the direction to all by means of adaptive way
DE	Differential Evolution
DERand1Bin	Version of DE
DERand2Bin	Version of DE
DEBest2Bin	Version of DE
DELocalToBest	Version of DE
DERand1DIter	Version of DE
DEBest1JIter	Version of DE
PopSize	Number of individuals in population
CR	Control parameter of DE, crossover constant
F	Control parameter of DE, mutable constant
Generations	Stopping parameter of DE, number of loops in all evolution

Migrations	Stopping parameter of SOMA, number of migration loops
MinDiv	Stopping parameter of SOMA, minimal accepted error between the best and worst individual in population
NP	Number of individuals in population
PathLength	Control parameter of SOMA; it determines the stopping position of the movement of an individual
PRTVector	Vector of zeros and ones, it interacts with the movement of an individual
Step	Control parameter of SOMA, length of step of an individual during search
n	step in iteration
a, b, c, d, h, k, r,	parameters of chaotic systems
i, j	indexes
t	times
x, y, z, u, w	space variable
l, m	simulation interval
CSK	Chaos Shift Keying
CMS	Chaotic Masking Scheme
PC	Pecora and Caroll method
APD	Active Passive Decomposition method
FB	Feedback method

1. Introduction and State of Art

Chaotic secure communication has attracted very extensive research activity since Pecora and Carroll proposed a method to synchronize two identical chaotic systems under different initial conditions. Several secure communication techniques were proposed and analysed including chaos masking (CMS), chaotic shift keying (CSK), differential chaos shift keying (DCSK), chaotic frequency modulation, and in-phase/ anti phase synchronization, *etc*[3]. Most of the systems are based on synchronization of chaos between a transmitter and a receiver, which are linked by a transmission channel. The synchronization between the transmitter and receiver is compulsory in these systems. Several types of synchronization have been considered in chaos communication systems, such as PC method [5], OGY method [7], feedback approach [9], adaptive method [10], time-delay feedback approach [11], back stepping design technique [12], *etc*.

In order to achieve chaos synchronization, the receiver dynamical system needs to be identical to the transmitter dynamical system. The receiver is further coupled to the transmitter through the transmission channel. When the parameters of the receiver are respectively identical to those of the transmitter and the coupling strength is strong enough, the receiver can synchronize to the transmitter in all dynamical states including the chaotic state. Therefore, the output of the receiver can reproduce the "original chaotic waveform" from the transmitter. The decoding is achieved by comparing the received signal with the reproduced chaotic waveform. However, because of the difference in the driving forces, the receiver chaotic system may not have exactly the same parameters as those of the transmitter system, synchronization of the two chaotic waveforms generated by the transmitter and the receiver is not complete. Therefore, the system performance generally depends on the quality of chaos synchronization. To ensure the quality of chaotic communication, minimization of synchronization errors is very important.

Nowadays, the evolutionary algorithms (EA) are known as powerful tool for almost difficult and complex optimization problems. They have attracted much attention and wide applications in different fields. Motivated by the aforementioned studies, this study aims to present the using of evolutionary algorithms to enhance the quality of recovered signal in chaos secure communication systems. The parameters of chaotic dynamic system are estimated by minimizing the synchronization error via evolutionary algorithms. By this way, the quality of recovered signal is increased if the synchronization error approaches to minimum value. Depending on the applications of chaotic communications, different encoding and decoding schemes can be selected. Based on the optimum results from evolutionary algorithms, the estimated parameters are used to synchronize two chaotic systems. The quality of received signal which is recovered with estimated parameters is higher than that of original parameters.

The dissertation consists of three main parts: introduction, theory and experiment.

The first chapter gives the overview of the research area of chaotic secure communication, whereas the second chapter formulates the main aims of this dissertation.

The theoretical section contains chapters on the description and theoretical knowledge about the secure communication based on chaos (Chapter 3), Methods for synchronization of chaos (Chapter 4), description of 3,4,5,6 dimensional chaotic systems (Chapter5), with the description of evolutionary algorithms used in the work (Chapter 6).

The experimental section covers chapters in the design of experiment – Cost function (Chapter 7), Synchronization of 3-D Lotka-Volterra system via PC method (Chapter 8), Synchronization of 4-D Qi chaotic system via APD method (Chapter 9), Synchronization of 4-D Liu chaotic system via Feedback method (Chapter 10), Synchronization of 5-D Lorenz chaotic system (Chapter 11), Six dimensional simulation: Synchronization of 6-D Lorenz chaotic system (Chapter 12), Synchronization of two different chaotic system (Chapter 13), Application on chaotic secure communication system (Chapter 14).

Chapter 15 gives the brief discussion of the obtained results from all case studies and conclusion of the achieved goals in this work together with an outlook for the future research.

2. The Aims of Dissertation

The main focus of dissertation showed how the evolutionary algorithms can be used to enhance the quality of chaotic secure communication. Basic concepts and synchronization methods were reviewed. Experimental results were presented to demonstrate the fundamental concepts. Numerical computations were employed for searching the optimum values and illustrating the powerful of EA. The objective is to provide a method, which uses to minimize the chaos synchronization errors in the chaotic secure communication systems.

Some similar research in this field has recently been done in theory for estimating unknown parameters of chaos systems. It is to focus on finding the synchronization between two or more chaos systems. But the approach described here is different. EA was used to find optimal values of unknown parameters of chaotic system by minimizing the synchronization error between two chaotic systems. The synchronization error is decreased with estimated parameters. It was not only used to synchronize two chaos systems but also enhance the quality of synchronization of transmitter and receiver.

The thesis would contain all following points:

- To simulate several examples of identical chaos synchronization (3, 4, 5, 6-dimensional chaos systems).
- To simulate the using of EA for synchronization between two difference chaos systems.
- To simulate a synchronization via PC, APD and Feedback methods.
- To prove that EA are able to estimate the unknown parameters of chaos systems.
- To optimum cost function with SOMA and DE, enhancing the quality of chaos synchronization.
- To test a performance of EA in CMS scheme.

THEORETICAL SECTION

3. Secure Communication Based on Chaos

3.1. General secure communication system

Block diagram of general secure communication system is shown in Figure 3.1. The information source block provides the data for source coding block where it was coded in an optimum way for further transmission. The encryption block re-codes the data in order to enhance transmission security. The channel coding block executes a variety of transformations on the input data to minimize the overall degradation due to channel impairments. Modulation impresses the encoded data onto the radio frequency carrier, which is then combined with other signals in a multiple access scheme, and finally delivered to the transmitter antenna. The receiver recovers the information by reversing these steps. In conventional digital communication systems, each symbol to be sent is represented by a piece of sinusoidal signal. In chaos-based secure communication systems, each symbol is now denoted by a section of chaotic signal, which is non-periodic. Therefore, even if the same symbol is being sent repeatedly, the chaotic signals representing the same symbol are different. In the following, the chaotic secure communication schemes based on chaos are presented.

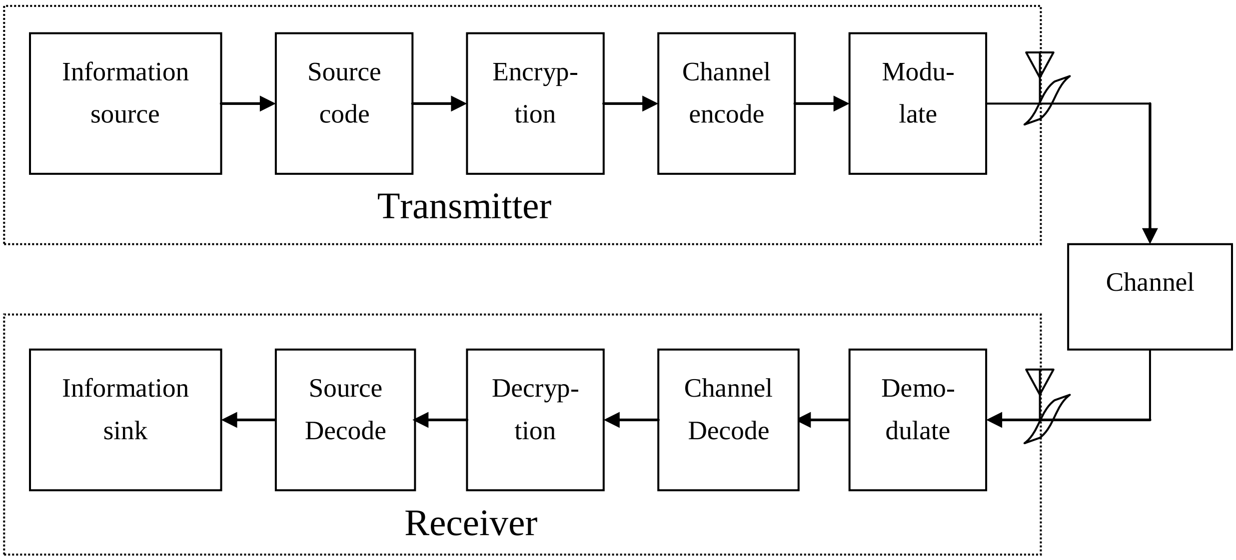


Figure 3.1. General secure communication system

3.2. Chaos Shift Keying (CSK)

Chaos shift keying (CSK) is one of the earliest chaotic communication methods. CSK was first proposed by Dedieu and Hasler [3]. Most widely studied CSK system is the binary CSK where two identical chaotic systems are present at the transmitter and the receiver. Block diagram of CSK communication system is shown in Figure 3.2. Depending on the message m (information bit $b_k=\pm1$), one of these chaotic systems are selected and the state variable corresponding to that system is transmitted. The operating principle can be described as follows. Chaotic signals with different bit energies are used to transmit the binary information. The modulator is a very simple circuit: for bit "+1", a chaotic sample function with mean bit energy s_1 is radiated, for bit (-1), a chaotic sample function with mean bit energy s_2 is radiated. That mean if a binary (+1) is to be sent, $f_1(t)$ is transmitted, and if (-1) is to be sent, $f_2(t)$ is transmitted. The required chaotic signals having different bit energies can be generated by different chaotic circuits or they can be produced by the same chaotic circuit and multiplied by two different constants. In both cases, the binary information to be transmitted is mapped to the bit energies of chaotic sample functions. The bit energy can be estimated at the receiver, as shown in block diagram of CSK system.

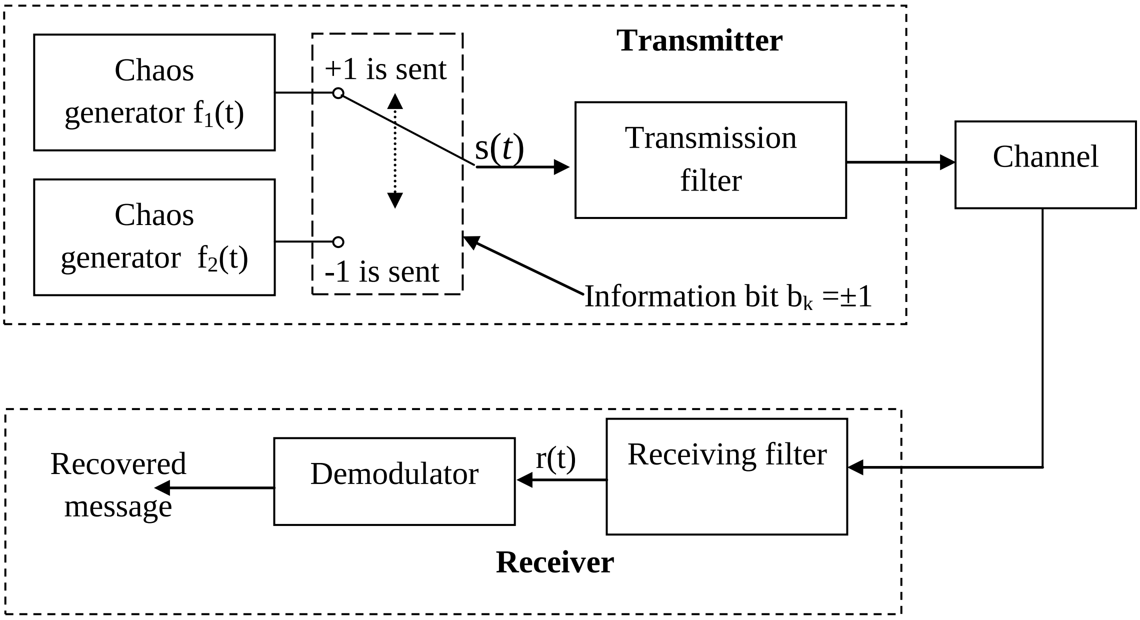


Figure 3.2. Block diagram of CSK system

In chaos shift keying, the transmitter dynamics is dissipative and chaotic. The transmitter state trajectory converges to a strange attractor. A message is transmitted by altering one or more parameters of the transmitter dynamics which result in a change of the attractor position. At the receiver the message is decoded by estimating to which attractor the received signal belongs.

3.3. Chaotic Masking Scheme (CMS)

Chaotic Masking Scheme (CMS) that is based on chaos synchronization and mixing of a chaotic signal with a message is shown in Figure 3.3. In this scheme, a message signal is added to a chaotic signal generated by a chaotic dynamical system at the transmitter, and the sum of the two is transmitted through the channel. The message is added into carrier signal before being sent to the receiver as the "hide" message. When a secret message is being encrypted, the encryption should be as complex as possible to avoid someone intercept the message.

A block diagram of a chaotic masking system is shown in where the information signal is recovered by subtracting the synchronized chaotic signal from the received waveform. The chaotic component is subtracted from the received signal to recover the original transmitted message at the receiver. The receiver is synchronized to the transmitter.

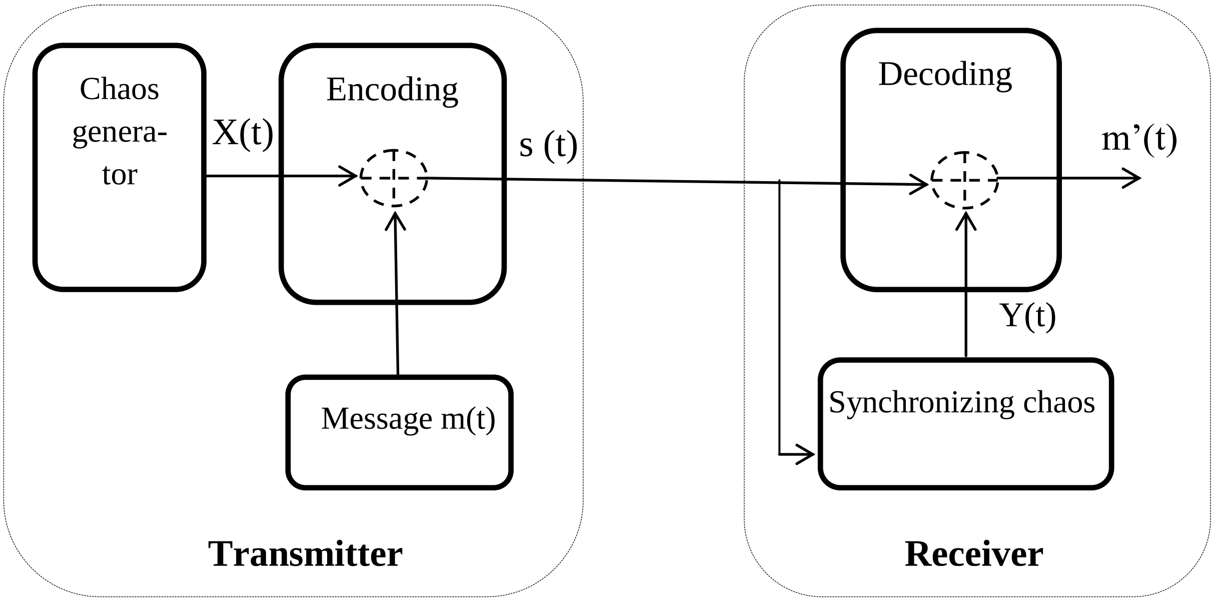


Figure 3.3. Chaotic Masking Scheme

4. Synchronization Methods

The idea of synchronizing two chaotic systems attracts attention of the researchers and engineers since Pecora and Carroll proposed a method to synchronize two identical chaotic systems under different initial conditions in 1989.

The possibility of encoding a message within a chaotic dynamics through perturbations of chaotic system was used to produce secure message communication between a sender and a receiver. A lot of secure communication schemes using chaotic dynamics are based on identical synchronization.

Here are some methods, which were used to synchronize two chaotic systems.

4.1. Pecora and Carroll method

In 1989, Pecora and Carroll introduced a method for constructing synchronizing chaotic systems [5]. They showed that when a state variable from a chaotic system was input into a replica subsystem of the original one, both of systems can be synchronized identically. They decomposed the dynamical system

$$\dot{\mathbf{u}} = \mathbf{g}(\mathbf{u}) \qquad (1)$$

into two subsystems,

$$\begin{aligned} \dot{\mathbf{v}} &= \mathbf{g}_{\mathbf{v}}(\mathbf{v},\mathbf{w}) \\ \dot{\mathbf{w}} &= \mathbf{g}_{\mathbf{w}}(\mathbf{v},\mathbf{w}) \end{aligned} \qquad (2)$$

with $v=(u_1, \ldots , u_k)$ and $w=(u_{k+1}, \ldots , u_n)$.

and considering one of the decomposed subsystems as the driving signal, say v, to be injected into the response system,

$$\dot{\mathbf{w}}' = \mathbf{g}_{\mathbf{w}}(\mathbf{v},\mathbf{w}') \qquad (3)$$

that was given by the same vector field g_w, the same driving v, but different variables w´ synchronizes with the original w subsystem.

Consider the difference of these two systems e=w´ – w. The synchronization of the pair of identical systems (2) and (3) occurs if the dynamical system describes the evolution of the difference $|w'-w| \rightarrow 0$ as $t \rightarrow \infty$.

4.2. Active-Passive Decomposition method

L. Kocarev and U. Parlitz [6] proposed a general drive response scheme named as Active Passive Decomposition (APD). The basic idea of the active passive synchronization approach consisted in a decomposition of a given chaotic system into an active and a passive part where different copies of the passive part synchronize when driven by the same active component. In the following, they explained the basic concept and terminology of the active passive decomposition.

Consider an autonomous n-dimensional dynamical system, which is chaotic as

$$\dot{\mathbf{u}} = \mathbf{g}(\mathbf{u}) \quad (4)$$

The system is rewritten as a non-autonomous system:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x},\mathbf{s}) \quad (5)$$

where x is a new state vector corresponding to u and s is some vector valued function of time given by

$$\mathbf{s} = \mathbf{h}(\mathbf{x}) \quad (6)$$

The pair of functions f and h constitutes a decomposition of the original vector field g, and are chosen such that any system

$$\dot{\mathbf{y}} = \mathbf{f}(\mathbf{y},\mathbf{s}) \quad (7)$$

given by the same vector field f, the same driving signal s, but different variables y, synchronizes with the original system. Here, x constitutes the active system while y is the passive one.

The synchronization of the pair of identical systems (5) and (7) occurs if the dynamical system describes the evolution of the difference $|y - x| \to 0$ for $t \to \infty$.

4.3. Feedback method

In 1986, Afraimovich-Verichev-Rabinovich presented their works using a mathematical definition of synchronization, and a system of coupled nonautonomous nonlinear oscillator. The concepts were used by Kapitaniak [14] and Ding and Ott in 1994 [8], *etc*. Consider an n-dimensional dynamical system, which is chaotic, the formulation of the feedback method for identical synchronization of chaos is described as

$$\dot{\mathbf{U}} = \mathbf{F}(\mathbf{U}) \tag{8}$$

where $U=(u_1,u_2,\ldots u_n)T$ and $F(U)=(f_1(U),f_2(U),\ldots,f_n(U))T$. Now choose a dynamical variable as drive variable from it e.g. ui ($1 \leq i \leq n$). Consider another chaotic system identical to Eq. (8) but starting from different initial conditions (i.e. with different variables), as

$$\dot{\mathbf{U}}' = \mathbf{F}(\mathbf{U}') \tag{9}$$

with $U'=(u_1',u_2',\ldots u_n')^T$ and $F(U')=(f_1(U'),f_2(U'),\ldots,f_n(U'))^T$. Now the feedback control, which is proportional to the difference of the drive variable u_i and its counterpart u_i' in the response, is applied to response system. Hence the response systems $\mathbf{U}'^{c}$ look as

$$\dot{\mathbf{U}}'^{\mathbf{c}} = \mathbf{F}(\mathbf{U}') - \mathbf{g}(\mathbf{u}_i' - \mathbf{u}_i) \tag{10}$$

where g is a constant and termed as feedback constant or coupling strength. Consider the difference of these two systems $e=U'^{c} - U$. The synchronization of the pair drive (9) and response (10) dynamical systems occurs if the dynamical system describes the evolution of the difference $|U'^{c} - U| \rightarrow 0$ as $t \rightarrow \infty$.

5. Chaotic Systems

Theory of chaos is one of the most important achievements of nonlinear system research. In 1963, Edward Lorenz discovered the deterministic chaos while trying to forecast the weather. Deterministic chaos has three important dynamic properties: the sensitive dependence on initial conditions, the intrinsic stochastic property and ergodicity. The most attractive feature of chaos systems is the sensitive dependence on initial conditions; a small disruption finally causes a large change in the state of the system. Applying for the secure communication seems to be quite meaningful. The secure of communication system is increasing with the high unpredictability of high dimensional chaos system. Therefore, this section is the description of the 3, 4, 5, 6 dimensional chaos systems, which will be used to study in this dissertation.

5.1. Three dimensional systems

5.1.1. Lorenz system

The Lorenz system is a 3-dimensional dynamical flow which allows chaotic behavior. It was introduced by Edward Lorenz in 1963 [2]. The mathematical model developed, and has been used in a lot of studies. The equations which describe the Lorenz system are:

$$u = \begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \tag{11}$$

Lorenz chose parameter values σ=10, β=8/3, and ρ=28. With these choices for the parameters, the Lorenz system is chaotic, exhibiting the traits described in the definition given for chaos. The Lorenz attractor is depicted on Figure 5.1.

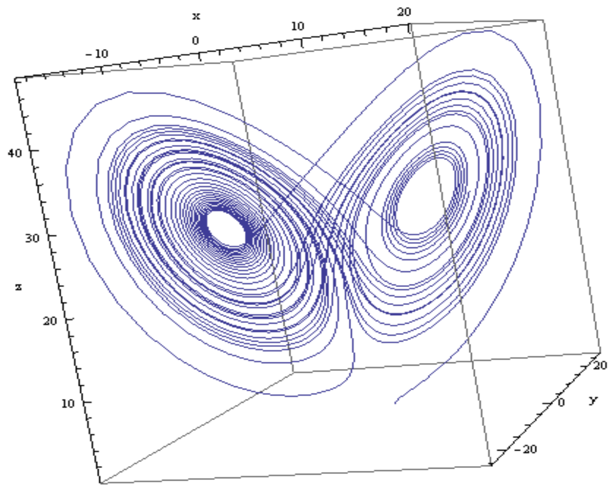


Figure 5.1. Lorenz attractor

5.1.2. Rössler system

A three-dimensional dynamical system which is simpler than the Lorenz model was proposed by Rössler [28] in 1976. The system consists of three coupled first-order differential equations

$$u = \begin{cases} \dot{x} = -y - z, \\ \dot{y} = x + ay, \\ \dot{z} = z(x - c) + b \end{cases} \qquad (12)$$

The system exhibits a chaotic attractor for a=0.45, b=2 and c=4. The Rössler attractor is depicted on Figure 5.2.

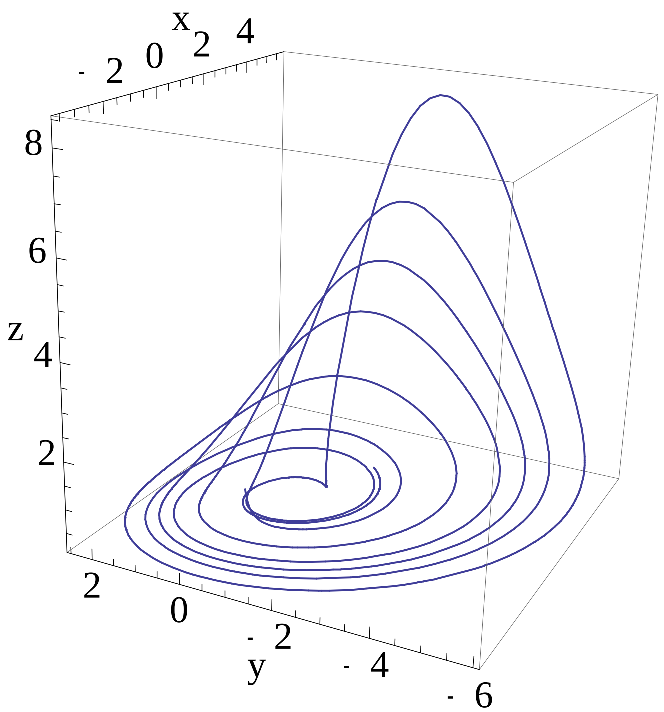


Figure 5.2. Rössler attractor

5.1.3. Lü system

Lü *et al.* proposed a unified chaotic system [29], which is a typical transition system between Lorenz and Chen attractor. The complex Lü system of equations is expressed by:

$$u = \begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -xz + cy \\ \dot{z} = xy - bz \end{cases} \tag{13}$$

which have chaotic attractor as shown in Figure 5.3 when a=36, b=3 and c2=20.

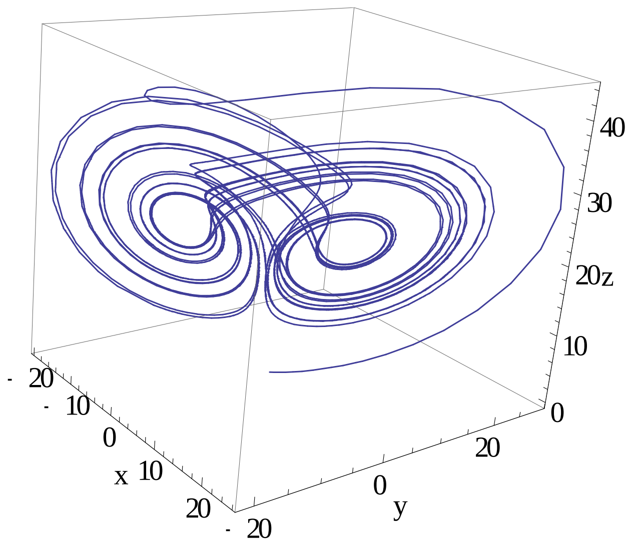


Figure 5.3. Lü attractor

5.1.4. Lotka-Volterra system

The Lotka-Volterra system was formulated by Volterra in 1926 to describe the relationship between a predator and a prey [17]. The Lotka-Volterra equations are a system of equations proposed to provide a simplified model of two-species predator/prey population dynamics. In 1988, Samardzija and Greller proposed the 3D Lotka-Volterra equations, which included two-predator and one-prey. The mathematical description of 3D Lotka-Volterra system is as follows:

$$u=\begin{cases}\dot{x}=x-xy+cx^2-azx^2\\ \dot{y}=-y+xy\\ \dot{z}=-bz+azx^2\end{cases} \tag{14}$$

where x, y and z are the state variables, and a,b and c are the positive real constants. The Lotka-Volterra system exhibits a chaotic attractor for a=2.95, b=3 and c=2 as shown in Figure 5.4.

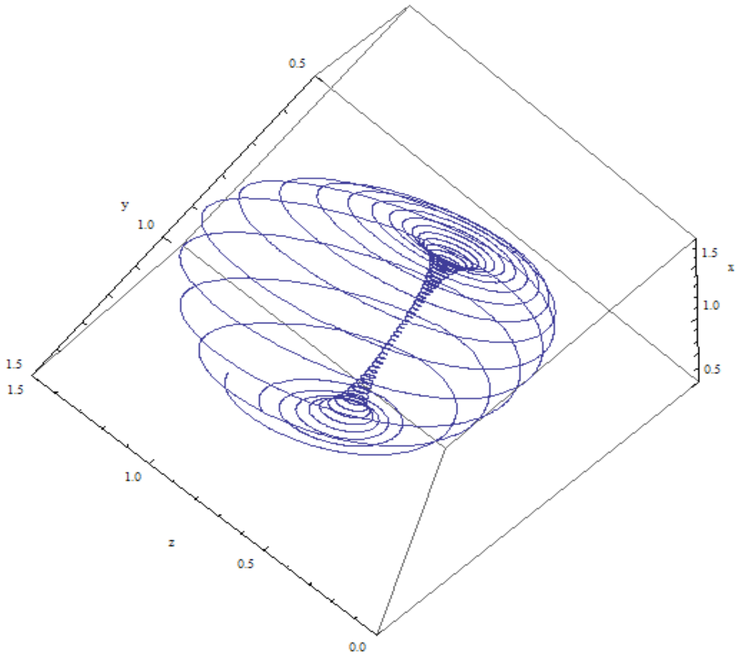


Figure 5.4. Lotka-Volterra attractor

5.2. Four dimensional systems

5.2.1. Lorenz – Stenflo system

Stenflo presented a four-dimensional system by adding an additional state into the three-dimensional Lorenz system [18]. It was originally introduced as an example of very simple chaotic flow containing chaos; in fact, it was expected to be similar to the Lorenz attractor in behavior, but easier in analyzing. This attractor has some similarities to the Lorenz attractor, but is simpler and has only one manifold. The equations which describe the Lorenz- Stenflo system are:

$$U=\begin{cases}\dot{x}=a(y-x)+cw\\ \dot{y}=x(r-z)-y\\ \dot{z}=xy-bz\\ \dot{w}=-x-aw\end{cases} \tag{15}$$

where x, y, z and w are the state variables, and a, b, c and r are the positive real constants. The L-S system exhibits a chaotic attractor for a=10, b=40, c=2.5, d=20, h=4 and k=1 as shown in Figure 5.5.

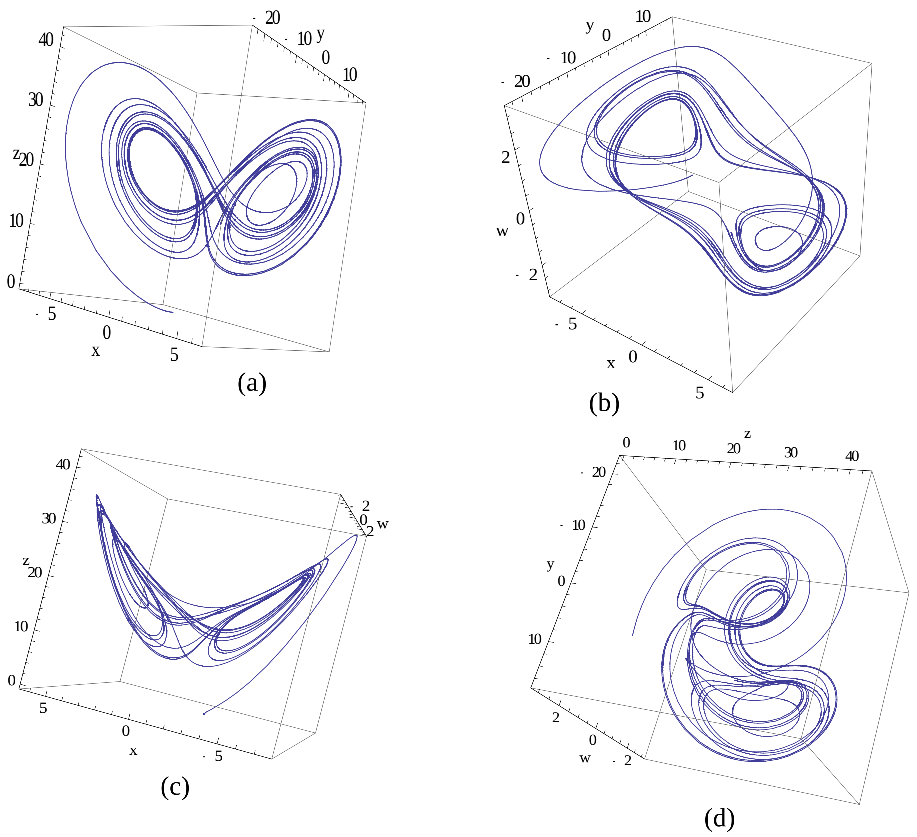


Figure 5.5. Views of the chaotic attractor of LS system

5.2.2. Qi system

Qi presented a four-dimensional system by using cross-product nonlinearities to generate chaos from an autonomous system [19]. Basic properties of the four-dimensional system have been analyzed by means of the Lyapunov exponents and bifurcation diagrams. Their study shows that the system can generate various complex chaotic attractors when the system parameters were changed. The Qi system is given by following set of equations:

$$U = \begin{cases} \dot{x} = a(y-x) + yzw \\ \dot{y} = b(x+y) - xzw \\ \dot{z} = -cz + xyw \\ \dot{w} = -dw + xyz \end{cases} \tag{16}$$

Qi studied the chaotic attractor with a=31, b=10, c=1 and d=10, which shows a simple chaotic attractor with the trajectory rotating around a fixed point. Together with increasing of value *a* chaotic behavior and period doubling in the attractor is achieved. Figure 5.6 shows the views of Qi attractor.

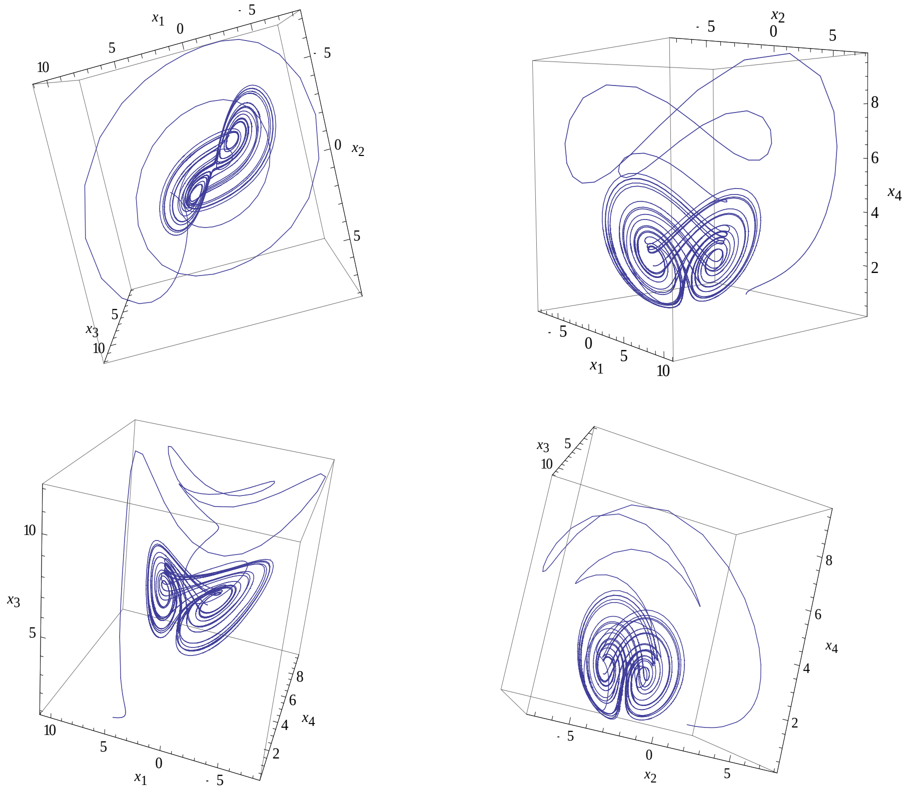


Figure 5.6. Views of the chaotic attractor of Qi system

5.2.3. Liu system

In 2007, Liu *et al.* [26] proposed a new hyperchaotic dynamical system called four-dimensional Liu system, the mathematical description of system is as follows:

$$U=\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=bx-kxz+w\\ \dot{z}=-cz+hx^2\\ \dot{w}=-dx\end{cases} \tag{17}$$

where x, y, z and w are the state variables, and a, b, c, d, k and h are the positive real constants. The Liu system (17) exhibits a chaotic attractor for a=10, b=40, c=2.5, d=20, h=4 and k=1 as shown in Figure 5.7.

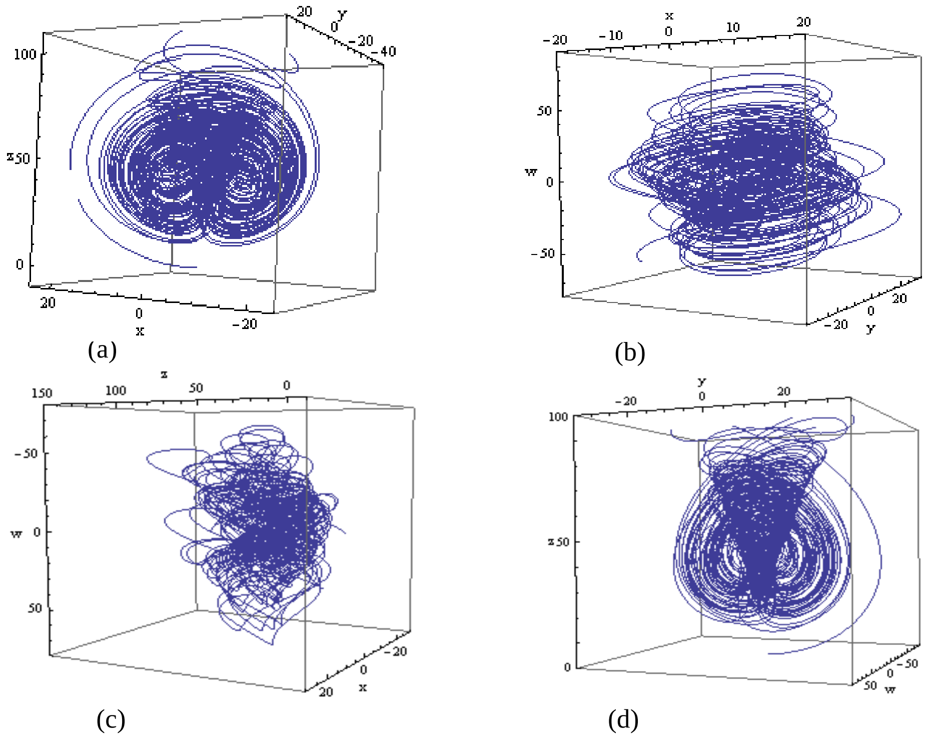


Figure 5.7. Views of the chaotic attractor of Liu system

5.3. Five dimensional system

Roy and Musielak presented a five-dimensional system by adding an additional state into the three-dimensional Lorenz system [20]. Basic properties of the five-dimensional system have been analyzed by means of the Lyapunov exponents and bifurcation diagrams. The mathematical description of 5D system is as follow:

$$U = \begin{cases} \dot{x} = a(y-x) \\ \dot{y} = rx - y - zx \\ \dot{z} = xy - bz + 2uw \\ u = -cau + 2(a/c)w \\ \dot{w} = -2uz + 2ru - cw \end{cases} \tag{18}$$

where x, y, z, u and w are the state variables, and a, b, c and r are the positive real constants. System exhibits a chaotic attractor for a=10, b=8/3, c=2 and r=24.75 as shown in Figure 5.8.

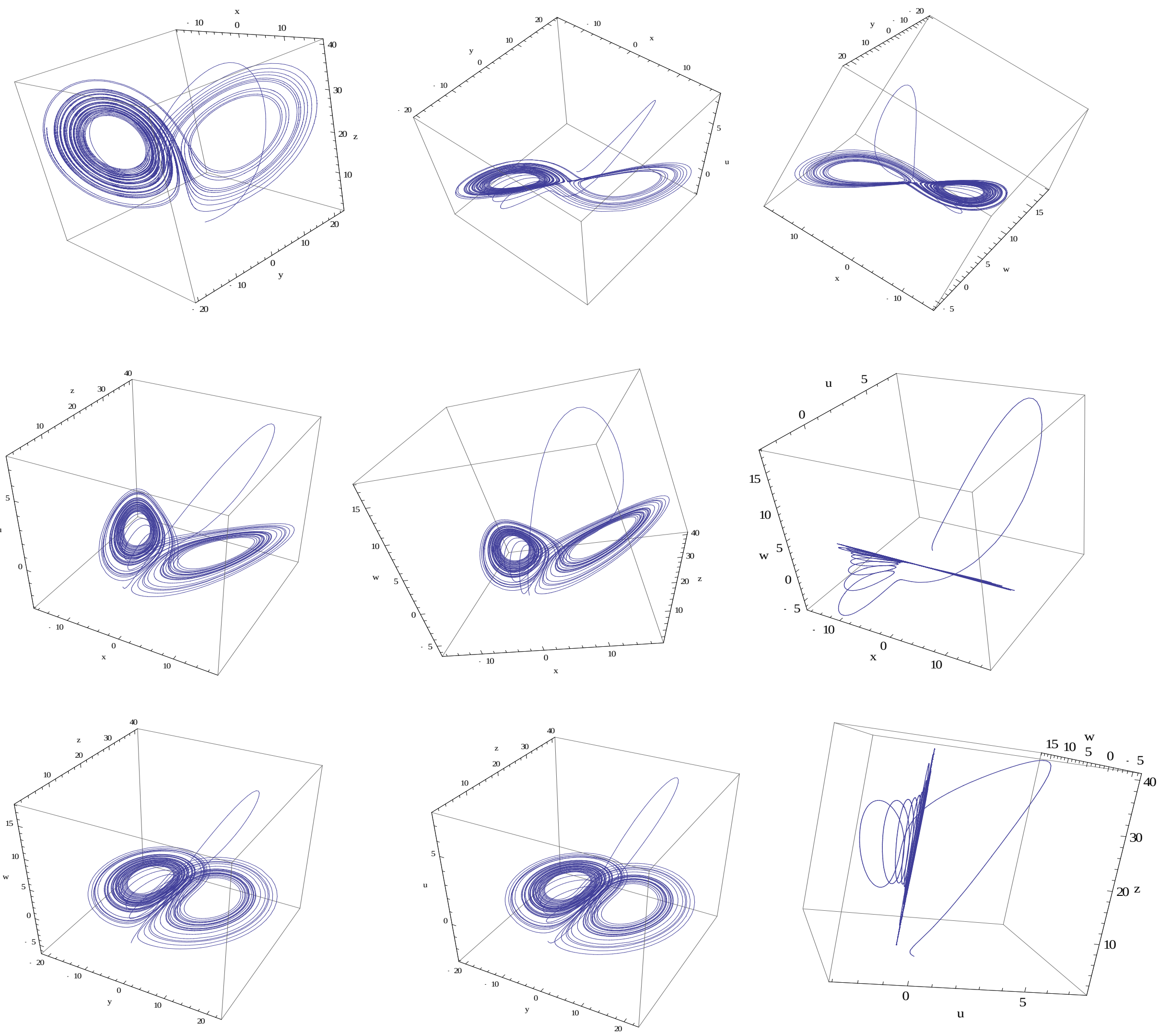


Figure 5.8. Views of the chaotic attractor of 5D chaotic system

5.4. Six dimensional system

The 6D Lorenz system was constructed by Kennamer in his M.S thesis in 1995 [30]. The 6D Lorenz systems have similar strange attractors with the 3D Lorenz system. In addition, the route to chaos via chaotic transients observed in the 6D systems is the same as that identified for the 3D Lorenz system. The only important difference between these models is that each one of them exhibits fully developed chaos for a different value of the parameter "**r**". The 6D Lorenz system is described by following nonlinear differential equations:

$$X = \begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = rx_1 - x_2 - x_1x_3 + x_3x_4 - 2x_4x_6 \\ \dot{x}_3 = x_1x_2 - bx_3 - x_1x_5 - x_2x_4 \\ \dot{x}_4 = -cax_4 + (a/c)x_5 \\ \dot{x}_5 = x_1x_3 - 2x_1x_6 + rx_4 - cx_5 \\ \dot{x}_6 = 2x_1x_5 + 2x_2x_4 - 4bx_6 \end{cases} \quad (19)$$

where x_1-x_6 are the state variables, and a, b, c and r are the positive real constants. The system has a chaotic attractor as shown in Figure 5.9 when a=10, b=8/3, c=3 and r=41.

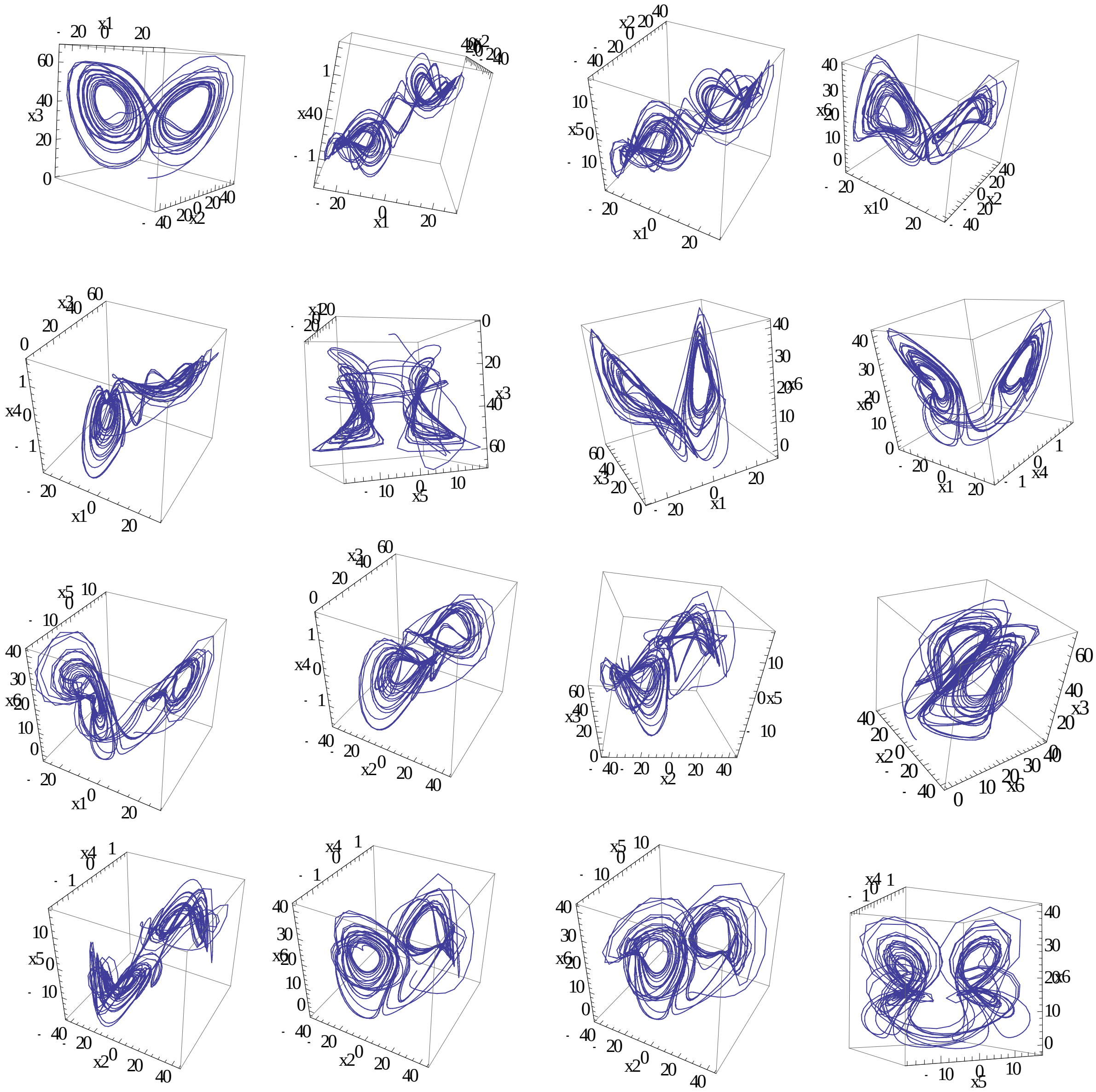


Figure 5.9. Views of the chaotic attractor of 6D Lorenz chaotic system

6. Evolutionary Algorithms

An overview of evolutionary algorithms is presented in this section, which will be used to simulate in dissertation.

6.1. Differential Evolution (DE)

DE is the simple yet efficient population-based evolutionary algorithm introduced by Storn and Price in 1995 [24]. Over the last few years, DE has been investigated by many researches and proved very easily to be implemented with superior performance in many real optimization problems. In DE system, a population of solutions is initialized randomly, which is evolved to find optimal solutions through the mutation, crossover and selection of operation procedures. It uses a simple differential operator to create new candidate solutions and one-to-one competition scheme to select a new candidate, which works with real numbers in natural manner.

The procedure of standard DE could be described:

Step 1: Choose control parameters: Population size (NP), mutation factor (F), crossover rate (Cr) and the Generations (stopping criterion).

Step 2: Randomly initialize the population of DE with NP individuals in the search space.

Step 3: Evolving the system from a random initial state and obtain N sampling points of the state X at certain time points.

Step 4: Evaluate the objective function value: first, for each individual of DE, evolves the system from the same initial state as Step 3 and obtains N sampling points of the state X at the same time points as Step 3, then calculate objective function value. Determine X_{best} in current generation.

Step 5: Perform mutation operation.

Step 6: Perform crossover operation to obtain crossover trial vectors.

Step 7: Calculate the objective function value of crossover trial vectors.

Step 8: Perform selection operation to generate individual for next generation.

Step 9: Determine the best individual of the current new generation with the best objective value. If the objective function value is better than the objective function value of X_{best}, then update X_{best} and its objective value with the value and objective value of the current best individual.

Step 10: Check if the stopping criterion is met, then output X_{best}; otherwise, go to Step 4.

More detailed description of DE can be found in [23], [24].

6.2. Self-Organizing Migrating Algorithm (SOMA)

Self-Organizing Migration Algorithm (SOMA) is one of the evolutionary algorithms was chosen. It imitates nature process of wildlife migration. The method was established in 1999, developed by Prof. Ivan Zelinka at the University of Tomas Bata, Zlín. SOMA is a stochastic optimization algorithm that is modeled on the social behavior of cooperating individuals [21]. The approach is similar to that of genetic algorithms, although it is based on the idea of a series of “migrations” by a fixed set of individuals, rather than the development of successive generations. It can be applied to any cost-minimization problem with a bounded parameter space, and is robust to local minima. SOMA works on a population of candidate solutions in loops called migration loops. The population is initialized randomly distributed over the search space at the beginning of the search. In each loop, the population is evaluated and the solution with the highest fitness becomes the leader L. Apart from the leader, in one migration loop, all individuals will traverse the input space in the direction of the leader. Mutation, the random perturbation of individuals, is an important operation for evolutionary strategies (ES). It ensures the diversity amongst the individuals and also provides the means to restore lost information in a population. Mutation is different in SOMA compared with other ES strategies. SOMA uses a parameter called PRT to achieve perturbation. This parameter has the same effect for SOMA as mutation has for GA.

The novelty of this approach is that the PRT vector is created before an individual starts its journey over the search space. The PRT vector defines the final movement of an active individual in search space.

The randomly generated binary perturbation vector controls allowed dimensions for an individual. If an element of the perturbation vector is set to zero, then the individual is not allowed to change its position in the corresponding dimension.

An individual will travel a certain distance (called the Path Length) towards the leader in n steps of defined length. If the Part Length is chosen to be greater than one, then the individual will overshot the leader. This path is perturbed randomly.

There are specified following parameters of SOMA algorithm:

Cost function: Determines how to evaluate individuals.

Specimen: Describes a form of individuals.

Population size: The number of individuals in the population which is contained in one migration.

Migrations: The maximum number of migrations to complete.

Step: The step size of individual during migration.

Part Length: Duration of path which uses individuals for migration.

PRT: Perturbation of migration.

Minimal diversity: Diversity of evolutionary process.

More detailed description of SOMA can be found in [21], [22].

EXPERIMENT SECTION

7. Design of Experiment – Cost function

This study is to focus on the estimation parameters of chaos synchronization by using EA. The estimated parameters are used to reconstruct the chaotic system, which is used to synchronize and decode. By this way, the quality of chaotic communication is increased.

The synchronization between the transmitter and receiver is compulsory in chaos communication systems. PC method, APD method and Feedback method are used to achieve chaos synchronization at receiver. The retrieved message is achieved by comparing the received signal with the reproduced chaotic waveform. These synchronization errors cause errors in the recovery message, the system performance is decreased. This impairment can be improved by reducing the synchronization errors between the transmitter and the receiver. EA is used to find the estimated parameters of chaotic system by minimizing the difference between the transmitter and receiver.

The simplest and most intuitive method to quantitatively measure the quality of synchronization is to calculate the difference between the traces of the transmitter output and the receiver output. By minimizing synchronization errors, the quality of recovered signal could be increased. Therefore, minimizing synchronization errors e=X-Y can be used to formulate the Cost function of the optimization problem by estimating the parameters of chaos system.

$$CF=\sqrt{\frac{1}{m}\sum_{t=1}^{m}|X_t - Y_t|^2} \tag{20}$$

Where: - m denotes length of time used for parameter estimation
- X_t - the transmission chaos system
- Y_t - the response chaos system

Because of the irregular dynamic behavior of chaos systems, the parameter estimation for chaos systems is a multidimensional continuous optimization problem, the parameters are not easy to obtain. In addition, there are often multiple variables in the problem and multiple local optimums in the landscape of cost function as shown in Figure 8.1 and Figure 8.5. So traditional optimization methods are easily trapped in local optima and it is difficult to achieve the global optimal parameters. Therefore, DE and SOMA were chosen because they have been proven that the algorithm is able to converge toward the global optimum. DE and SOMA were used to solve the systems, which the control parameters setting are given in Table 1 and Table 2. Simulations were implemented using Mathematica programming language and executed on Pentium D 2.0G, 2GB and HP 8200 core i3-2120 3.3 GHz, 12GB personal computers.

Table 1. DE parameter setting

Parameter	Value
Population size NP	20
Crossover rate Cr	0.3
Mutation factor F	0.9
Generation number	100

Table 2. SOMA parameter setting

Parameter	Value
Population size	20
Migrations	50
Step	0.11
Path length	3
Perturbation	0.1
Minimal diversity	-1

8. Synchronization of 3D Lotka-Volterra System via Pecora and Carroll method

In this chapter, the Pecora and Carroll method is applied to achieve the synchronization between two identical Lotka-Volterra systems. We use a subscript d to denote the signals in the drive, and use a subscript r for the signals in the response. Using y of the decomposed subsystems as the driving signal, in this case, y was injected into the response system. Since $y_d=y_r=y$, we only consider the following drive and response subsystems:

$$W=\begin{cases}\dot{x}_d = x_d - x_d y_d + 2x_d{}^2 - 2.95 z_d x_d{}^2 \\ \dot{z}_d = -3z_d + 2.95 z_d x_d{}^2\end{cases} \tag{21}$$

And the response system W' is described by the following equations:

$$W'=\begin{cases}\dot{x}_r = x_r - x_r y_r + c x_r{}^2 - a z_r x_r{}^2 \\ \dot{z}_r = -b z_r + a z_r x_r{}^2\end{cases} \tag{22}$$

where a, b, c are unknown parameter of response system,

Consider the difference of these two systems e=W´ – W. The synchronization of the pair of identical systems W and W' occurs if the dynamical system describes the evolution of the difference $|w'-w|\to 0$ as $t\to\infty$. Subtracting system W from system W' yields the error dynamical system between two systems e_t=($(x_r,z_r)_t-(x_d,z_d)_t$) which were used to create a cost function CF representing the root mean square error (RMSE) of synchronization between W and W':

$$\mathrm{CF}=\sqrt{\frac{1}{M}\sum_{t=1}^{M}|W'_t(x_r,z_r)-W_t(x_d,z_d)|^{2}} \tag{23}$$

The parameter estimation can be formulated as a multidimensional nonlinear problem to minimize the Cost function CF. SOMA and DE are used to find a suitable parameter a, b, c such that the Cost function CF can be asymptotical approach to minimum point. The minimum value of cost function guarantee of the best solution with suitable parameters. Systems are asymptotically synchronized.

In this simulations, the initial states of the drive system and the response system are taken as $x_d(0)=1$, $z_d(0)=1$ and $x_r(0)=1.5$, $z_r(0)=1.5$, respectively. Hence the error system has the initial values $e_1(0)=0.5$ and $e_2(0)=0.5$. SOMA-All-To-One and

DERand/1/Bin were used to solve the systems, which the control parameters setting are given in Table 1 and Table 2. Simulations were implemented using Mathematica programming language and executed on Pentium D 2.0G, 2GB personal computer.

8.1. Case study 1: simulation on one-dimensional parameter

In the first case, one-dimensional parameter estimation is considered. That means two parameters b and c (or ac, ab) are known in advance with the original value, one of a (or b, c) is unknown and needs to be estimated. The initial guesses are in the range [1,5] for a (or b, c). DE and SOMA have found the best results, and the estimated parameters were collected. Both the worst and the best values of the cost function gradually approach to minimum value after 75 generations in DE and 5 migrations in SOMA as shown in Figure 8.2 and Figure 8.3. DE and SOMA have found the optimum value of a, b, c as shown in Table 3. It can be seen that the best results (estimated values) obtained by DE and SOMA are almost the same and very close to the true values. Figure 8.4 points out that CF_a are the smallest in this case.

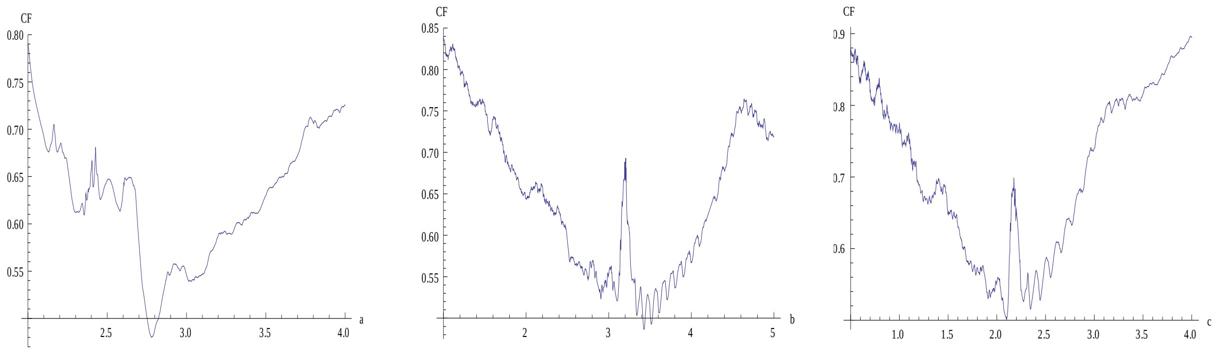


Figure 8.1. CF depending on a, b and c

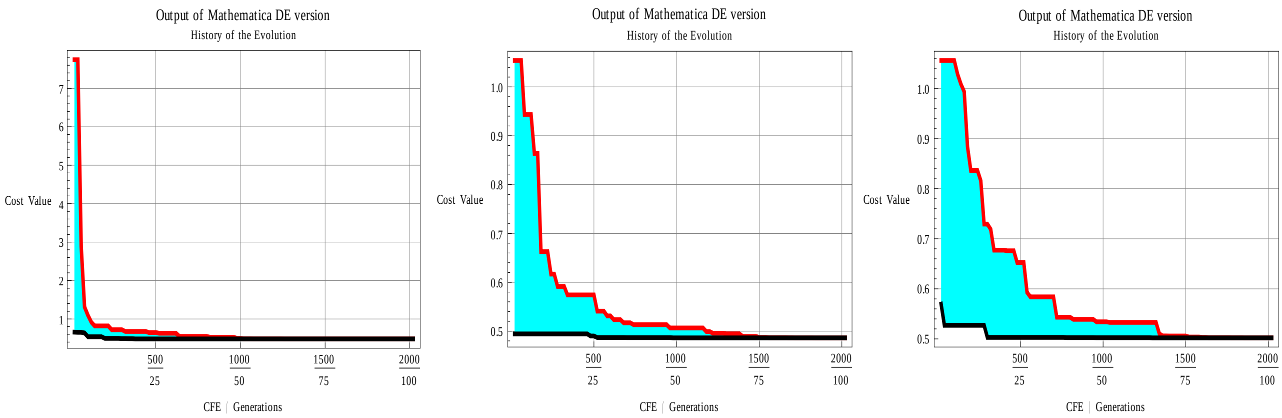


Figure 8.2. $CF_{a,b,c}$ evolution by DE

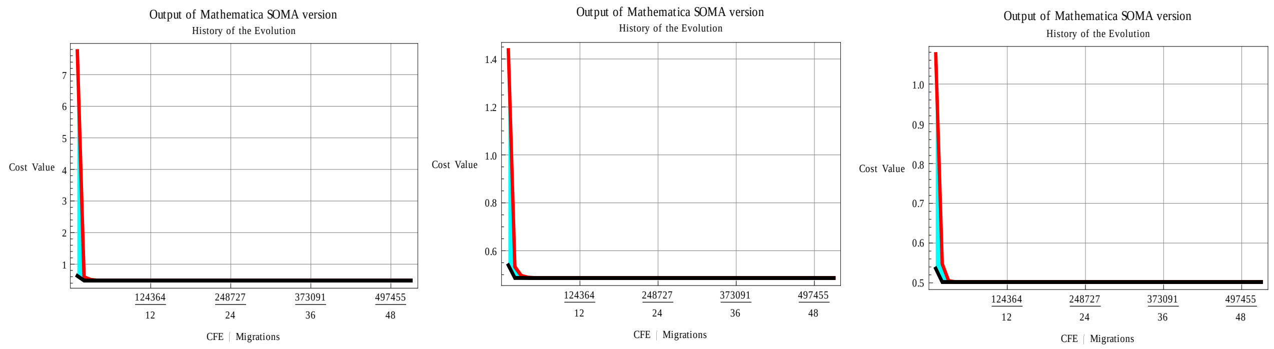


Figure 8.3. $CF_{a,b,c}$ evolution by SOMA

Table 3. 1D estimated parameters of LV system by DE and SOMA

	a	CF_a	b	CF_b	c	CF_c
DE	2.779	0.480169	3.42588	0.486321	2.10006	0.502083
SOMA	2.779	0.480169	3.42588	0.486321	2.10007	0.502083

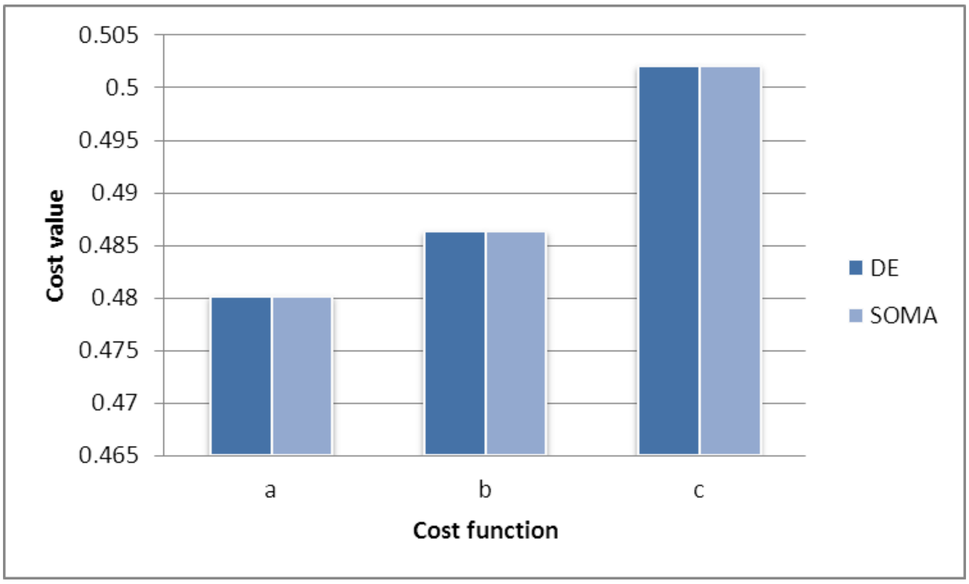


Figure 8.4. Comparison of CF by DE and SOMA

8.2. Case study 2: simulation on two-dimensional parameter

The pair parameters ab, bc or ac are unknown and need to be estimated, the other is known with the original value. The initial guesses are in the range [1, 5] for a,b,c. As shown in Figure 8.5, 3D cost functions are so complex and have a lot of local optimum. SOMA has found the best results collected with parameters a,b,c as shown in Table 4. Both the worst and the best values of cost function approach minimum gradually after 30 migrations as shown in Figure 8.7. DE has also found the best results, and both the worst and the best values of the cost function gradually approach minimum values as shown in Figure 8.6. SOMA and DE had found the optimum values of a,b,c, the cost function are minimum and the estimated parameters have the similar values with original parameters.

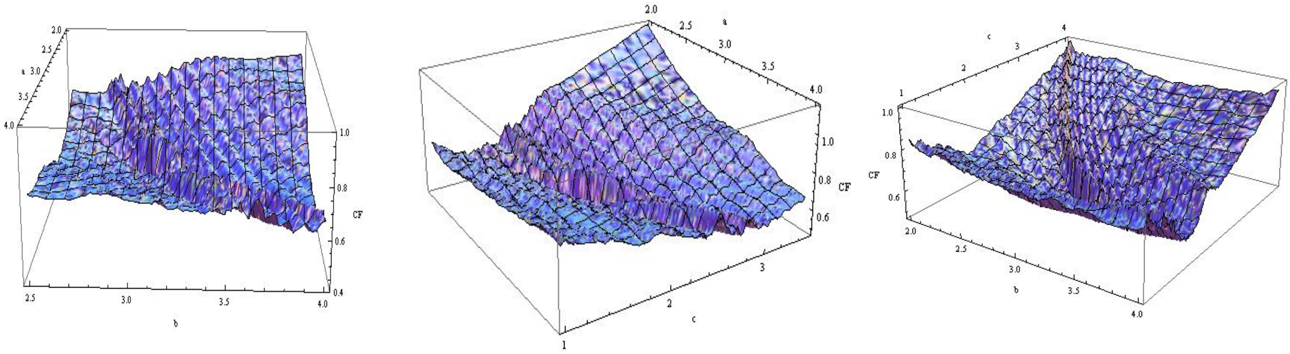


Figure 8.5. CF depending on ab, ac and bc

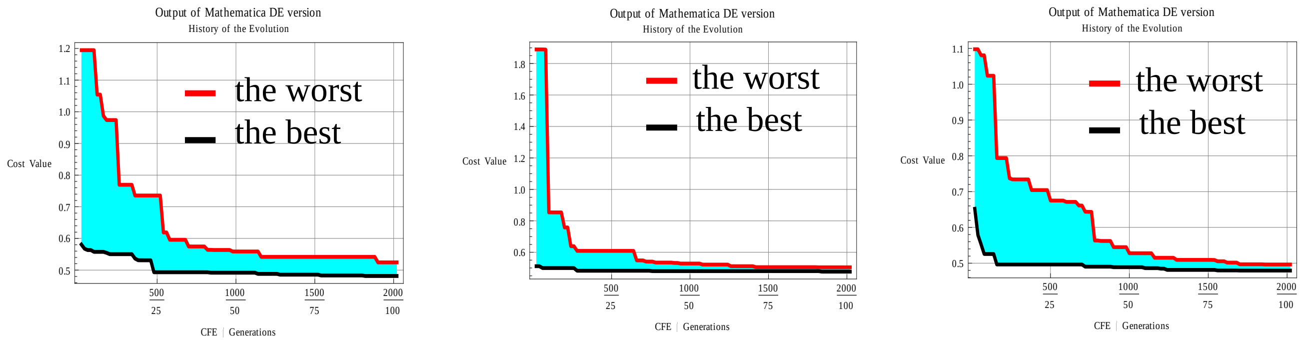


Figure 8.6. CF_{ab}, CF_{ac}, CF_{bc} evolution by DE

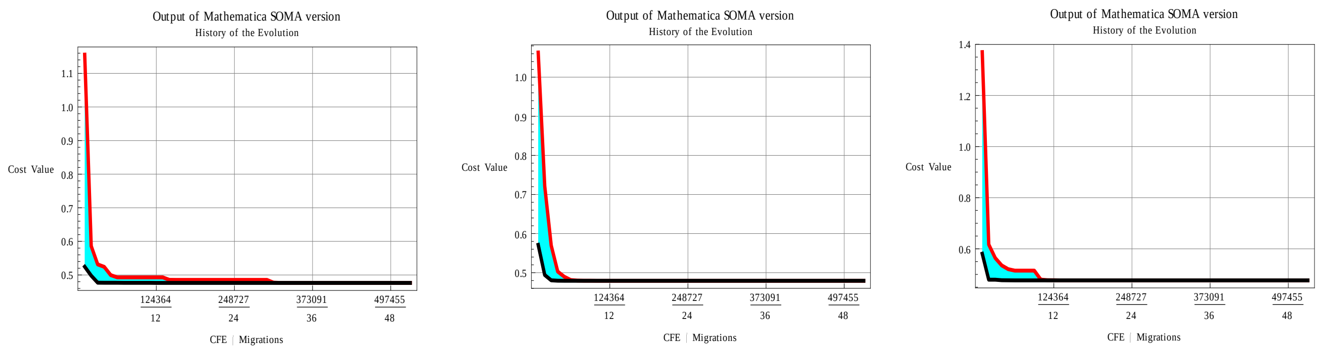


Figure 8.7. CF_{ab}, CF_{ac}, CF_{bc} evolution by SOMA

Table 4. 2D estimated parameters of LV system by DE and SOMA

	Estimated parameter			Cost function
DE	a,b	2.81069	3.02428	0.476887
	a,c	2.81069	3.02428	0.476887
	b,c	3.33735	2.08066	0.479435
SOMA	a,b	2.81306	3.02785	0.476420
	a,c	2.83086	2.03276	0.476717
	b,c	3.33753	2.08018	0.479364

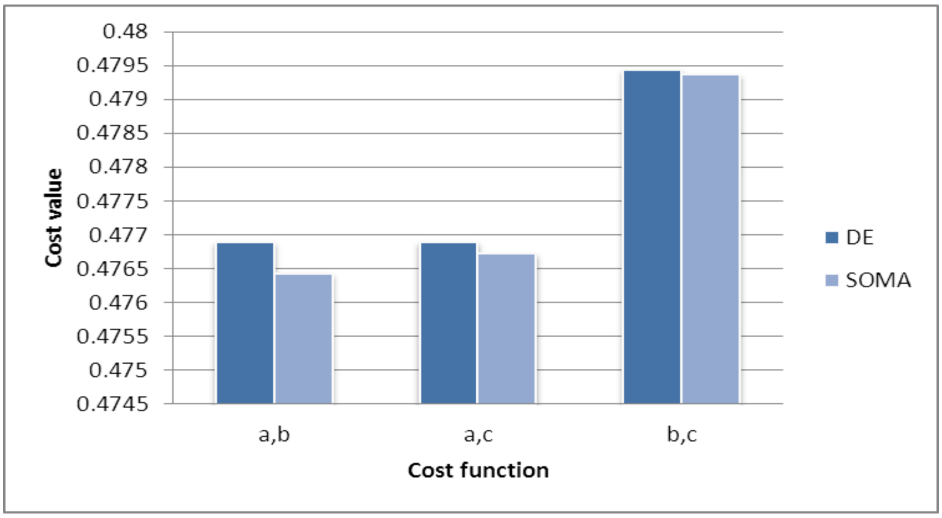
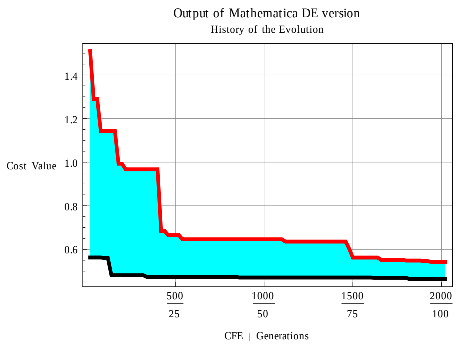


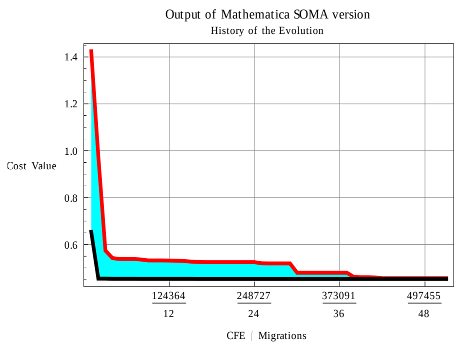
Figure 8.8. Comparison of 2D cost function by DE and SOMA

8.3. Case study 3: simulation on three-dimensional parameter

Three-dimensional simulations are considered in this part. That means all parameter a,b,c are unknown and need to be estimated. The initial guesses are in the range [1,5] for a,b,c. SOMA has found the best result was collected with parameters a,b,c as shown in Table 5. Both the worst and the best values of cost function approach minimum gradually after 40 migrations as shown in Figure 8.9.b. DE has also found the best result at the minimum CF=0.463220. After 100 generations, both the worst and the best values of the cost function gradually approach minimum value as shown in Figure 8.9.a. The estimated parameter values found by SOMA and DE have the similar values with original parameters.



(a)



(b)

Figure 8.9. CF_{abc} evolution by DE and SOMA

Table 5. 3D estimated parameters of LV system by DE and SOMA

	a	b	c	CF_{abc}
DE	3.32287	3.36376	2.25692	0.463220
SOMA	3.29627	3.36522	2.25622	0.452946

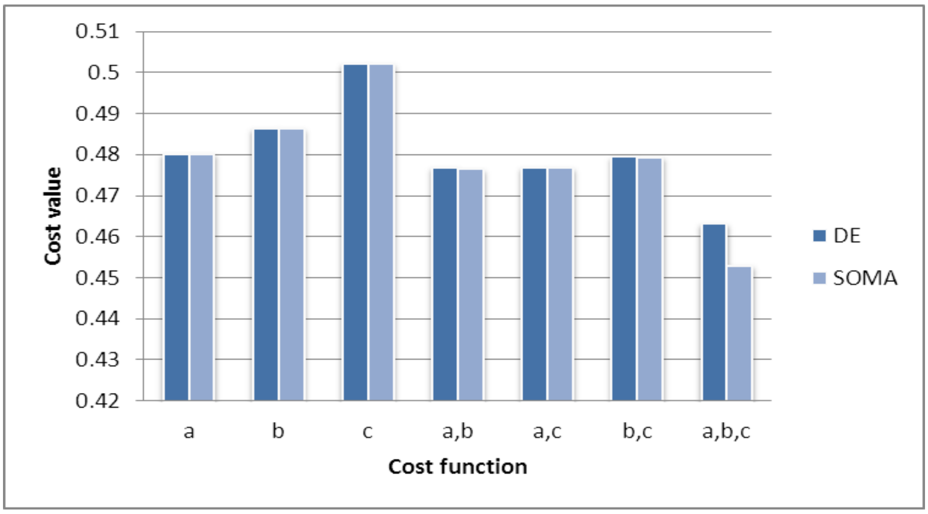


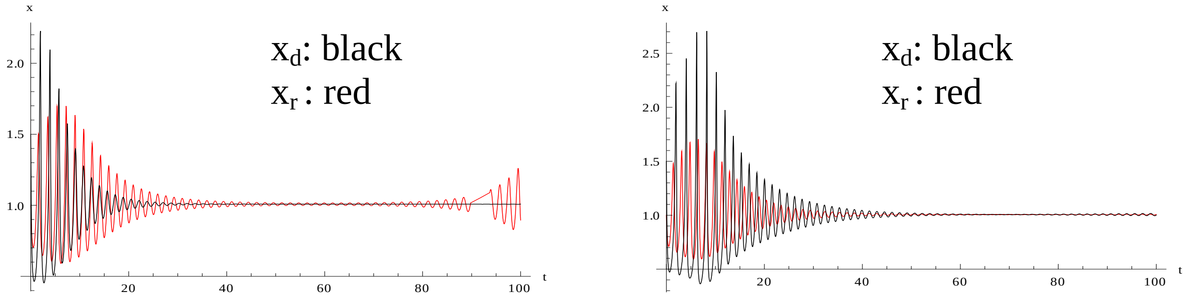
Figure 8.10. Comparison of $CF_{1D,2D,3D}$ by DE and SOMA

Figure 8.10 showed the comparison of all cost functions, the minimum CF was easily recognized at CF_{abc}, the cost function CF_{SOMA}=0.452946 is smaller than CF_{DE}=0.463220. So that, the final estimated values were chosen: a=3.29627, b=3.36522 and c=2.25622. Thus, the actual parameters were fully identified, the values of cost function always approach to minimum values. The estimated parameters obtained by SOMA and DE, and original parameters have the similar values. So, it has proven that SOMA and DE are effective to estimate parameters for chaos synchronization system.

8.4. Synchronization between two systems with estimated parameters

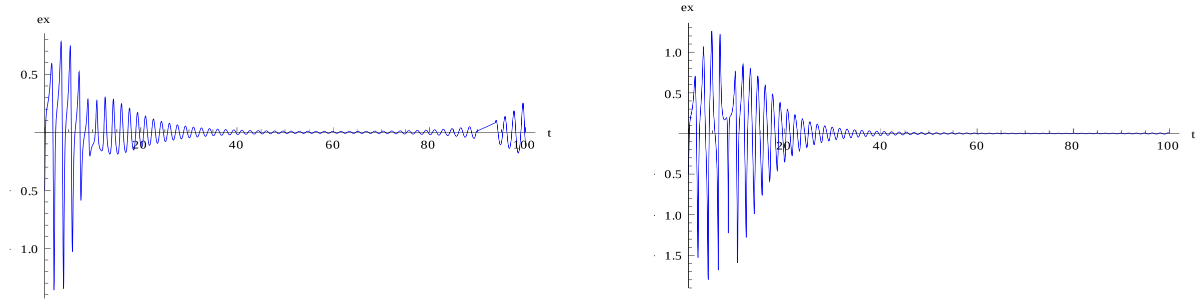
Based on the values were estimated by EA, the response system was constructed. The effective of the estimated value on the synchronization errors of driver systems X and response system Y via PC method were demonstrated.

As shown in Figure 8.11.a, Figure 8.13.a, the synchronization between two systems were not identified without PC method, and the trajectories of error e(t) were unpredicted as shown in Figure 8.12.a, Figure 8.14.a. In the opposite, Figure 8.12.b, Figure 8.13.b display that the trajectories of e(t) tends to zero after t > 50, and trajectories of x_r, z_r converged to x_d, z_d when PC was applied as shown in Figure 8.11.b, Figure 8.13.b. It has proven that the estimated values and PC method are effective to synchronize for two Lotka-Volterra chaotic systems.



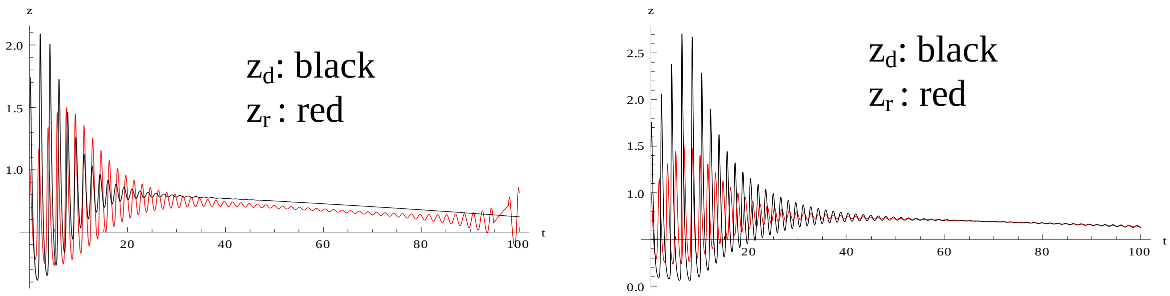
(a) (b)

Figure 8.11. a) Non-synchronization of x_d and x_r ; b) and synchronization



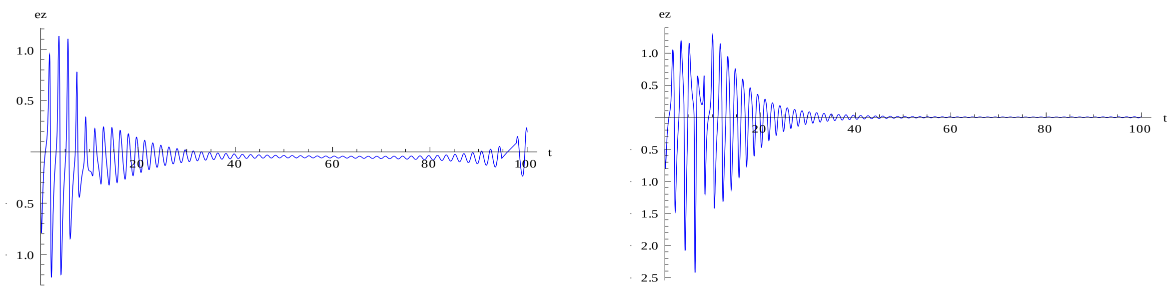
(a) (b)

Figure 8.12. Difference between x_d-x_r with and without PC and estimated parameters



(a) (b)

Figure 8.13. a) Non-synchronization of z_d and z_r ; b) and synchronization



(a) (b)

Figure 8.14. Difference between z_d-z_r with and without PC and estimated parameters

9. Synchronization of 4D Qi Chaotic System via Active-Passive Decomposition method

The ADP technique is applied to achieve the synchronization between two identical 4-D chaotic systems, which have been studied in detail by Qi [18]. A subscript d is used to denote the signals in the drive, and a subscript r is used for the signals in the response. Synchronization has been done by variables x_d. The driver system X is described by the following equations:

$$X=\begin{cases}\dot{x}=a(y_d-x_d)+y_d z_d w_d\\ \dot{y}=b(x_d+y_d)-x_d z_d w_d\\ \dot{z}=-cz_d+x_d y_d w_d\\ \dot{w}=-dw_d+x_d y_d z_d\end{cases} \tag{24}$$

And the response system Y is described by the following equations:

$$Y=\begin{cases}\dot{x}=a(y_r-x_r)+y_r z_r w_r\\ \dot{y}=b(s_t+y_r)-x_r z_r w_r\\ \dot{z}=-cz_r+x_r y_r w_r\\ \dot{w}=-dw_r+x_r y_r z_r\end{cases} \tag{25}$$

where a, b, c and d are unknown parameters in response system, $s_t=x_d$ is the transmitted signal.

Consider the difference of these two systems e=Y – X. The synchronization of the pair of identical systems (24) and (25) occurs if the dynamical system describes the evolution of the difference $|Y_{(t)}-X_{(t)}|\to 0$ as t $\to\infty$. Subtracting system (24) from system (25) yields the error dynamical system between two system e_t=($(x_r,y_r,z_r,w_r)_t-(x_d,y_d,z_d,w_d)_t$) which were used to create a cost function CF representing the root mean square error (RMSE) of synchronization between X and Y:

$$\text{CF}=\sqrt{\frac{1}{m}\sum_{t=1}^{m}|Y_t\,(x_r,y_r,z_r,w_r)-X_t(x_d,y_d,z_d,w_d)|^{\,2}} \tag{26}$$

The parameter estimation can be formulated as a multidimensional nonlinear problem to minimize the cost function CF. DE and SOMA are used to find a suitable parameter a, b, c and d such that the cost function CF can be asymptotical approach to minimum point. The minimum value of cost function guarantee of the best solution with suitable parameters. Systems are asymptotically synchronized.

In this simulations, the initial states of the drive system and the response system are taken as $x_d(0)=5$, $y_d(0)=2$, $z_d(0)=1$, $w_d(0)=1$ and $x_r(0)=3$, $y_r(0)=1$, $z_r(0)=2$, $w_r(0)=2$, respectively. Hence the error system has the initial values $e_x(0)=2$, $e_y(0)=1$, $e_z(0)=-1$ and $e_w(0)=-1$. DERand/1/Bin and SOMAATO were used to find the optimal value of CF and estimated parameters.

9.1. Case study 1: simulation on one-dimensional parameter

First at all, we assume that parameters a, b, c were known in advance and d was unknown, the initial guesses are in the range [5, 15] for d. As shown in Figure 9.1, the cost function CF looks so complex and have a lot of local optimum. But after 35 generations as shown in Figure 9.2.a, DE has found the best results of CF=0.884101, the best values of the cost function approach to minimum value quickly. DE had found the optimum value of d= 10.0315 as shown in Figure 9.3.a. SOMA has also found the best results with estimated parameter d=10.0213, the cost function approaches minimum value after 12 migrations as shown in Figure 9.2.b, with evolution history of parameter d can be seen in Figure 9.3.b.

Similar to others, the initial guesses are in the range for $a\in[25,35]$, $b\in[5,15]$ and $c\in[0,2]$; the estimated parameter a, b, c were also found by SOMA and DE as shown in Table 6. It can be seen that the best results (estimated values) obtained by SOMA and DE are almost the same. Both SOMA and DE had found the optimum value of CF with estimated parameters. The minimum value of CF is recognized at $CF_{a\text{-}DE}$ as shown in Figure 9.4

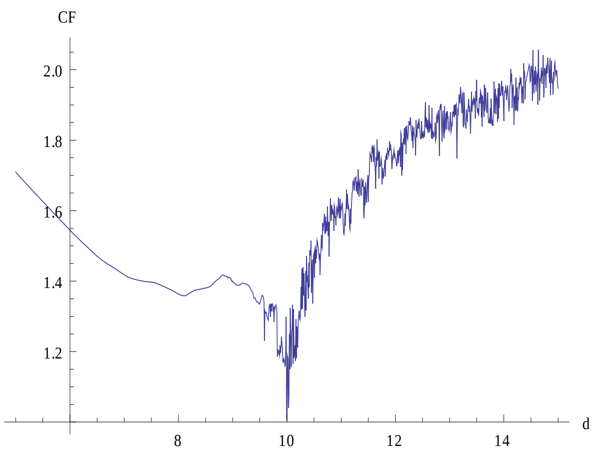
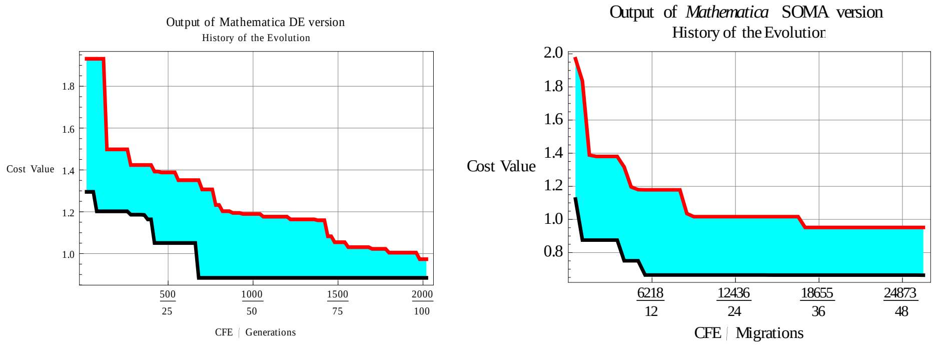
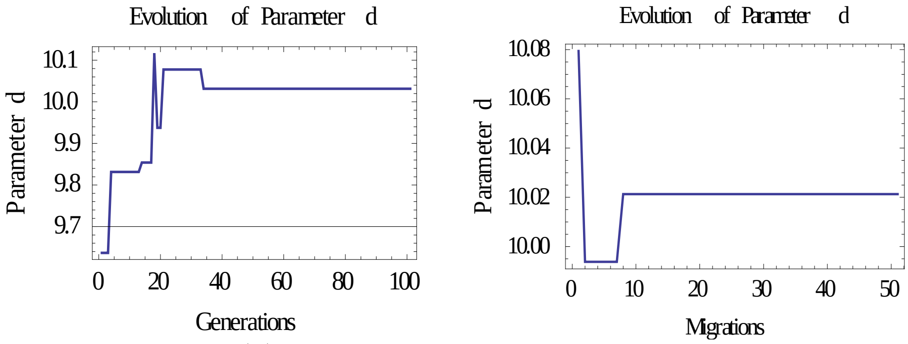


Figure 9.1. CF depending on d



(a) (b)

Figure 9.2. CF_d evolution by DE and SOMA



(a) (b)

Figure 9.3. History evolution of d by DE and SOMA

Table 6. 1D estimated parameters of Qi system by DE and SOMA

	Estimated parameter		Cost function	
	DE	SOMA	DE	SOMA
a	30.9750	30.6612	0.858905	0.984790
b	10.0157	10.0058	0.976032	0.962670
c	0.99879	0.99731	0.973315	0.990173
d	10.0315	10.0213	0.884101	0.863452

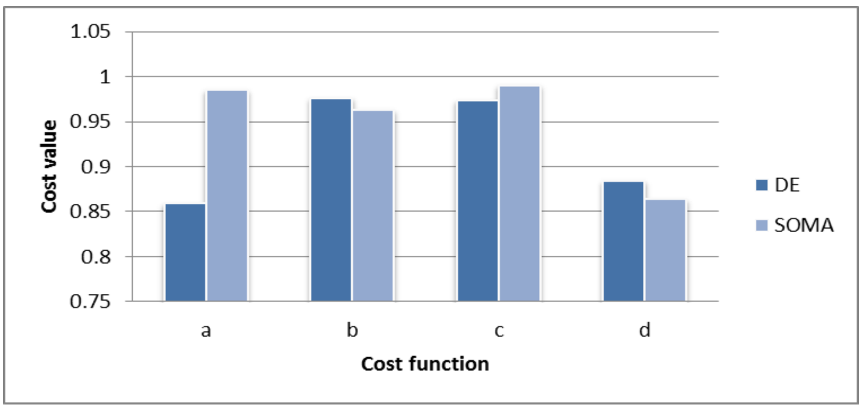


Figure 9.4. Comparison of 1D cost function by DE and SOMA

9.2. Case study 2: simulation on two-dimensional parameter

Second, the two-dimensional parameter estimation is considered. That means the pair parameters ab, ac or ad, *etc*… are unknown and need to be estimated, the others were known with the original value. The initial guesses are in the range for $a \in [25,35]$, $b \in [5,15]$, $c \in [0,2]$, $d \in [5,15]$. When the pair parameter b, c is unknown, 3D cost function is complex as shown in Figure 9.5. EA has found the best results of CF, which were collected with parameters b, c by DE and SOMA. The best values of CF approach to minimum gradually after 75 generations in DE and 15 migrations in SOMA as shown in Figure 9.6.

The same for the others, 3D cost functions are also complex with a lot of local optimum. But this problem was solved by DE and SOMA. The estimated parameters were found as shown in Table 7. These results have the similar values with original parameters. Both SOMA and DE pointed out that the minimum cost function is CF_{ac}=0.946636 as can be seen in Figure 9.7.

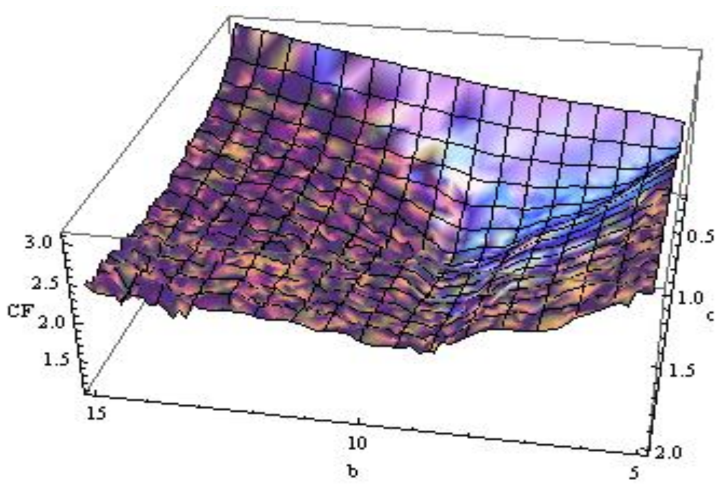
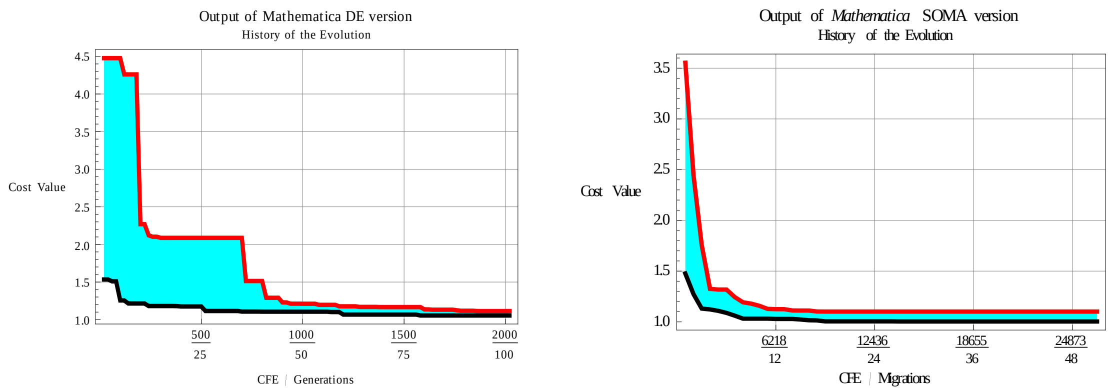


Figure 9.5. CF depending on b and c



(a) (b)

Figure 9.6. CF_{bc} evolution by DE and SOMA

Table 7. 2D estimated parameters of Qi system by DE and SOMA

	Estimated parameter			Cost function
DE	a,b	34.9270	10.07280	0.978242
	a,c	34.8526	0.949745	0.946636
	a,d	34.8742	10.13280	0.962033
	b,c	9.67836	0.894254	1.055130
	b,d	9.70204	10.32910	1.108310
	c,d	0.91972	9.723660	1.150370
SOMA	a,b	34.9270	10.07280	0.978242
	a,c	34.8526	0.949745	0.946636
	a,d	34.8742	10.13280	0.962033
	b,c	9.67836	0.894254	1.055130
	b,d	9.70204	10.32910	1.108310
	c,d	0.91972	9.723660	1.150370

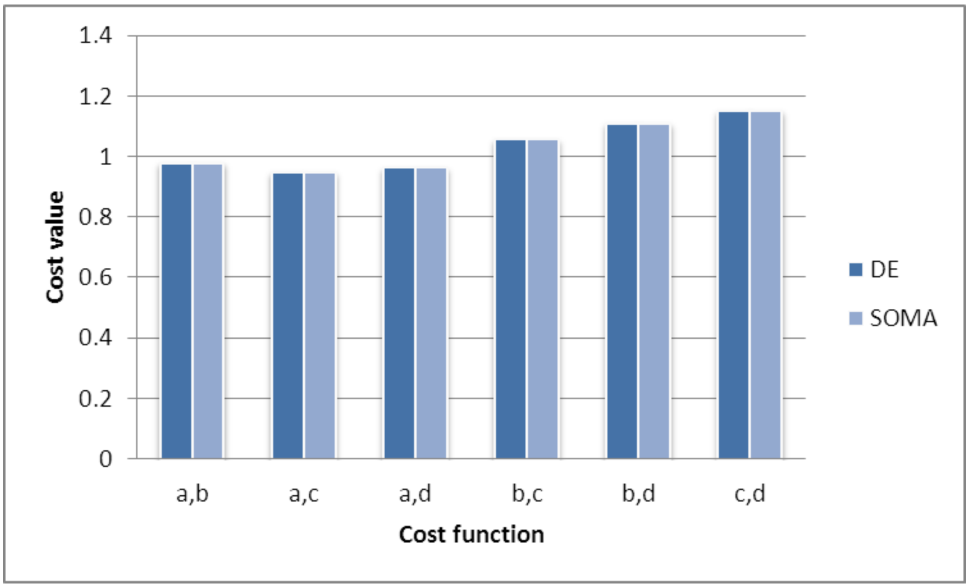


Figure 9.7. Comparison of 2D cost function by DE and SOMA

9.3. Case study 3: simulation on 3 and 4-dimensional parameter

The last of these experiments, we consider 3D and 4D parameter estimations. The group of parameters abc, abd, bcd or all parameter a, b, c, d are unknown and need to be estimated. DE and SOMA has also found the best results of CF, the estimated parameters (a, b, c, d) were collected as shown in Table 8. The history evolution of the best values of cost function gradually approaches to minimum as shown in Figure 9.8. The estimated parameters collected by DE and SOMA, which are similar together, and also similarly with the original parameters.

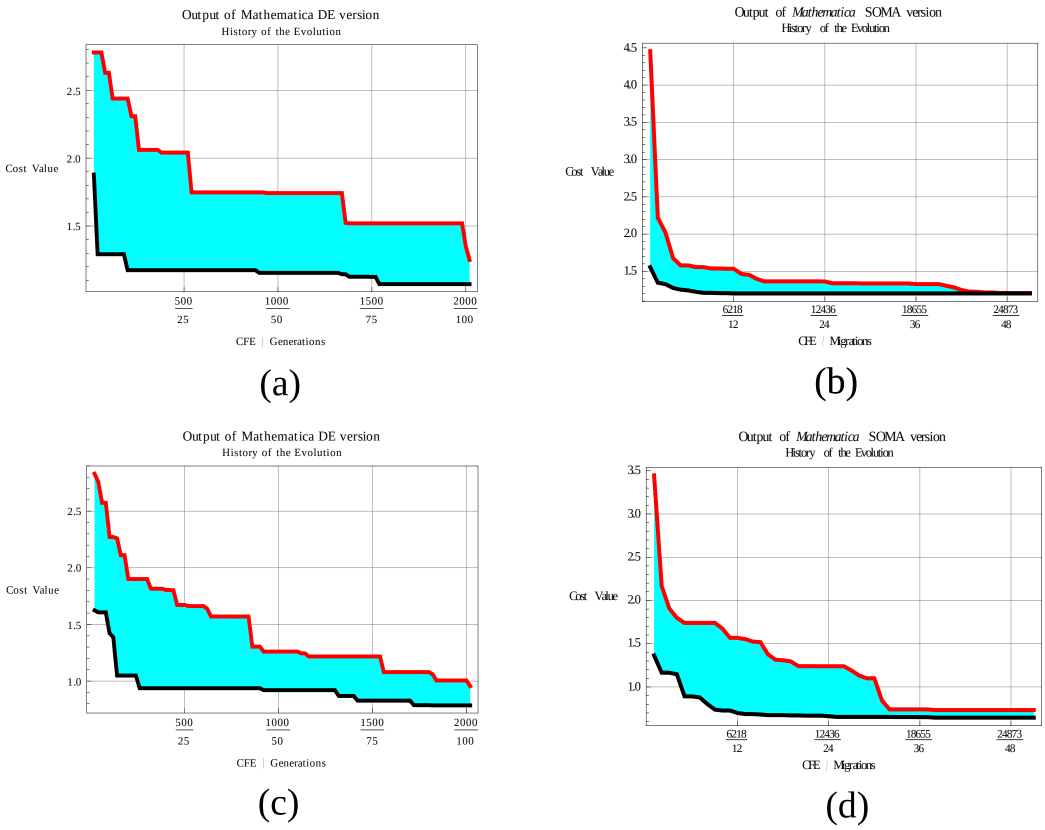


Figure 9.8. CF_{bcd}, CF_{abcd} evolution by DE (a, c) and SOMA (b, d)

Table 8. 3,4 D estimated parameters of Qi system by DE and SOMA

		Estimated parameters				Cost function
		a	b	c	d	
DE	3D	32.6767	9.65742	0.87802		0.819492
		32.8903	9.41245		10.5771	0.820018
			9.55362	0.96593	10.3546	1.072620
	4D	32.9425	9.43714	0.92480	10.3062	0.785671
SOMA	3D	32.7773	9.70486	0.87753		0.804929
		32.7776	9.48361		10.5594	0.733430
			8.96513	0.93814	9.84057	1.202670
	4D	32.8538	9.47672	0.99035	10.5400	0.644608

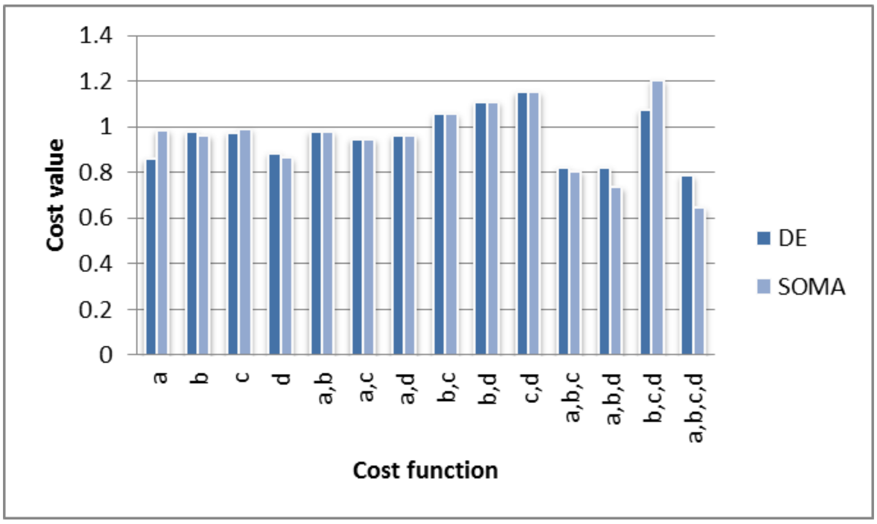


Figure 9.9. Comparison of CF by DE and SOMA

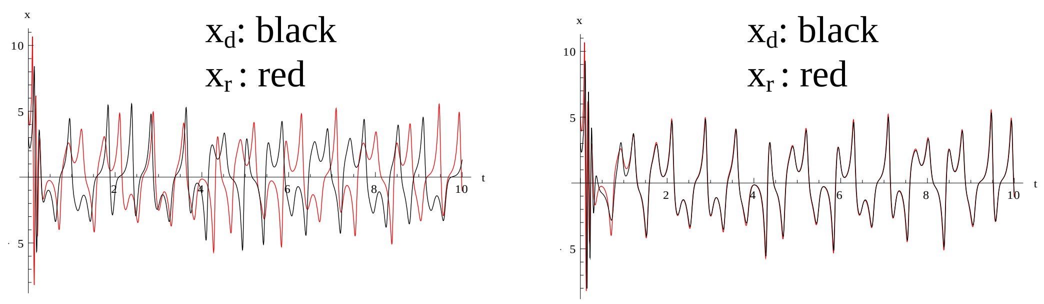
After several experiments, the values of cost function always approach to minimum values. The estimated parameters obtained by DE and SOMA, which are like to the value of original parameters. So, it has proven that DE and SOMA were efficient to estimate parameters for 4D-chaos synchronization system.

The minimum CF can be recognized at $CF_{4D\text{-}SOMA}$ in Figure 9.9. So that, the final estimated values were chosen: a=32.8538, b=9.47672, c=0.99035 and d=10.5400. Thus, the actual parameters were fully identified.

9.4. Synchronization of 4D Qi chaotic system with estimated parameters

Based on the values were estimated by SOMA, the response system was constructed. The effects of the estimated values on the synchronization errors of driver systems X and response system Y via APD method were demonstrated as shown in Figure 9.10-Figure 9.13.

Without ADP, the synchronization between x_d and x_r was not synchronization as shown in Figure 9.10.a. In the opposite, Figure 9.10.b displays that the trajectories of x_r converged to x_d when ADP was applied with estimated parameters.



(a) (b)

Figure 9.10. a) Non-synchronization of x_d and x_r ; b) and synchronization

This is also the same for the others (y,z,w) as shown in Figure 9.11-Figure 9.13. It has proven that the estimated values and APD method are efficient to synchronize for two 4D-chaotic systems.

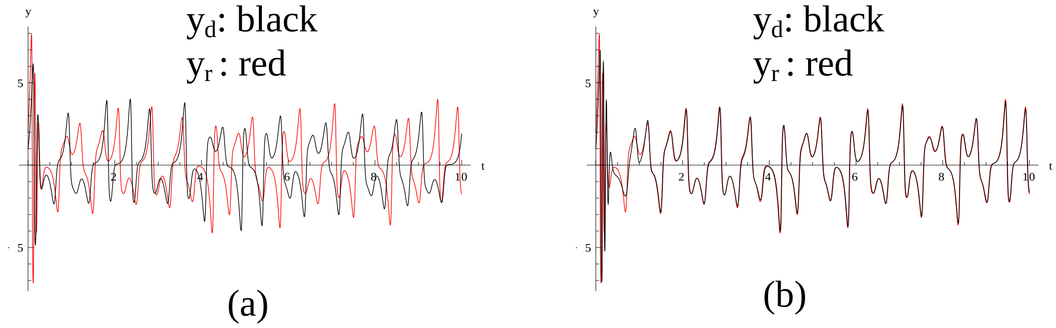


Figure 9.11. a) Non-synchronization of y_d and y_r ; b) and synchronization

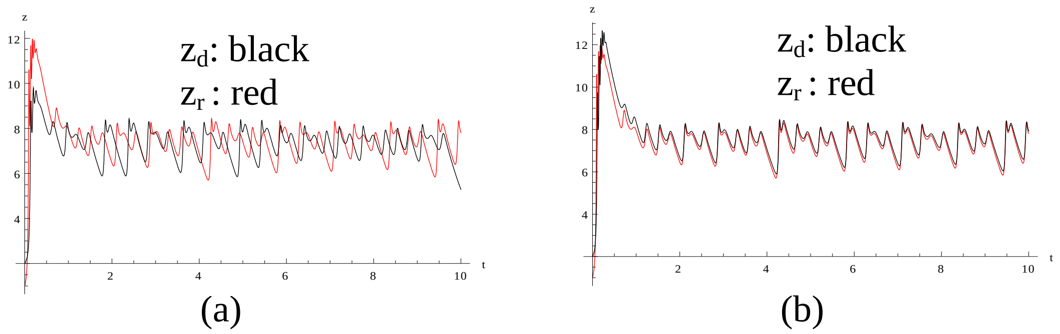


Figure 9.12. a) Non-synchronization of z_d and z_r ; b) and synchronization

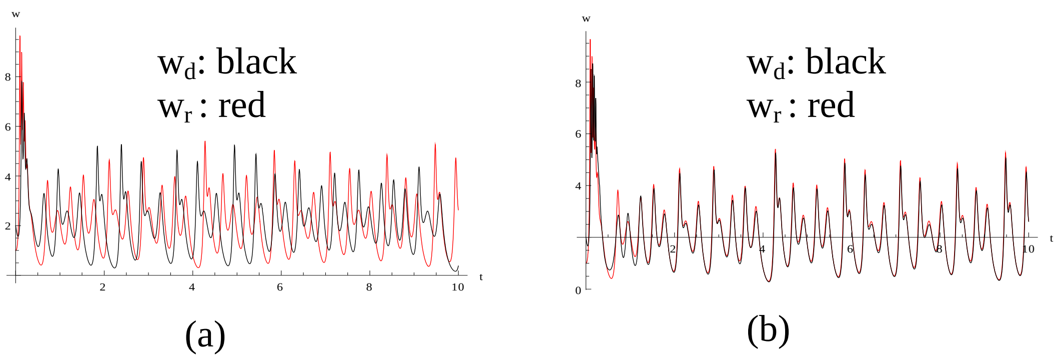


Figure 9.13. a) Non-synchronization of w_d and w_r ; b) and synchronization

10. Synchronization of 4D Liu Chaotic System via Feedback method

The Feedback technique is applied to achieve the synchronization between two identical 4D Liu systems. Using a subscript 'd' denotes the signals in the drive, and using a subscript 'r' for the signals in the response. Synchronization has been done by coupling of variables x_d, x_r via control parameter g. The driver system U is described by the following equations:

$$U=\begin{cases}\dot{x}_d = a(y_d - x_d)\\ \dot{y}_d = bx_d - kx_d z_d + w_d\\ \dot{z}_d = -cz_d + hx_d^{\ 2}\\ \dot{w}_d = -dx_d\end{cases} \qquad (27)$$

And the response system U'^c is described by the following equations:

$$U'^{c}=\begin{cases}\dot{x}_r = a(y_r - x_r) - g(x_r - x_d)\\ \dot{y}_r = bx_r - kx_r z_r + w_r\\ \dot{z}_r = -cz_r + hx_r^{\ 2}\\ \dot{w}_r = -dx_r\end{cases} \qquad (28)$$

where a, b, c, d, h, k and g are unknown parameters in response system.

Consider the difference of these two systems e=U´^{c} – U. The synchronization of the pair of identical systems (6) and (7) occurs if the dynamical system describes the evolution of the difference $|U'^{c}_{(t)} - U_{(t)}| \to 0$ as $t \to \infty$.

Subtracting system (6) from system (7) yields the error dynamical system between two system e_t=($(x_r, y_r, z_r, w_r)_t - (x_d, y_d, z_d, w_d)_t$) which were used to create a cost function CF representing the root mean square error (RMSE) of synchronization between U and U´^{c}:

$$CF=\sqrt{\frac{1}{m}\sum_{t=1}^{m}|U'^{c}_{t}(x_r, y_r, z_r, w_r) - U_t(x_d, y_d, z_d, w_d)|^{\ 2}} \qquad (29)$$

The parameter estimation can be formulated as a multidimensional nonlinear problem to minimize the cost function CF. DE and SOMA are used to find a suitable parameter a, b, c, d, h, k and g such that the cost function CF can be asymptotical approach to minimum point. The minimum value of cost function guarantees of the best solution with suitable parameters. Systems are synchronized via estimated parameters.

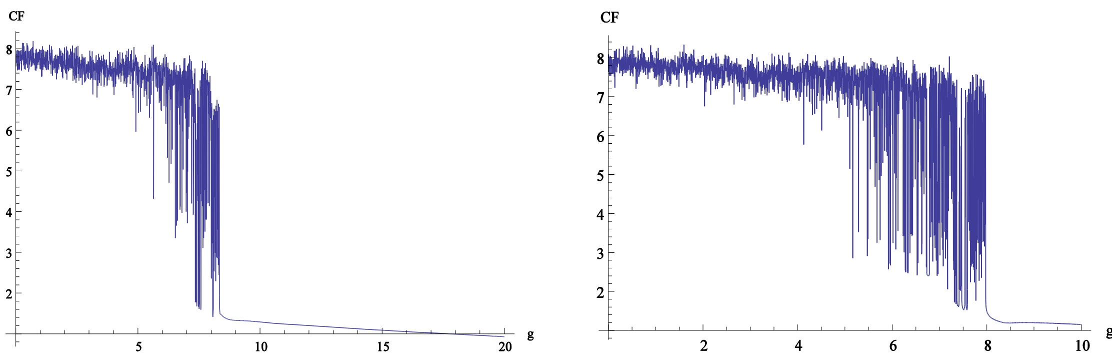
The initial states of the drive system and the response system are taken as $x_d(0)=1$, $y_d(0)=2$, $z_d(0)=1$, $w_d(0)=1$ and $x_r(0)=12$, $y_r(0)=1$, $z_r(0)=10$, $w_r(0)=-1$, respectively. Hence the error system has the initial values $e_x(0)=11$, $e_y(0)=-1$, $e_z(0)=9$ and $e_w(0)=-2$. DE and SOMA were used to solve the systems, which the control parameters setting are given in Table 1 and Table 2. Simulations were implemented using Mathematica programming language and executed on Pentium D 2.0G, 2GB personal computer.

10.1. Case study 1: simulation on one-dimensional parameter

In first case, we consider one-dimensional parameter estimation. That means just one of parameters a, b, c, d, h, k, g was unknown and needed to be estimated, the others were known in advance with original value.

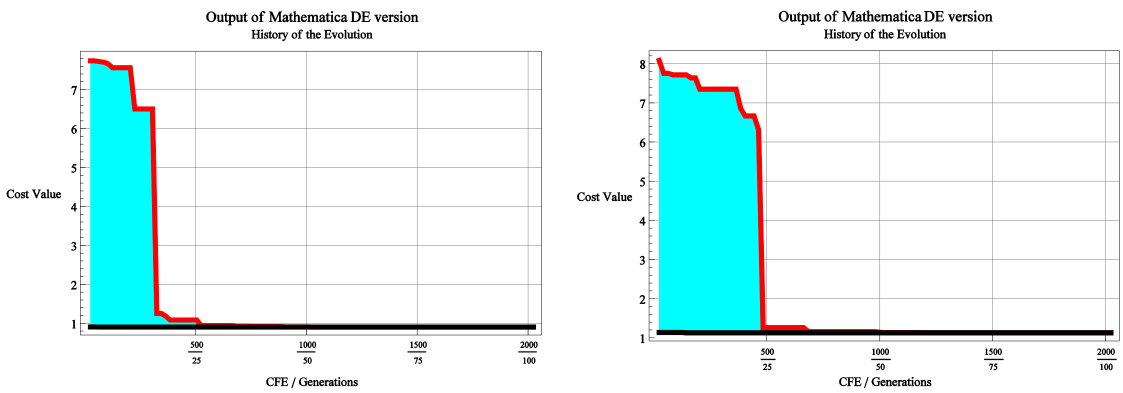
First at all, we assume that control parameter g is unknown, the initial guesses are in the range [0, 20] for g, and the control parameters were set as Table 1. DE has found the best results of CF=0.92615, both the worst and the best values of the cost function approach minimum value quickly after 25 generations as shown in Figure 10.2(a). The minimum value of CF is found at g=19.9998 as shown in Figure 10.1(a).

When the initial g guesses in range [0,10], we also got the similar result, the estimated parameter g=9.99999 had been found by DE. The value of cost function CF is 1.21594 as shown in Figure 10.1.(b). It can be seen that the estimated values g located in the right of the chosen range. As referred in literature, the value of control parameter g was increased from zero, CF got a complex result with g belong 0 to 8, from g≥8, the cost function value (CF) incline to the right of the chosen range as can be seen in Figure 10.1. That means the synchronization appeared with g≥8.



(a) $CF_g(0,20)$ (b) $CF_g(0,10)$

Figure 10.1. Cost function depending on parameter g



(a) $CF_g(0,20)$ (b) $CF_g(0,10)$

Figure 10.2. History evolution of CF_g

The CF value decreased when parameter g increased, the cost-function approaches the minimum when 'g' approaches infinity. However, an infinity value could not be chosen in this case, a relative value g=10 are chosen to ensure that the synchronization is done.

When a control parameter was chosen g=10. We assume that parameter a is unknown, the others were known in advance with original value, the initial guesses are in the range [0,20] for a. Figure 10.4.a. showed the complexity of cost function and there are a lot of local optimum. But after 60 generations, DE has been successful in finding the optimum result of CF, and parameter a=10.0001 was collected. Both the worst and the best values of the cost function gradually approach minimum value after 60 generations as shown in Figure 10.5.a.

Similar to others, with b Є [30,50], c Є [0,5], d Є [10,30], h Є [0,10], k Є [0,5]. These CF also have a lot of local optimum as shown in Figure 10.3. Similarly as above, the best results of parameters b, c, d, k, h were also collected as shown in Table 9. As can be seen in Figure 10.3, the minimum value of 1D cost function CF_{1D}=1.21328 is achieved with a=10, b=40, c=2.5, h=4, k=1 and estimated parameter d=19.9978.

Table 9. 1D estimated parameters of Liu system by DE

	Estimated parameters	Cost function
a	10.0001	1.21593
b	40.0000	1.21595
c	2.50010	1.21561
d	19.9978	1.21328
h	3.99944	1.21417
k	0.99988	1.21514

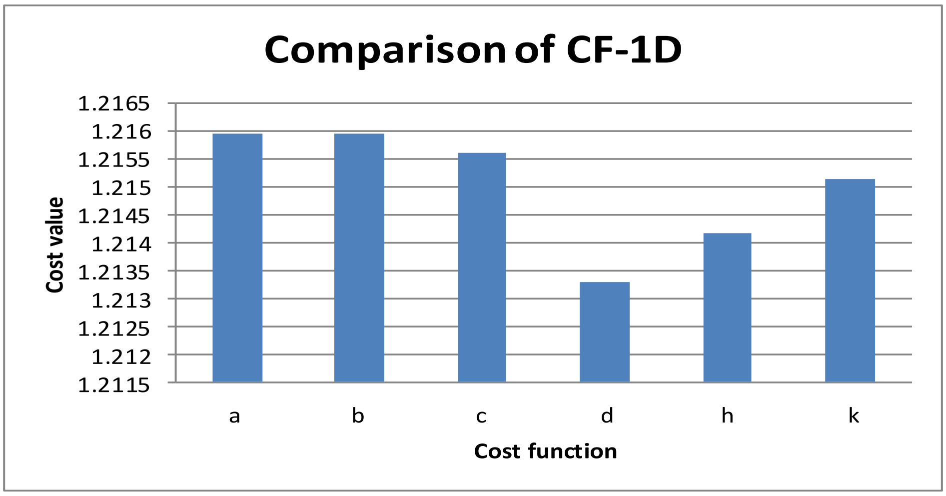
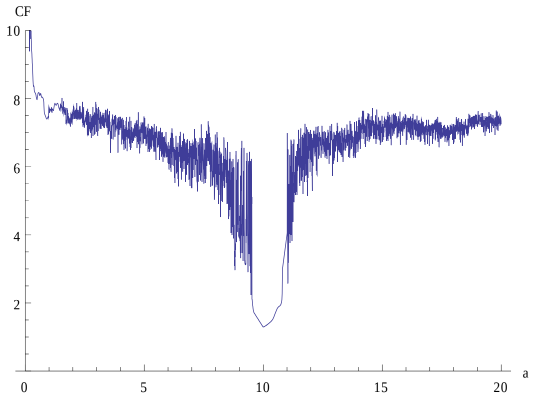
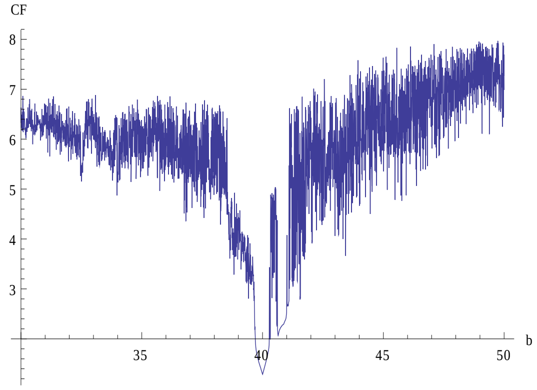


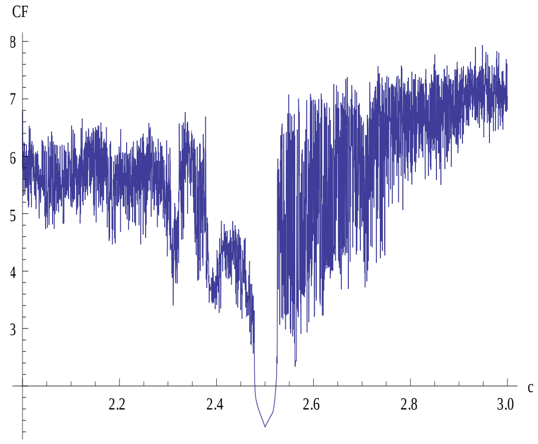
Figure 10.3. Comparison of 1D cost function



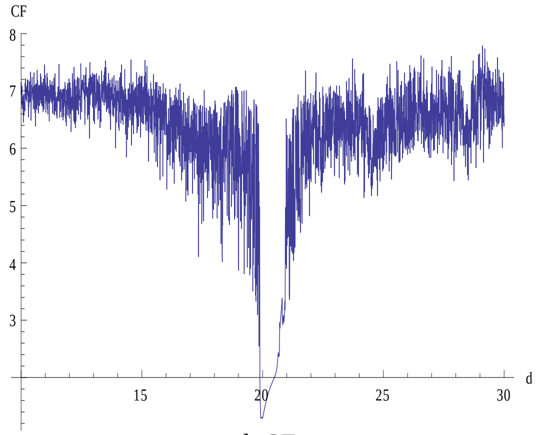
a. CF_a



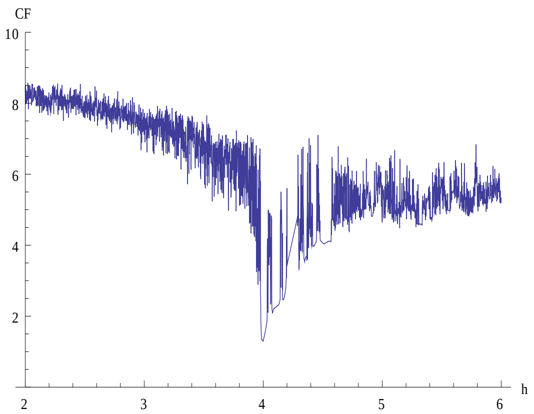
b. CF_b



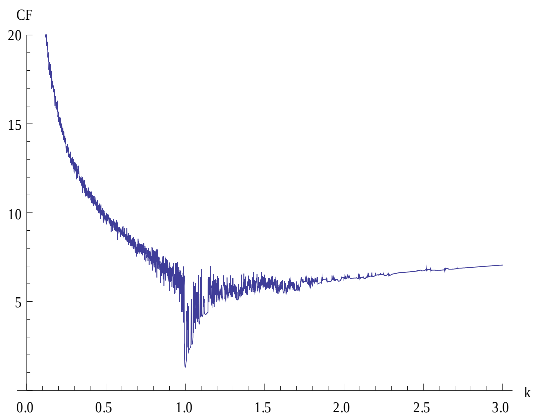
c. CF_c



d. CF_d

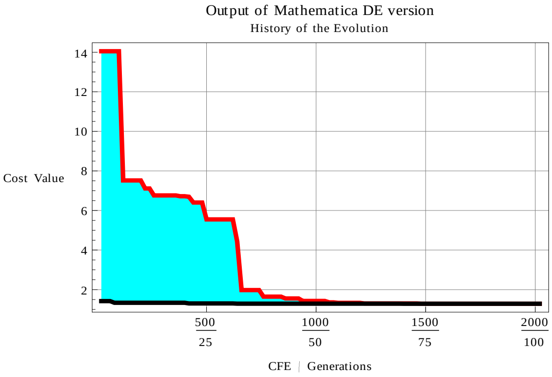


e. CF_h

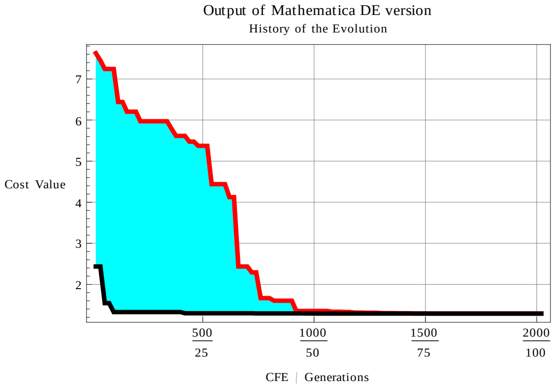


f. CF_k

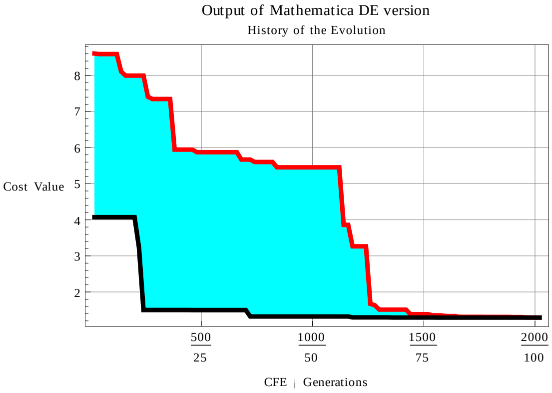
Figure 10.4. Cost function depending on 1 parameter



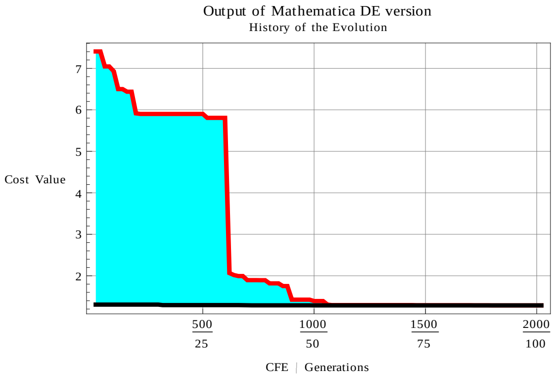
a. CF_a



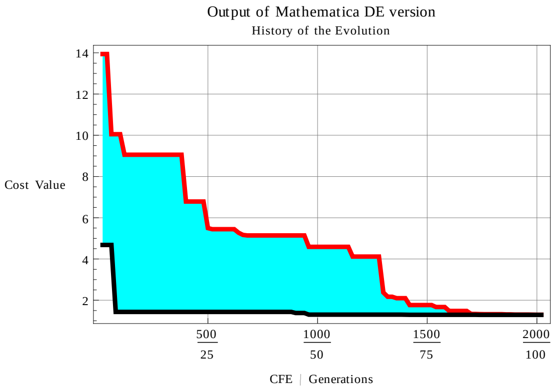
b. CF_b



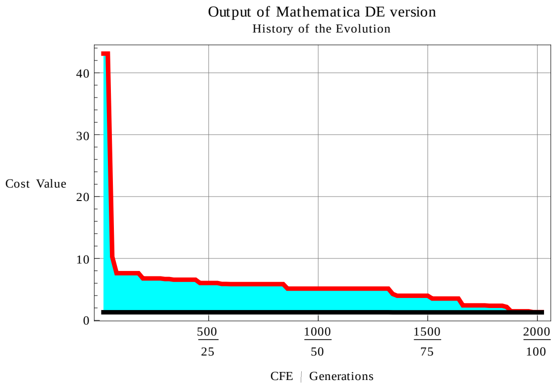
c. CF_c



d. CF_d



e. CF_h



f. CF_k

Figure 10.5. History evolution of $CF_{a,b,c,d,h,k}$

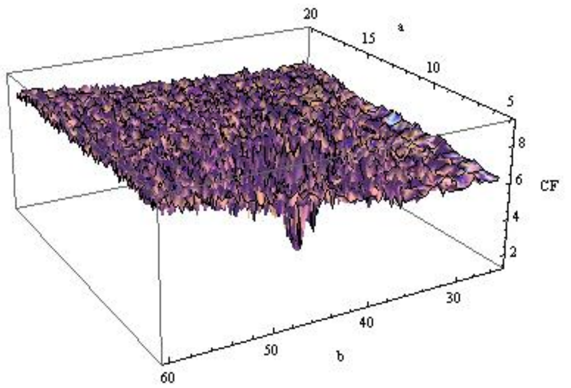
10.2. Case study 2: simulation on two-dimensional parameter

In this case, two-dimensional parameter estimation is considered. That means the pair parameters ab, ac or ad, *etc*… were unknown and needed to be estimated, the others were known with the original value and g=10. The initial guesses are in the range for $a \in [0,20]$, $b \in [30,50]$, $c \in [0,5]$, $d \in [10,30]$, $h \in [0,10]$, $k \in [0,5]$. When the pair parameter a,b are unknown, cost function so complex as shown in Figure 10.6.a. DE has been successful in finding the optimum result of CF_{ab}. The best value of CF approaches minimum gradually after 50 generations, and the worst value also approaches minimum after 65 generations as shown in Figure 10.6.b.

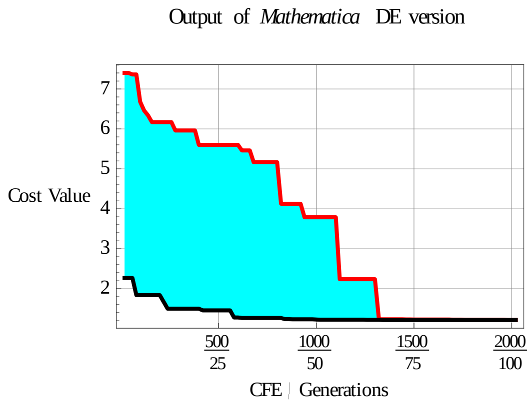
The same for the others, the estimated parameters were found by DE as shown in Table 10. The estimated parameters have the similar value with original parameters. From comparison Figure 10.7, the minimum CF_{2D}=1.21465 is collected with estimated parameters a=10.0038, k=0.99985 and original value of parameters b,c,d,h.

Table 10. 2D estimated parameters of Liu system by DE

	Estimated parameter		Cost function
a,b	10.0018	39.9992	1.21620
a,c	10.0209	2.50026	1.22343
a,d	10.0922	19.9427	1.25945
a,h	10.0026	4.00840	1.32523
a,k	10.0038	0.99985	1.21465
b,c	39.9358	2.50564	1.26759
b,d	40.1128	20.0392	1.36760
b,h	40.1250	3.98963	1.34315
b,k	39.9577	1.00006	1.24608
c,d	2.49675	19.9783	1.24195
c,h	2.50004	3.99938	1.21502
c,k	2.50132	1.00087	1.36667
d,h	20.0621	3.99041	1.30076
d,k	19.9954	1.00012	1.21481
h,k	3.98863	1.00109	1.33481



a. CF depending on a and b



b. CF_{ab} evolution by DE

Figure 10.6. Cost function depending on ab and history evolution

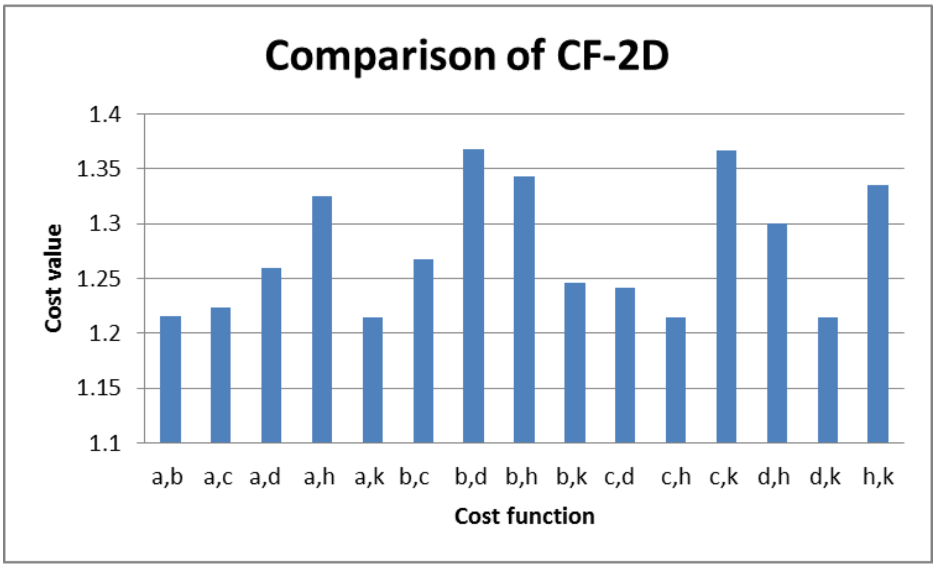


Figure 10.7. Comparison of 2D cost function

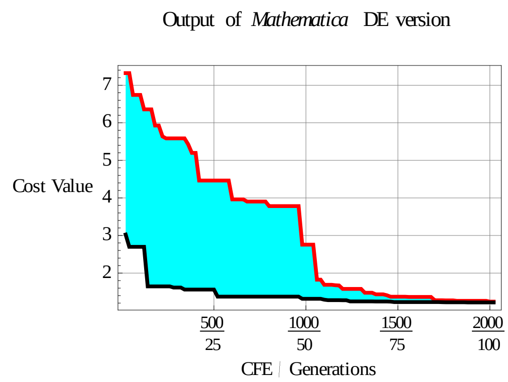
10.3. Case study 3: simulation on 3,4,5,6 dimensional parameter

The group of parameters abc, abcd,.., abcdhk are unknown and need to be estimated in this case. DE has also found the best results collected with parameters a,b,c,d,h,k as shown in Table 11. The best values of CF approach minimum gradually as shown in the history evolution Figure 10.8.

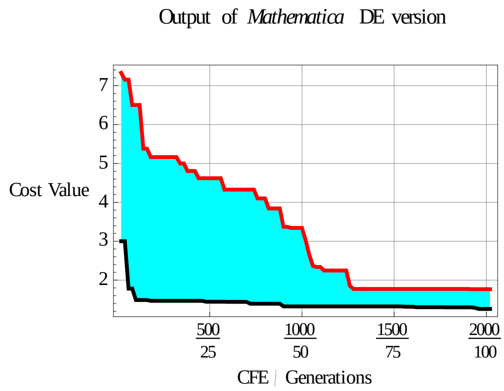
Table 11. 3-6D estimated parameters of Liu system by DE

	Estimated parameters						Cost function
	a	b	c	d	h	k	
3D	10.0012	40.0001	2.50022				1.21518
4D	10.0037	40.0023	2.49952	19.9938			1.21082
5D	10.0054	40.0044	2.49933	19.9949	3.99938		1.21072
6D	10.0028	40.0081	2.49943	19.9965	3.99863	1.00017	1.21006

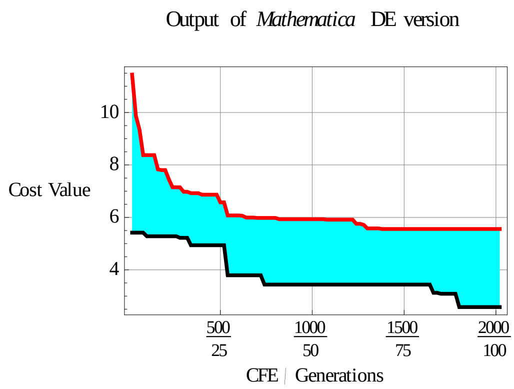
As shown in Figure 10.5, Figure 10.6.b and Figure 10.8, the values of CF always approach to minimum. The estimated parameters obtained by DE and original parameters have the similar values. So, it demonstrated that DE was effective to estimate parameters for 4D-chaos synchronization system.



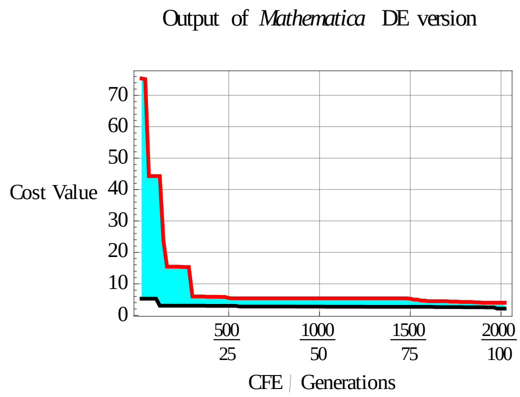
a. CF_{abc}



b. CF_{abcd}



c. CF_{abcdh}



d. CF_{abcdhk}

Figure 10.8. Evolution history of 3-6D estimation by DE

To compare with DE, SOMA is used to estimate the parameters of response system. The strategy rule SOMA-All-To-All is used with migration=20 in this study. SOMA has found the best results of CF and parameters as presented in Table 12. The estimated parameters by SOMA and DE have the similar value together.

Table 12. Estimated parameters of Liu system by SOMA

	Estimated parameters						Cost function
	a	b	c	d	h	k	
1D				19.9978			1.21328
2D	10.0037					0.99987	1.21447
3D	10.0012	39.9999	2.50022				1.21518
4D	10.0132	39.9958	2.50042	19.9966			1.22486
5D	10.1307	39.9742	2.48898	19.9292	3.99966		1.32890
6D	10.0054	40.0576	2.49753	20.0139	3.98601	1.00148	1.22587

Using the best results from case study 1, 2 and data of Table 11 and Table 12, the comparison of CF_{1D}, CF_{2D}, .., CF_{6D} was displayed in Figure 10.9. The results in each case are similar together, the smallest value of CF was recognized at $CF_{6D\text{-}DE}$=1.21006. Thus, the final estimated values were chosen to ensure that the synchronization error approaches to minimum, the actual parameters were identified with a=10.0028, b=40.0081, c=2.49943, d=19.9965, h=3.99863, k=1.00017 and control parameter g=10.

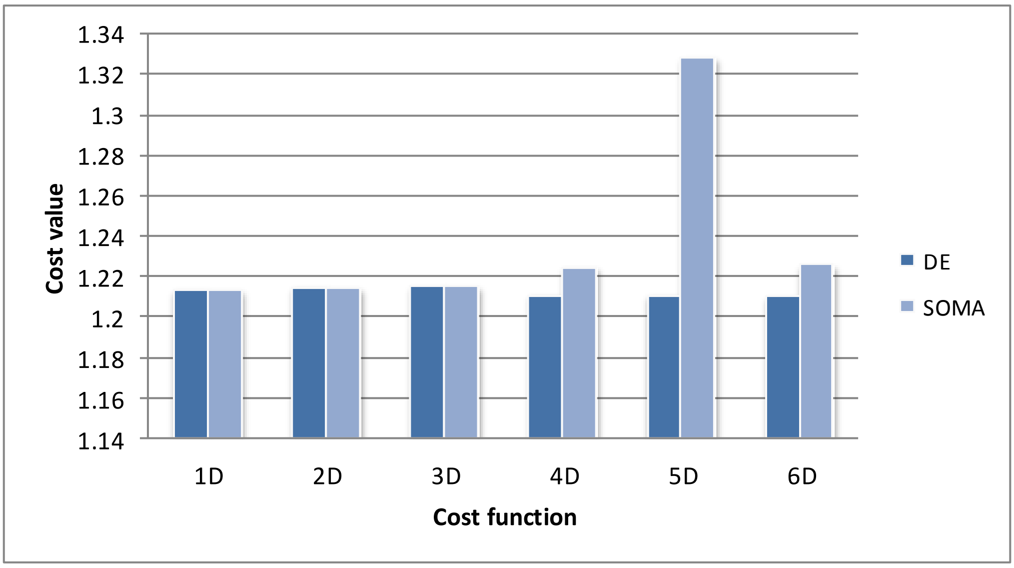
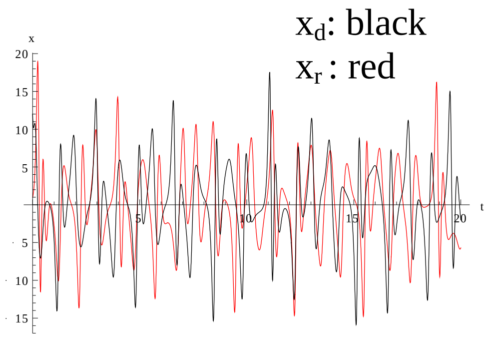


Figure 10.9. Comparison of 1-6D cost function

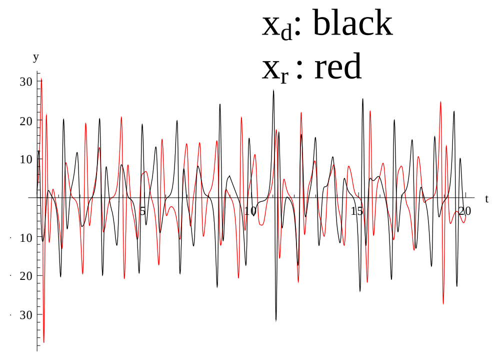
10.4. Synchronization of 4D Liu chaotic system with estimated parameters

Based on the values were estimated by DE, the response system was constructed. The effective of the estimated value on the synchronization errors of driver systems U and response system U'^{c} via feedback method were demonstrated as shown in Figure 10.12 and Figure 10.13.

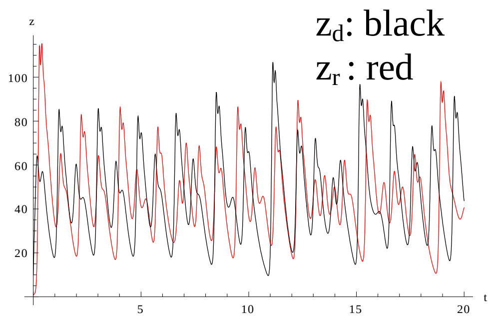
As shown in Figure 10.10, the synchronization between two systems did not exist with g=7, and the trajectories of error e(t) were unpredicted as shown in Figure 10.11. As can be seen below (with g=10), Figure 10.12 displayed that the trajectories of error e(t) approached to minimum after t>15, and trajectories of x_s, y_s, z_s, w_s converged to x_m, y_m, z_m, w_m when FB method was applied as shown in Figure 10.13. It showed that the estimated values and feedback method were effective in synchronization of two 4D chaotic systems.



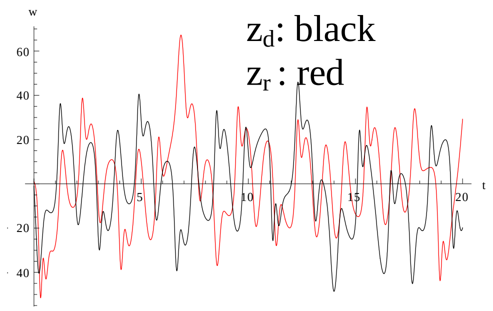
a. x_d and x_r



b. y_d and y_r

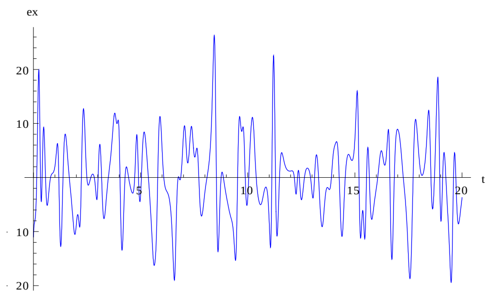


c. z_d and z_r

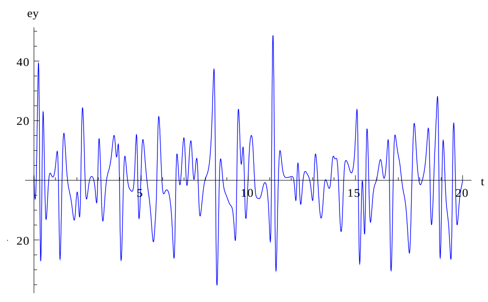


d. w_d and w_r

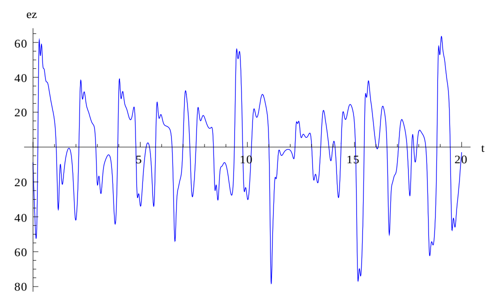
Figure 10.10. Non-synchronization when g=7



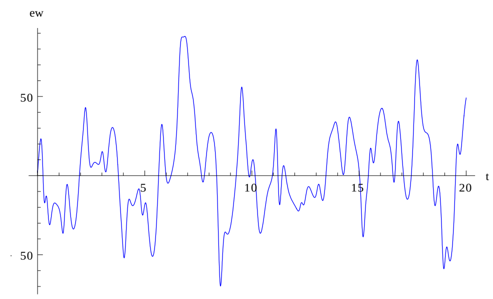
a. x_d-x_r



b. y_d-y_r

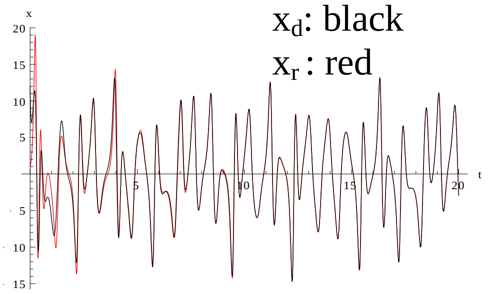


c. z_d-z_r

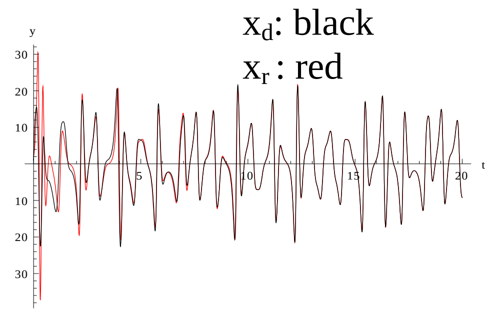


d. w_d-w_r

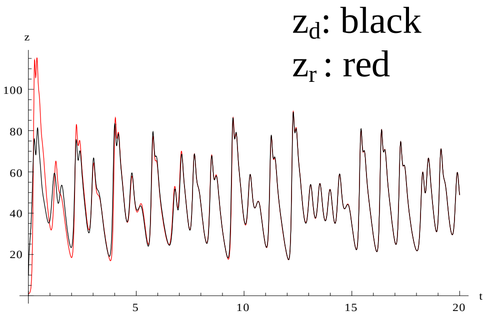
Figure 10.11. Difference between driver and response when g=7



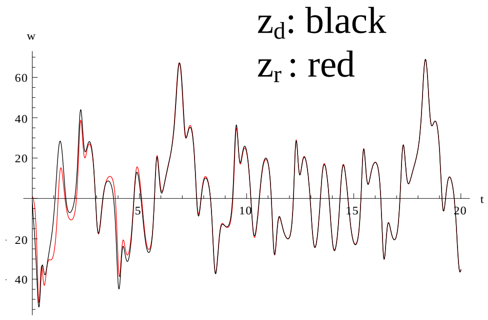
a. x_d and x_r



b. y_d and y_r

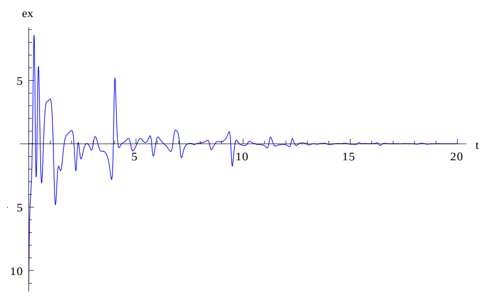


c. z_d and z_r

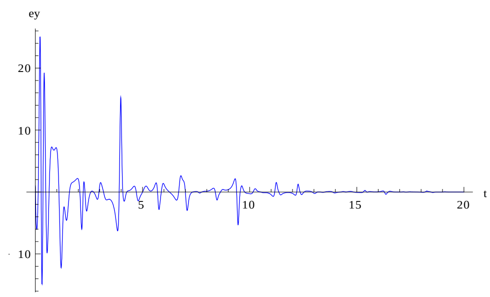


d. w_d and w_r

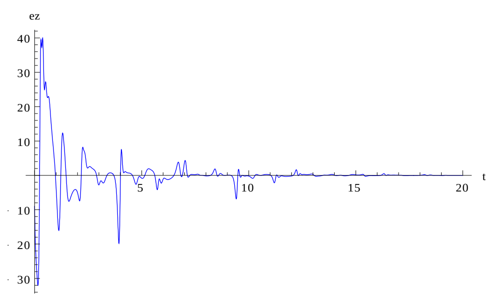
Figure 10.12. Synchronization when g=10



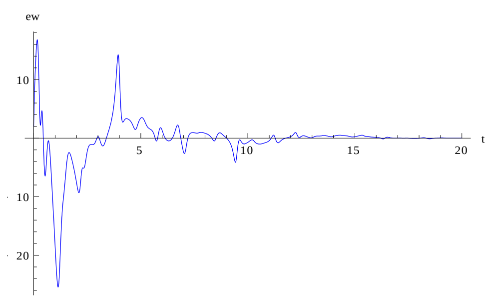
a. x_d-x_r



b. y_d-y_r



c. z_d-z_r



d. w_d-w_r

Figure 10.13. Difference between driver and response when g=10

This result indicated that the cost function was achieved with estimated parameters $CF_{estimated}$=1.21006 is smaller than that of original parameters $CF_{original}$=1.21595. The synchronization error which was achieved with estimated parameters was smaller as shown in Figure10.14. The quality of synchronization will be better with the smaller synchronization error. Therefore, it can be stated that the optimum of synchronization was executed by estimated parameters in case g was chosen in advance.

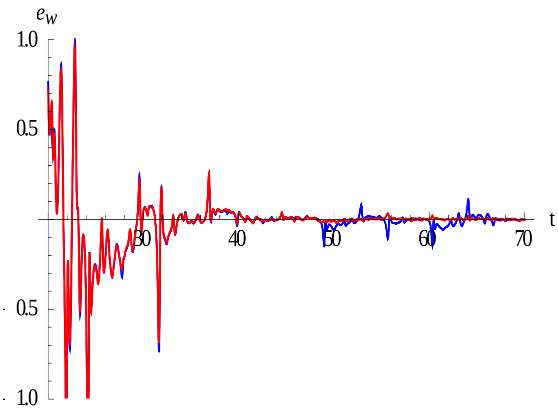


Figure10.14. Comparison of synchronization error between original parameters (blue line) and estimated parameters (red line)

In this part, the feedback method was applied to synchronize two identical Liu 4D-chaotic systems. The control parameter g had strong effect in synchronization system. Increasing g from 8 to infinity, the synchronization quality was gradually incremented between transmitter and receiver, while the synchronization could not achieve with g from 0 to 8. The infinity value of g ensures for the minimum synchronization error, but it cannot be used in real world. A relative value g=10 was chosen, and the synchronization error was used to formulate as a cost function. Differential evolution was used to estimate the optimum values for unknown parameters, and it easily escaped the local optimum trap and achieved the global optimum parameters. SOMA was executed to compare with DE. Based on the estimated parameters, the synchronization of two chaotic systems was done. The value of estimated-cost function was smaller than that of the original-cost function; it indicated that the estimated parameters are optimal choice in this case.

11. Synchronization of 5D Lorenz Chaotic System

In this chapter, the Pecora and Carroll technique is applied to synchronize two identical 5D chaotic systems. A subscript d is used to denote the signals in the drive and r for the signals in the response. Using x of the decomposed subsystems as the driving signal, x was injected into the response system. Since $x_d = x_r = x$, we only consider the following drive and response subsystems:

$$U_d = \begin{cases} \dot{y} = rx_d - y_d - z_d x_d \\ \dot{z} = x_d y_d - bz_d + 2u_d w_d \\ \dot{u} = -cau_d + 2(a/c)w_d \\ \dot{w} = -2u_d z_d + 2ru_d - c_d w_d \end{cases} \quad (30)$$

And the response system Ur is described by the following equations:

$$U_r = \begin{cases} \dot{y} = rx_r - y_r - z_r x_r \\ \dot{z} = x_r y_r - bz_r + 2u_r w_r \\ \dot{u} = -cau_r + 2(a/c)w_r \\ \dot{w} = -2u_r z_r + 2ru_r - cw_r \end{cases} \quad (31)$$

where a, b, c and r are unknown parameters in response system.

Consider the difference of these two systems $e = U_d - U_r$. The synchronization of the pair of identical systems (30) and (31) occurs if the dynamical system describes the evolution of the difference $\left\| U_d(t) - U_r(t) \right\| \to 0$ as $t \to \infty$. Subtracting system (31) from system (30) yields the error dynamical system between two system e(t)=$U_d(t) - U_r(t)$ which were used to create a cost function CF representing the root mean square error (RMSE) of synchronization between U_d and U_r:

$$\text{CF} = \sqrt{\frac{1}{m} \sum_{t=1}^{m} |(y_d, z_d, u_d, w_d)_{(t)} - (y_r, z_r, u_r, w_r)_{(t)}|^2} \quad (32)$$

The parameter estimation can be formulated as a multidimensional nonlinear problem to minimize the cost function CF. EA is used to find a suitable parameter a, b, c and r such that the cost function CF can be asymptotical approach to minimum point. The minimum CF guarantee for the best solution with suitable parameters.

SOMA-All-To-All and DERand1Bin were used to solve the systems in these simulations, the initial states of the drive system and the response system are taken as $x_d(0)=x=1$, $y_d(0)=2$, $z_d(0)=1$, $u_d(0)=1$, $w_d(0)=1$ and $x_r(0)=x=1$, $y_r(0)=-2$, $z_r(0)=-1$, $u_r(0)=-1$, $w_r(0)=-1$, respectively. Hence the error system has the initial values $e_x(0)=0$, $e_y(0)=4$, $e_z(0)=2$, $e_u(0)=2$ and $e_w(0)=2$. Simulations were implemented using Mathematica programming language and executed on Pentium D 2.0G, 2GB personal computer.

11.1. Case study 1: simulation on one-dimensional parameter

In this case, one-dimensional parameter estimation is considered. That means three parameters are known in advance with the original value; the parameter "**a**" is unknown and needs to be estimated. The initial guesses are in the range [5,15] for a. SOMA has found the best results presented in Table 13, both the worst and the best values of the cost function approach minimum value quickly after 3 migrations as shown in Figure 11.1.a. SOMA had found the optimum value of "**a**" as shown in Figure 11.2.a. DE has also found the best results with estimated parameter as shown in Table 13, both the worst and the best values of the cost function gradually approach minimum value after 25 generations as shown in Figure 11.1.b with evolution history can be seen in Figure 11.2.b.

Similar to others, the initial guesses are in the range for $b\in[0,5]$, $c\in[0,5]$ and $r\in[20,30]$; the estimated parameter b, c, r were also found by SOMA and DE as shown in Table 13. It can be seen that the best results (estimated values) obtained by SOMA and DE are almost the same and very close to the true values. Both SOMA and DE had found the optimum value of CF with estimated parameters.

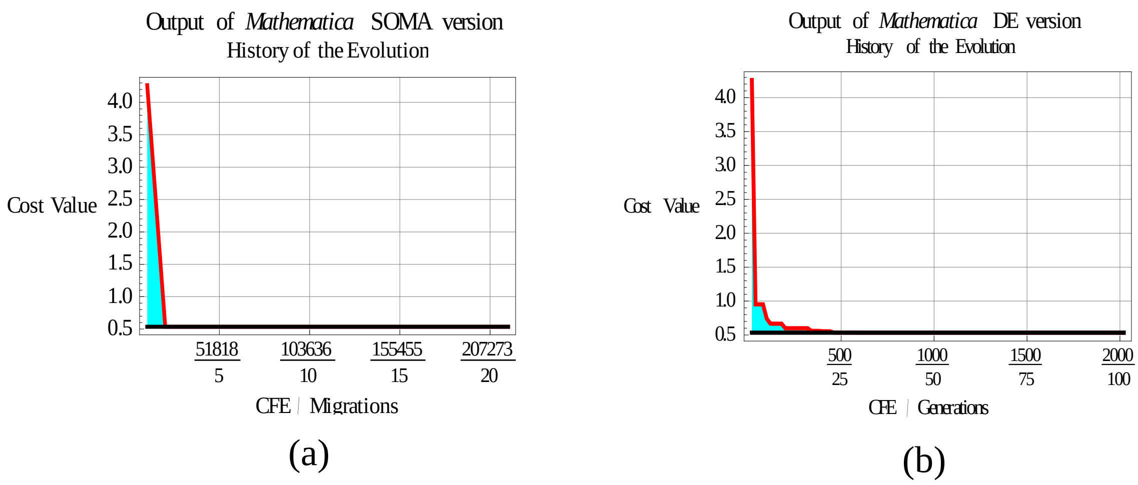
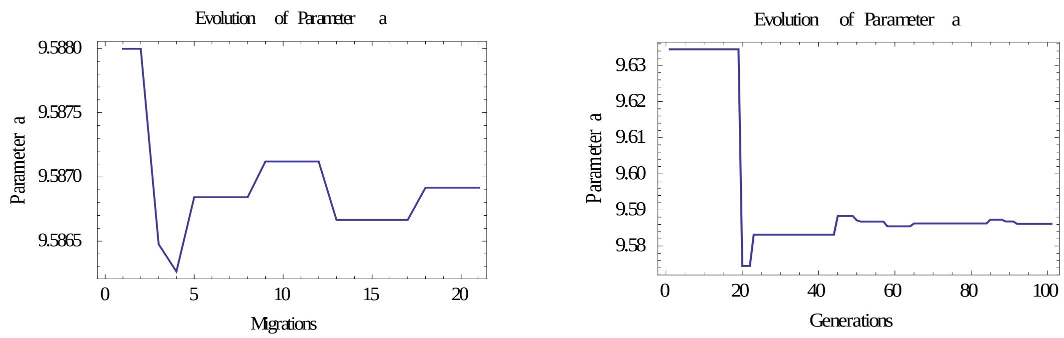


Figure 11.1. CF_a evolution



(a) (b)

Figure 11.2. Evolution history of a

Table 13. 1D Estimated parameters of 5D system by SOMA and DE

Estimated parameters			Cost function (CFa, CFb,CFc,CFd)	
	DE	SOMA	DE	SOMA
a	9.58614	9.58692	0.533740	0.533740
b	2.66667	2.66667	0.534798	0.534797
c	2.05215	2.05214	0.478855	0.478853
r	24.7500	24.7500	0.534798	0.534797

From comparison Figure 11.3, the minimum CF_{1D}=0.47885 is collected with estimated parameters **c**=2.0521 (and original value of parameters b, c, r).

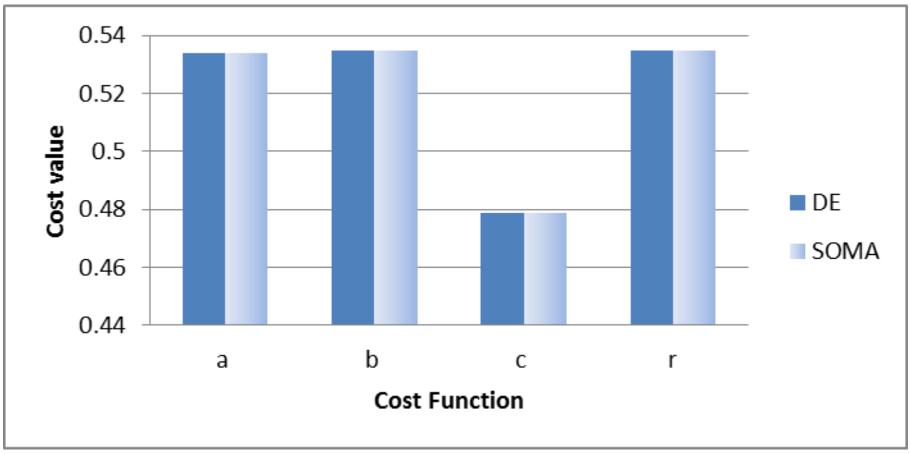


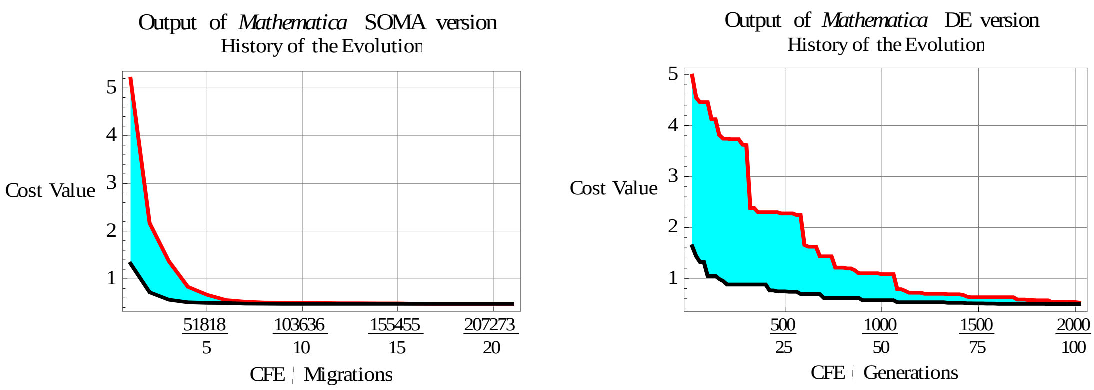
Figure 11.3. Comparison of 1D cost function

11.2. Case study 2: simulation on four-dimensional parameter

Four-dimensional parameter estimation is considered in this case. That means all of parameters a, b, c and r of response system were unknown and needed to be estimated, the parameters a, b, c and r were known with original value in driver system. The initial guesses are in the range for a∈[5,15], b∈[0,5], c∈[0,5] and r∈[20,30]. Because of the sensitive of chaotic system, the cost function CF is so complex and has a lot of local optimum. But after 5 migrations, SOMA has found the best results of CF=0.476868, the best values of the cost function approach minimum value quickly. Both the worst and the best values of cost function approach minimum gradually after 8 migrations as shown in Figure 11.4.a. SOMA had found the optimum value of a, b, c and r as shown in history evolution Figure 11.5.a. Similarly, DE has found the minimum values of the cost function with estimated parameters after 80 generations, both the worst and the best values of cost function approach minimum gradually after 100 generations as shown in Figure 11.4.b. Table 14 showed that the estimated parameters, which were obtained by SOMA and DE, have the similar value.

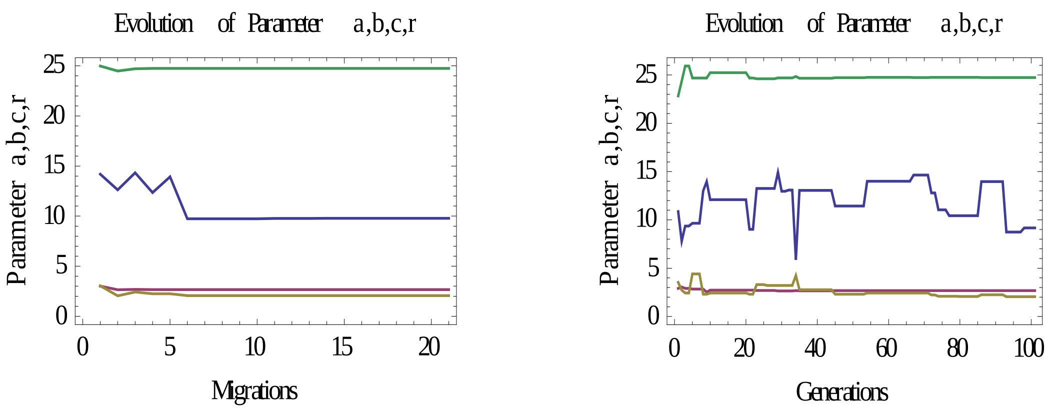
Table 14. 4D Estimated parameters of 5D system by SOMA and DE

	a	b	c	r	Cost function
SOMA	9.7775	2.66667	2.05443	24.7500	0. 476868
DE	9.7292	2.66668	2.05480	24.7500	0.477032



(a) (b)

Figure 11.4. CF_{abcr} evolution by SOMA and DE



(a) (b)

Figure 11.5. Evolution history of a,b,c,r

11.3. Case study 3: simulation on 2&3-dimensional parameter

In case 1 or 2 parameters among of a, b, c and r in response system were known in advance with the original value; the others (3 or 2) were also found with the optimum value by SOMA and DE as shown in Table 15 and Table 16. Both the worst and the best values of cost function CF_{ab}, CF_{abc} quickly approach minimum after 8 migrations as shown in Figure 11.6 in case SOMA was used, and after 70 generations with DE. From comparison Figure 11.8, the minimum CF_{2D} is collected with estimated parameters a, c (and original value of parameters b, r). The minimum of 3D cost function also recognized easily from Figure 11.9 with estimated of parameters a, c, r.

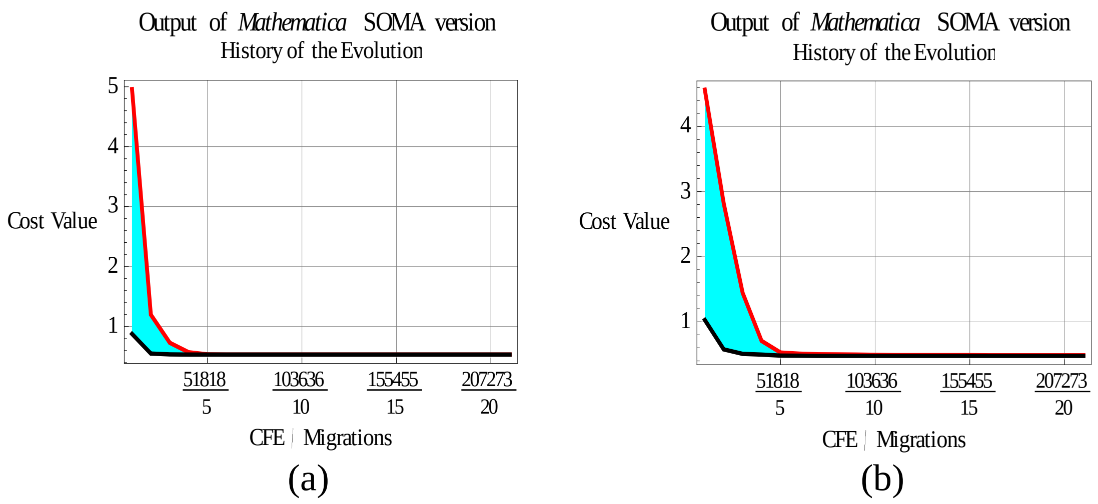


Figure 11.6. (a) CF_{ab} and (b) CF_{abc} evolution by SOMA

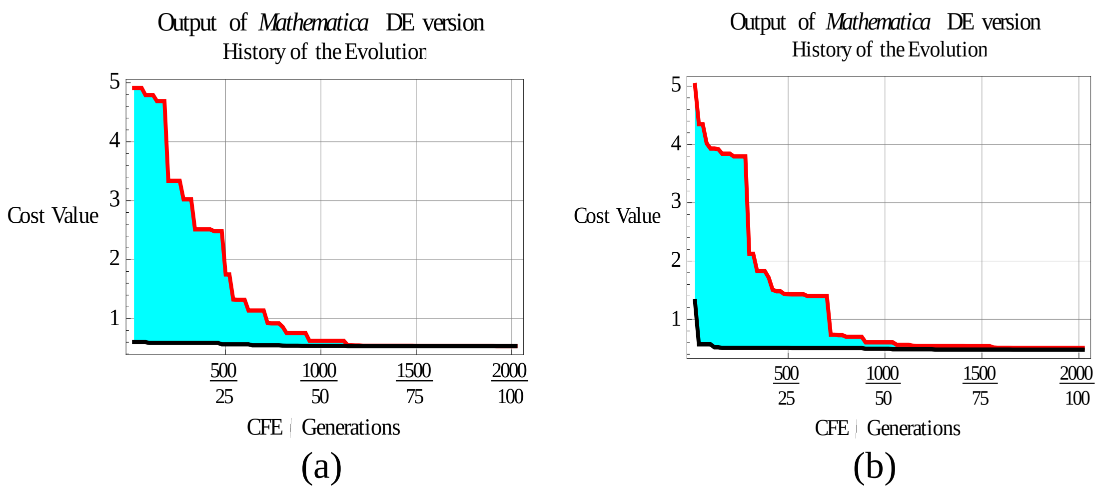


Figure 11.7. (a) CF_{ab} and (b) CF_{abc} evolution by DE

Table 15. 2D Estimated parameters of 5D system by SOMA and DE

	Estimated parameters			Cost function
SOMA	a,b	9.58676	2.66667	0.533740
	a,c	9.77759	2.05443	0.476897
	a,r	9.58691	24.7500	0.533740
	b,c	2.66667	2.05214	0.478853
	b,r	2.66667	24.7500	0.534797
	c,r	2.05215	24.7500	0.478853
DE	a,b	9.59080	2.66667	0.533750
	a,c	9.67232	2.05484	0.477077
	a,r	9.59037	24.7500	0.533748
	b,c	2.66666	2.05197	0.478994
	b,r	2.66664	24.7506	0.535338
	c,r	2.05217	24.7501	0.478930

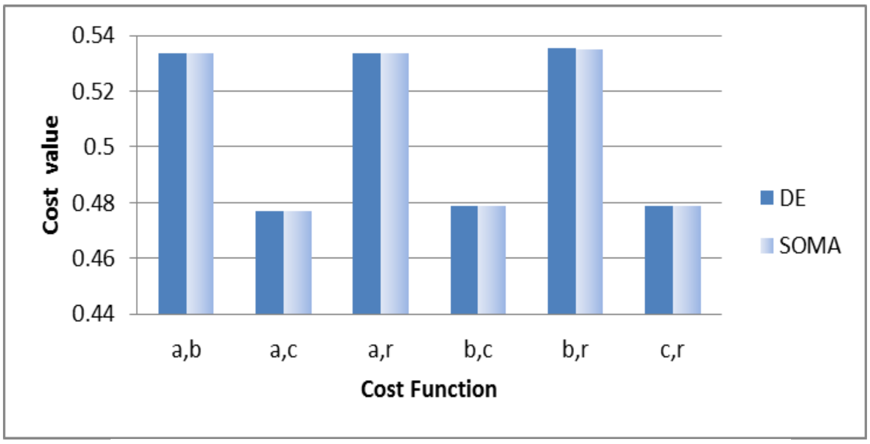


Figure 11.8. Comparison of 2D cost function

Table 16. 3D Estimated parameters of 5D system by SOMA and DE

	Estimated parameters				Cost function
SOMA	a,b,c	9.77758	2.66667	2.05443	0.476897
	a,b,r	9.58682	2.66667	24.7500	0.533740
	a,c,r	9.77761	2.05443	24.7500	0.476897
	b,c,r	2.66667	2.05214	24.7500	0.478853
DE	a,b,c	9.79553	2.66658	2.05743	0.479627
	a,b,r	9.58000	2.66667	24.7500	0.533755
	a,c,r	9.57451	2.05659	24.7499	0.477361
	b,c,r	2.66669	2.05119	24.7499	0.479565

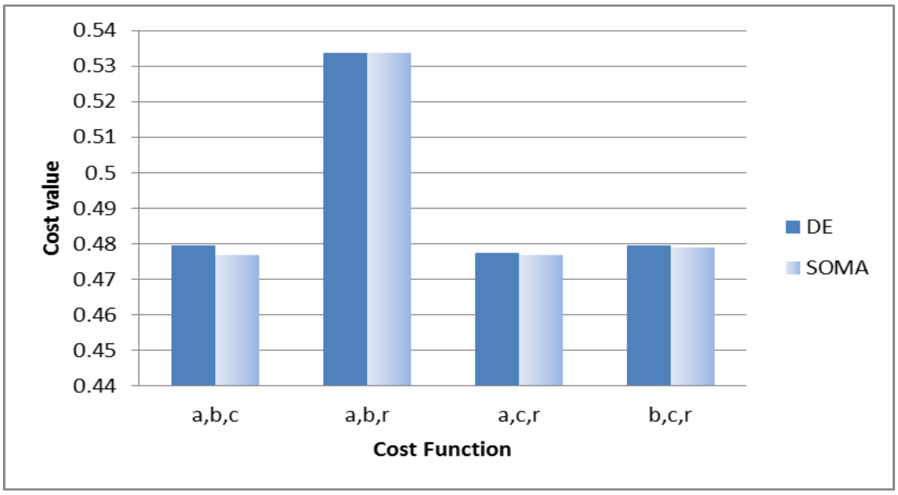


Figure 11.9. Comparison of 3D cost function

As shown in Table 13-Table 16, the estimated parameters always have the similar values with original values. However, we can also easily recognize the effect of parameter ‘c’ on parameter 'a' and on system. The estimated parameter ‘a’ always tends to achieve a=9.586xx with c=2 (such as in case study CF_{a}, CF_{ab}, CF_{ar}, CF_{abr}). While cost-functions CF always approach to area CF=0.47xxx with a=9.777xx when both 'a' and 'c' were estimated by SOMA (such as CF_{ac}, CF_{abc}, CF_{abcr}). It also has the similar effect when DE was used.

Using the best results from case study 1, 2 and 3, the comparison of CF_{1D}, CF_{2D}, CF_{3D}, CF_{4D} was displayed in Figure 11.10.

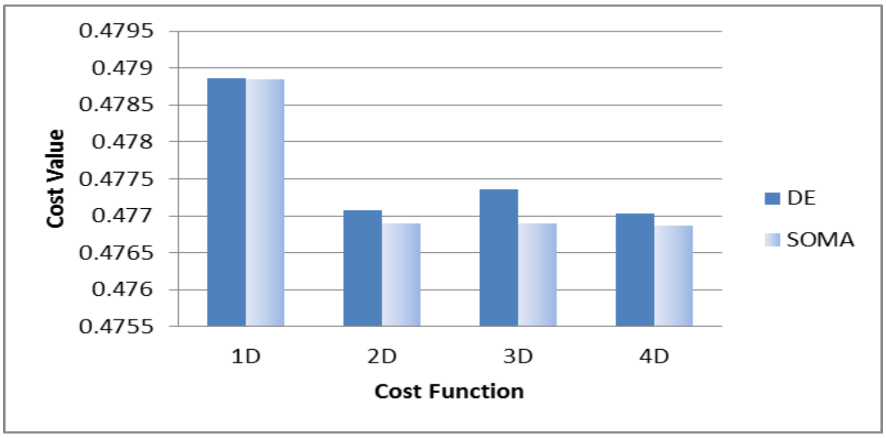


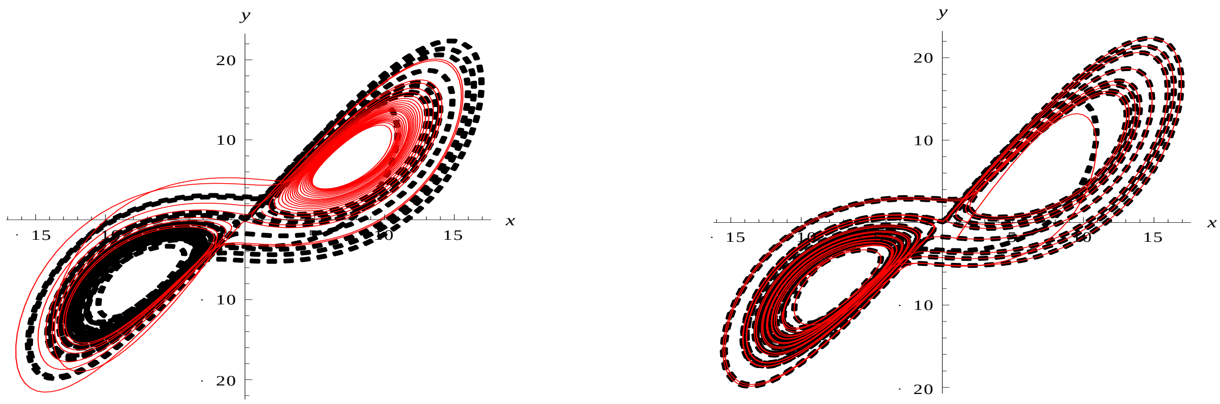
Figure 11.10. Comparison of 1-4D cost function

The results in each case are similar together, the smallest value of CF was recognized at CF_{4D}=0. 476868 with SOMA and CF_{4D}=0.477032 with DE. The cost-function CF_{SOMA}=0. 476868 is smaller than CF_{DE}=0.477032. So that, the final estimated values were chosen: a=9.7775, b=2.66667, c=2.05443 and r=24.75 to ensure that the synchronization error approaches to minimum. Thus, the actual parameters were identified. The values of cost function always approach to optimum values, the estimated parameters obtained by EA and original parameters have the similar values. The difference between DE and SOMA are not significant. So, it demonstrated that SOMA and DE are effective to estimate parameters for 5D-chaos synchronization system.

11.4. Synchronization of 5D chaotic system with estimated parameters

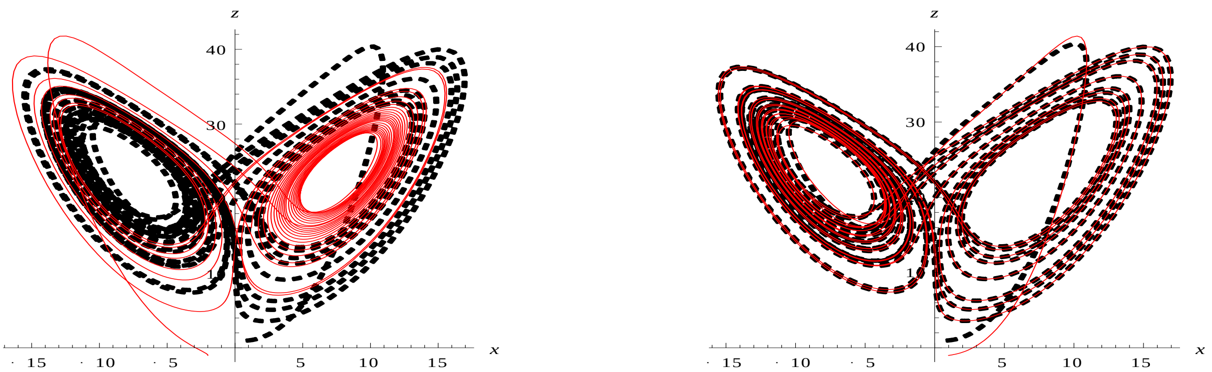
Based on the values estimated by EA, the response system was constructed. The effective of the estimated value on the synchronization errors of driver systems U_d and on response system U_r via PC method were demonstrated as shown in Figure 11.11- Figure 11.13.

As shown in Figure 11.11.a - Figure 11.13.a, the synchronization between driver system (dash black line) and response system (thin red line) do not exist in the phase space of chaotic attractor. In the opposite, when PC was applied with the estimated parameters, Figure 11.11.b - Figure 11.13.b display that the phase space of chaotic attractor between driver system and response system synchronized together.



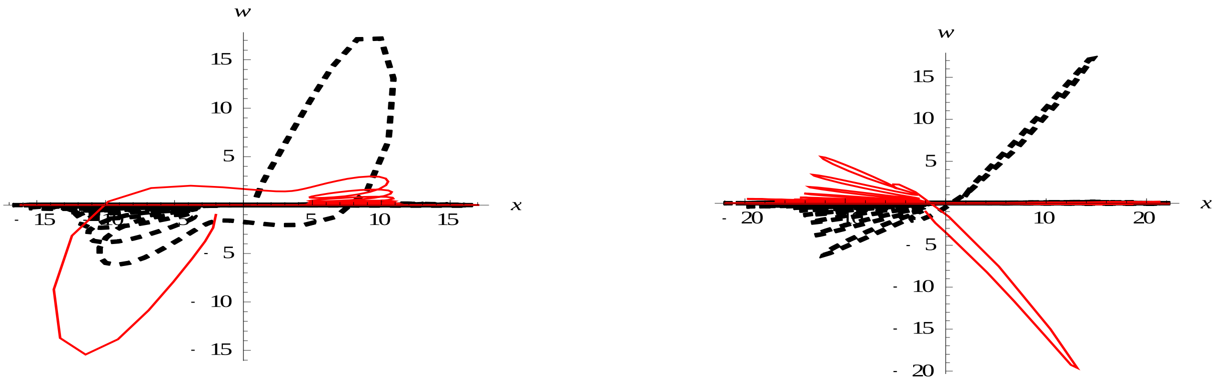
(a) Non-synchronization (b) Synchronization

Figure 11.11. Projection onto the x-y plane of the 5D Lorenz attractor.



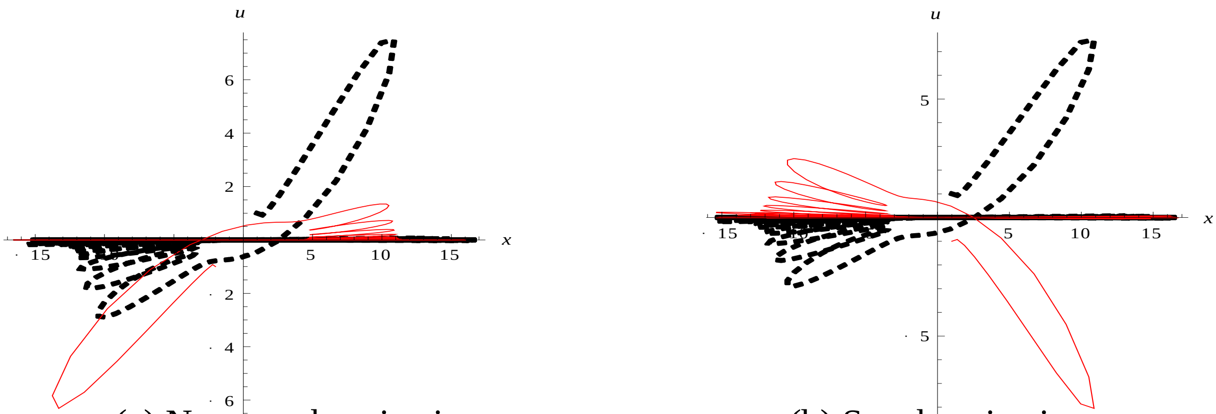
(a) Non-synchronization (b) Synchronization

Figure 11.12. Projection onto the x-z plane of the 5D Lorenz attractor.



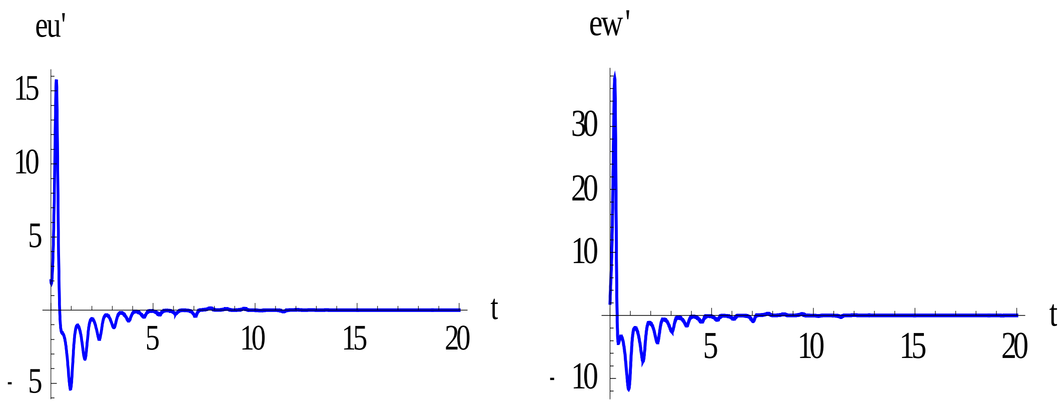
(a) Non-synchronization (b) Synchronization

Figure 11.13. Projection onto the x-w plane of the 5D Lorenz attractor.



(a) Non-synchronization (b) Synchronization

Figure 11.14. Projection onto the x-u plane of the 5D Lorenz attractor.

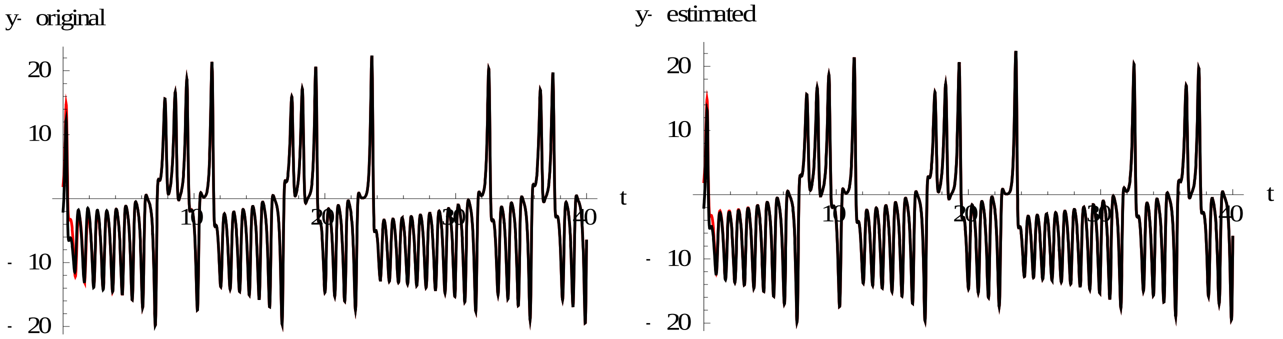


(a) $e_u=u_d-u_r$ (b) $e_u=w_d-w_r$

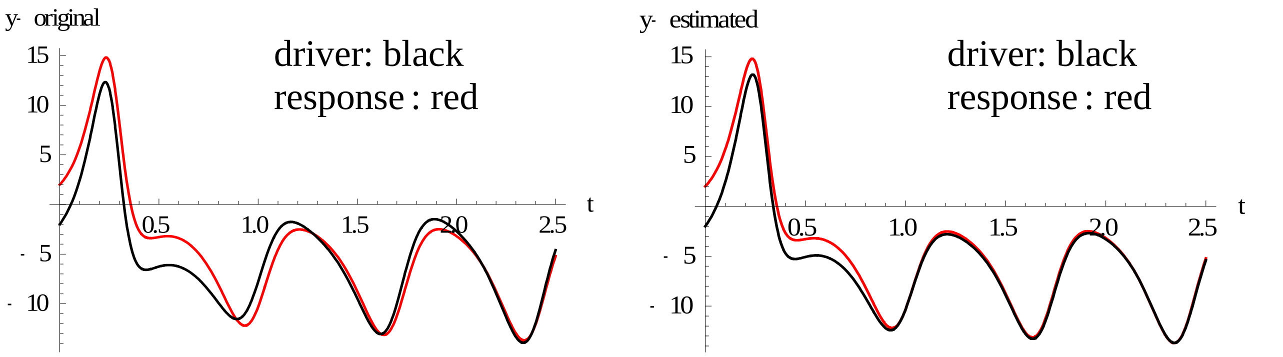
Figure 11.15. Synchronization error of variable ‘u’ and ‘w’

It seems that there are not synchronization between driver system and response system of variable ‘u’ and ‘w’ in Figure 11.13.b and Figure 11.14.b. But Figure 11.15 showed that the synchronization error of e_u & e_w approach to 0 after t>10. That means the synchronization was achieved when both variables ‘u’ and ‘w’ approached 0 with t>10. This is a characteristic of these 5D chaotic systems as shown in Figure 5.8. Therefore, it is demonstrated that the estimated values and PC method are effective to synchronize for two 5D-chaotic systems.

It is difficult to recognize what difference between Figure 11.16.a and Figure 11.16.b, but in its detail as shown in Figure 11.16.c and Figure 11.16.d, the quality of synchronization with estimated parameters is clearly higher than that of original parameters from t >0.9. That means the quality of communication system is increased with the estimated parameters.



a) Synchronization with original values b) Synchronization with estimated values



c)… and its detail d)…. and its detail

Figure 11.16. Comparison of the synchronization between original and estimated values

12. Six Dimensional Example: Synchronization of 6D Lorenz Chaotic System

The synchronization between two identical 6D chaotic systems is studied via PC method. Using x_1 of the decomposed subsystems as the driving signal in drive system X. In this case, x_1 is injected into the response system Y. Since $x_1=y_1$, we only consider the following drive and response subsystems:

$$X=\begin{cases}\dot{x}_2 = rx_1 - x_2 - x_1x_3 + x_3x_4 - 2x_4x_6 \\ \dot{x}_3 = x_1x_2 - bx_3 - x_1x_5 - x_2x_4 \\ \dot{x}_4 = -cax_4 + (a/c)x_5 \\ \dot{x}_5 = x_1x_3 - 2x_1x_6 + rx_4 - cx_5 \\ \dot{x}_6 = 2x_1x_5 + 2x_2x_4 - 4bx_6\end{cases} \tag{33}$$

And the response system Y is described by the following equations:

$$Y=\begin{cases}\dot{y}_2 = ry_1 - y_2 - y_1y_3 + y_3y_4 - 2y_4y_6 \\ \dot{y}_3 = y_1y_2 - by_3 - y_1y_5 - y_2y_4 \\ \dot{y}_4 = -cay_4 + (a/c)y_5 \\ \dot{y}_5 = y_1y_3 - 2y_1y_6 + ry_4 - cy_5 \\ \dot{y}_6 = 2y_1y_5 + 2y_2y_4 - 4by_6\end{cases} \tag{34}$$

where a, b, c and r are unknown parameters in response system.

Consider the difference of these two systems, the synchronization of the pair of identical systems (33) and (34) occurs if the dynamical system describes the evolution of the difference $\|X-Y\| \to 0$ as $t \to \infty$. Subtracting system (34) from system (33) yields the error dynamical system between two system e(t)=X(t)-Y(t) which were used to create a cost function CF representing the root mean square error (RMSE) of synchronization between X and Y:

$$\text{CF}=\sqrt{\frac{1}{m}\sum_{t=1}^{m}\left|(x_2,x_3,x_4,x_5,x_6)_{(t)}-(y_2,y_3,y_4,y_5,y_6)_{(t)}\right|^2} \tag{35}$$

The parameter estimation can be formulated as a multidimensional nonlinear problem to minimize the cost function CF. When estimating the parameters, suppose the structure of the system is known in advance, the transmitter (driver) system is set with original parameters and the parameter in receiver (response) system is unknown. EA is used to find a suitable parameter a, b, c and r such that the cost function CF can be asymptotical approach to minimum point.

The initial states of the drive system and the response system are taken as $x_1(0)=1$, $x_2(0)=1$, $x_3(0)=1$, $x_4(0)=1$, $x_5(0)=1$, $x_6(0)=1$ and $y_2(0)=0$, $y_3(0)=0$, $y_4(0)=0$, $y_5(0)=0$, $y_6(0)=0$, respectively. Hence the error system has the initial values $e_2(0)=1$, $e_3(0)=1$, $e_4(0)=1$, $e_5(0)=1$ and $e_6(0)=1$. DE and SOMA were used to solve the problem, which the control parameters setting are given in Table 1, Table 2 and Generations=200 in this case for DE. Simulations were implemented using Mathematica programming language and executed on HP 8200 core i3-2120 3.3Ghz, 12GB personal computer.

12.1. Experimental results

As mentioned above, the parameters a, b, c and r are known in advance with original value in driver system. In response system, they are unknown and need to be estimated. The initial guesses are in the range for $a\in[5,15]$, $b\in[0,5]$, $c\in[0,5]$ and $r\in[35,45]$. Because of the sensitive of chaotic system, the cost function CF is so complex and has a lot of local optimum. But DE has found the best results of CF as shown in Figure 12.1.a, it showed the best values of the cost function gradually approached minimum value (CF=0.225836) after 55 generations. There are huge differences between the worst and the best in first 5 generations as can be seen in Figure 12.1.c. But it quickly approached the best value after 10 generations; both the best and the worst approached the optimum value after 90 generations as shown in Figure 12.1.b.

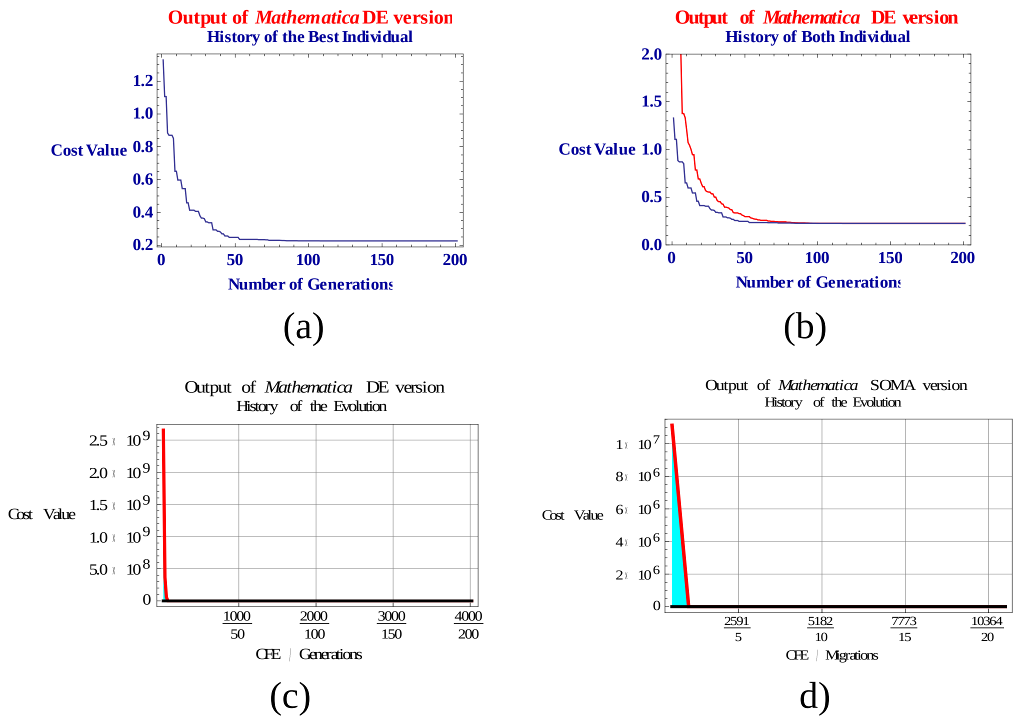


Figure 12.1. CF_{abcr} evolution by DE and SOMA

Similarly for SOMA, there is also having the significant difference between the worst and the best values of the cost function at first migration as shown in Figure 12.1.d. The worst value immediately dropped to minimum zone from $1*10^7$ after 2 migrations, and rapidly approached the best and the optimum value.

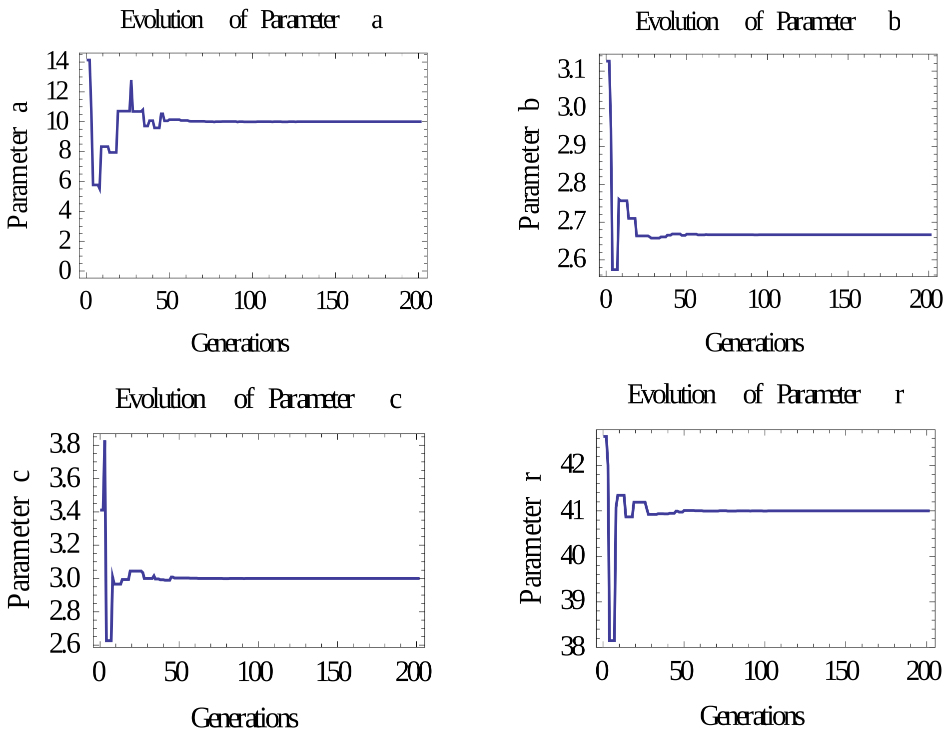


Figure 12.2. Evolution history of parameters by DE

Figure 12.2 displayed the evolution history of estimated parameters by DE. As can be seen in the history evolution of parameter 'a' in Figure 12.2.a, there was the instability in the early stages, but after 50 generations, it reached the stability with a value of 10. Similar to others, parameters b, c, r also achieved the optimum values after 50 generations as shown in Figure 12.2. For SOMA, the history evolution of parameter 'a' was also uncertainty in the first 15 migrations and it reached the stability after that. Therefore, it can be stated that DE and SOMA were successful in finding the unknown parameters of response chaotic system.

As shown in Table 17 and Figure 12.4, the estimated parameters were executed by 5 strategy rules of DE: DERand1Bin, DERand2Bin, DERBest2Bin, DELocalToBest, DERand1DIter and 4 strategy rules of SOMA: SOMA ATO, SOMAATR, SOMAATA, SOMAATAA, and they got the similar values together.

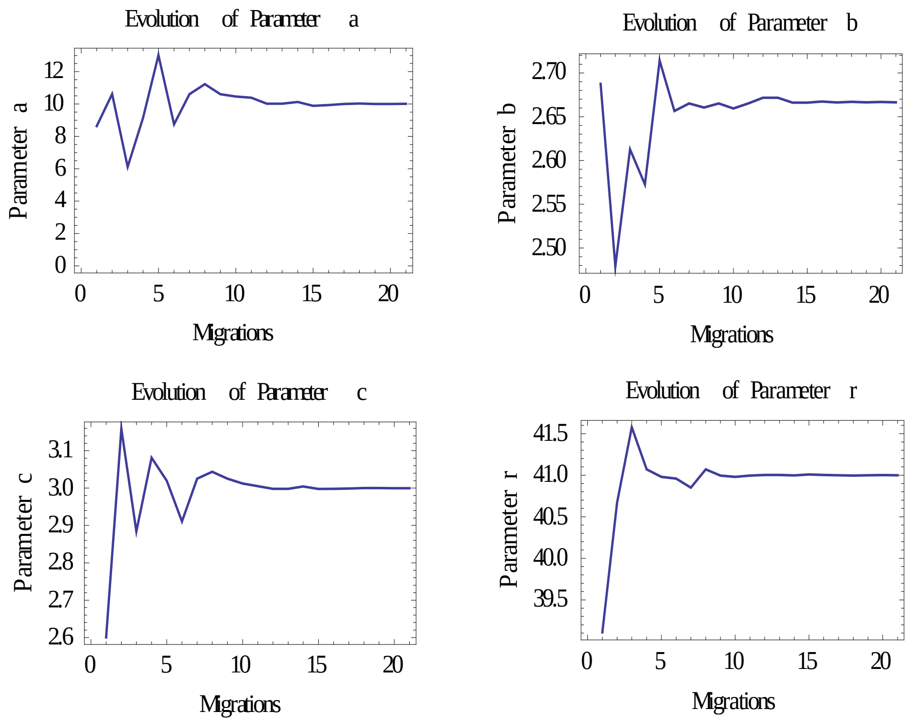


Figure 12.3. Evolution history of parameters by SOMA

The values of cost function always approach to optimum values. There were not significant differences among the results from 9 versions as shown in Figure 12.4 and Figure 12.5. The smallest value of CF is 0.225836 as can be seen in Figure 12.5. So that, the final estimated values were chosen: a=10.0000, b=2.66667, c=3 and r=41 to ensure that the synchronization error approaches to minimum. Thus, the parameters of response system were identified.

Table 17. Estimated parameters of 6D system by DE and SOMA

	a	b	c	r	Cost function
DERand1Bin	10.0000	2.66667	3	41	0.225836
DERand2Bin	10.0000	2.66667	3	40.9999	0.225890
DEBest2Bin	10.0000	2.66667	3	41	0.225836
DELocalToBest	10.0000	2.66667	3	41	0.225836
DERand1DIter	9.98794	2.66668	2.99974	41.0014	0.227494
SOMAATO	9.99649	2.66665	2.99996	40.9996	0.226222
SOMAATR	9.96808	2.66647	2.99933	40.9972	0.228797
SOMAATA	10.0000	2.66667	3	41	0.225836
SOMAATAA	10.0000	2.66667	3	41	0.225836

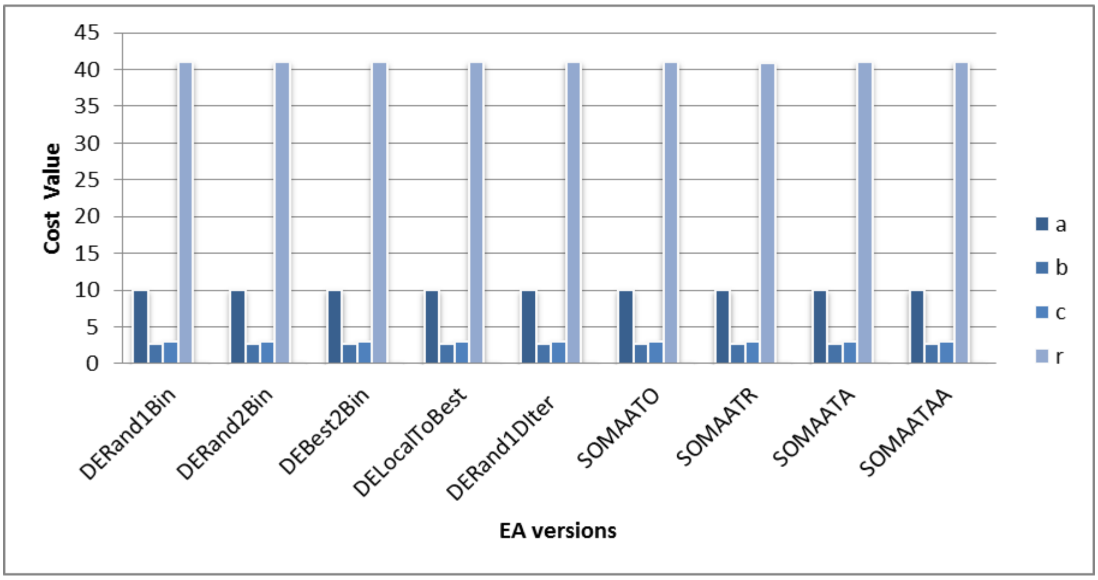


Figure 12.4. Comparison of the estimated parameters by SOMA and DE

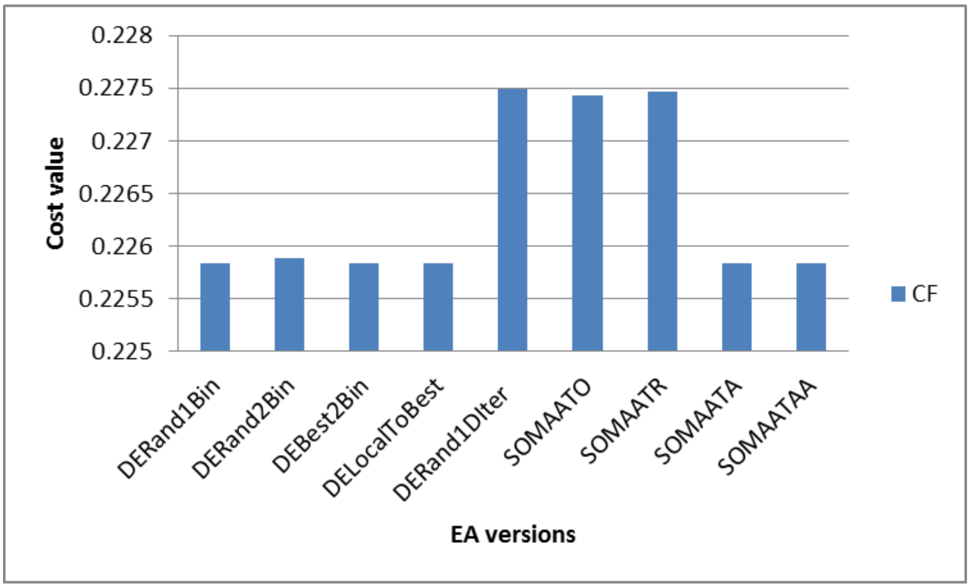


Figure 12.5. Comparison of cost function by EA versions

12.2. Synchronization of 6D chaotic systems with estimated parameters

The response system was constructed by the estimated parameters. The effective of the estimated value on the synchronization errors of driver systems X and on response system Y via PC method were demonstrated as shown in Figure 12.6. It can easily point out that the synchronization between variable x and y did not exist in the left side. But in opposite side, when PC was applied with the estimated parameters, the synchronization was achieved between two systems although they were started under different initial values. Therefore, it demonstrated that the estimated values are effective to synchronize for two 6D chaotic systems. The estimated parameters and the original parameters are the same; it indicated that the original parameters are optimal choice in this case.

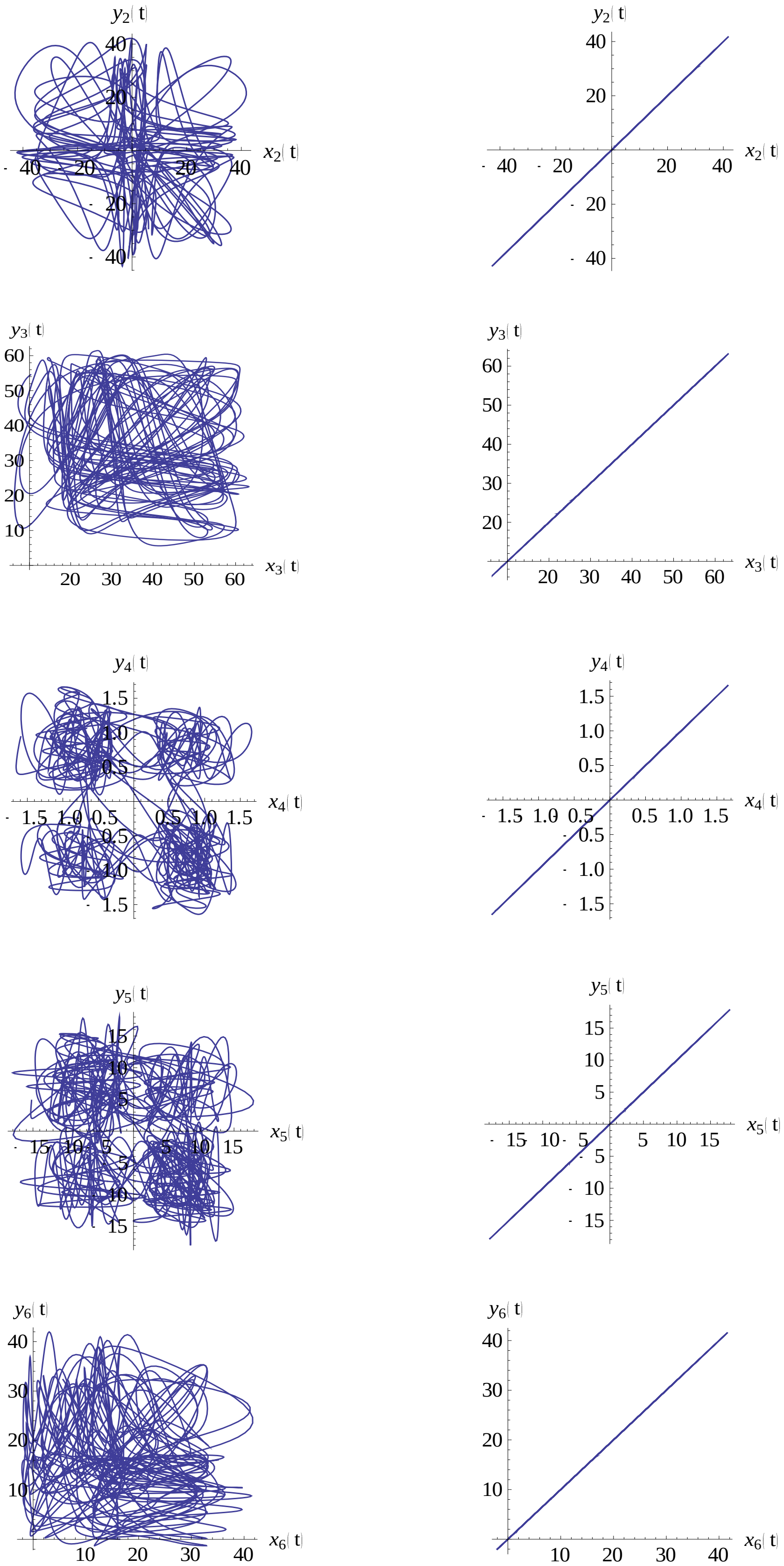


Figure 12.6. Non-synchronization and synchronization between two systems

13. Synchronization of Two Different Chaotic Systems

13.1. Problem formula

Synchronization of non-identical chaotic systems is studied in this chapter; EA is used to find the optimum parameters of control function, which were proposal to achieve the synchronization between Rössler and Lü systems. Using the Rössler system drives Lü system, in this case, the drive and response system is presented as follows

$$D=\begin{cases}\dot{x}_1=-y_1-z_1,\\ \dot{y}_1=x_1+a_1y_1,\\ \dot{z}_1=z_1(x_1-c_1)+b_1\end{cases} \tag{36}$$

And the response Lü system

$$R=\begin{cases}\dot{x}_2=a_2(y_2-x_2) \quad +u_1(t)\\ \dot{y}_2=-x_2z_2+c_2y_2 \quad +u_2(t)\\ \dot{z}_2=x_2y_2-b_2z_2 \quad +u_3(t)\end{cases} \tag{37}$$

Three functions $u_1(t)$, $u_2(t)$, $u_3(t)$ are control functions, which will be designed to synchronize two systems. So that, the error dynamical system between two system can be expressed by

$$E=\begin{cases}\dot{e}_1=-a_2e_1+a_2e_2+a_2(y_1-x_1)+y_1+z_1 \quad +u_1(t),\\ \dot{e}_2=c_2e_2-x_2z_2+(c_2-a_1)y_1-x_1 \quad +u_2(t),\\ \dot{e}_3=-b_2e_3-b_1-z_1(x_1-c_1-b_2)+x_2y_2 \quad +u_3(t)\end{cases} \tag{38}$$

There are a lot of definitions for control functions $u_1(t)$, $u_2(t)$, $u_3(t)$, in this case, they were proposed as follows

$$U=\begin{cases}u_1(t)=k_1x_1-k_2y_1-k_3z_1\\ u_2(t)=k_4x_1+k_5y_1-k_6y_2\\ u_3(t)=z_1(x_1-k_7)-k_8x_2y_2+k_9\end{cases} \tag{39}$$

From there, the response system can be rewritten as

$$R=\begin{cases}\dot{x}_2=a_2(y_2-x_2) & +k_1x_1-k_2y_1-k_3z_1\\ \dot{y}_2=-x_2z_2+c_2y_2 & +k_4x_1+k_5y_1-k_6y_2\\ \dot{z}_2=x_2y_2-b_2z_2 & +z_1(x_1-k_7)-k_8x_2y_2+k_9\end{cases} \quad (40)$$

Different with another research, in this study, the unknown parameters $\{k_1,\ldots,k_9\}$ will be estimated by EA via minimizing the synchronization error between two systems. By this way, the control functions are identified, the synchronization will be done between Rössler and Lü systems.

Subtracting system (40) from system (36) yields the error dynamical system between two system e=D-R which were used to create a cost function CF representing the root mean square error (RMSE) of synchronization between D and R:

$$CF=\sqrt{\frac{1}{m}\sum_{t=1}^{m}|D_{(t)}-R_{(t)}|^{2}} \quad (41)$$

13.2. Parameters setting

In this simulations, the initial states of the drive system and the response system are taken as $x_1(0)=-1$, $y_1(0)=0$, $z_1(0)=1$ and $x_2(0)=1$, $y_2(0)=2$, $z_2(0)=0$, respectively. Hence the error system has the initial values $e_x(0)=-2$, $e_y(0)=-2$ and $e_z(0)=1$. The initial guesses are in the range for $k_1\in[0,50]$, $k_2\in[0,50]$, $k_3\in[0,10]$, $k_4\in[0,10]$, $k_5\in[30,100]$, $k_6\in[30,100]$, $k_7\in[0,10]$, $k_8\in[0,10]$ and $k_9\in[0,10]$. DE and SOMA were used to solve the problem, which the control parameters setting are given in Table 1, Table 2 (Generations=150 for DE in this case). Simulations were implemented using Mathematica programming language and executed on HP 8200 core i3-2120 3.3 GHz, 12GB personal computer.

Table 18. Used versions of DE and SOMA

Index	Algorithm / Version
1	DERand1Bin
2	DERand1Bin
3	DEBest2Bin
4	DELocalToBest
5	DEBest1JIter
6	DERand1DIter
7	DERand1GenerationDIter
8	SOMAATO
9	SOMAATR
10	SOMAATA
11	SOMAATAA

13.3. Simulation and results

Because of the sensitive of chaotic system, the cost function CF is so complex and has a lot of local optimum. But DE and SOMA were successful in finding the optimum values of the unknown parameters k_i in control functions u_1, u_2, u_3. As shown in Figure 13.1, there are huge differences between the worst and the best in first 5 generations. But it quickly approached the best value after 10 generations; both the best and the worst approached the optimum value of cost function.

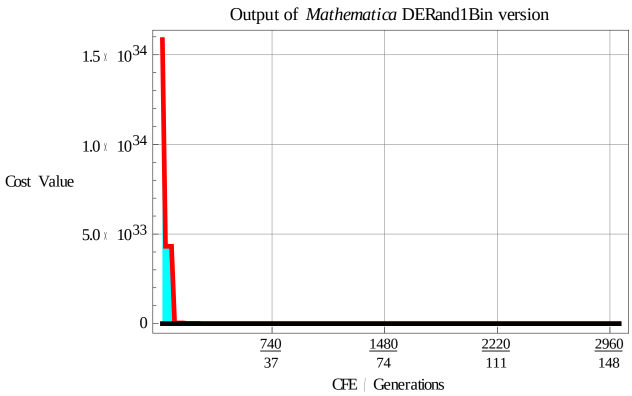


Figure 13.1. CF evolution by DE

Figure 13.2 displayed the evolution history of estimated parameters by DE. As can be seen in the history evolution of parameter 'k_1', there was the instability in the early stages, but after 110 generations, it reached the stability with value of 36.2710.

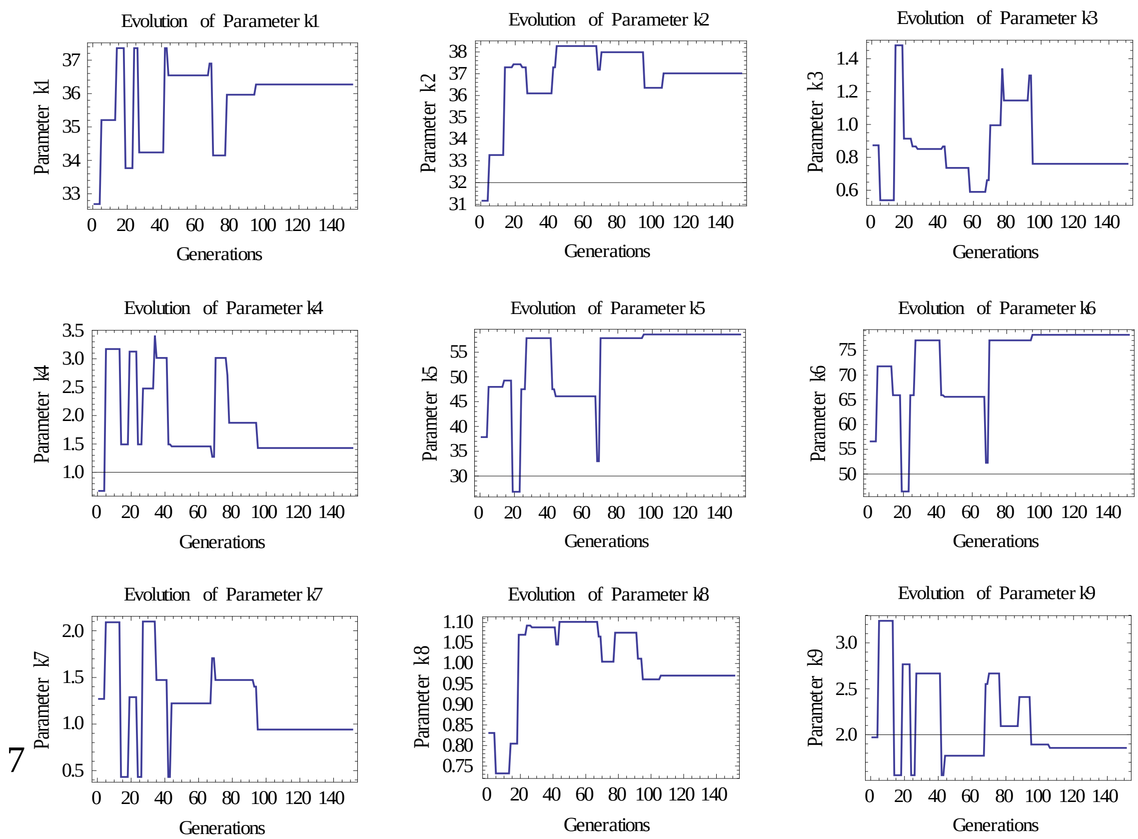


Figure 13.2. Evolution history of parameters by DERand1Bin

Similar to others, parameters $k_2, \ldots, k_9$ also achieved the optimum values after 110 generations as shown in Figure 13.2.

Similarly for SOMA, there is also the significant difference between the worst and the best values of the cost function at first migration as shown in Figure 13.3. The worst value immediately dropped to minimum zone from $3*10^{34}$ after 2 migrations, and rapidly approached the best and the optimum value.

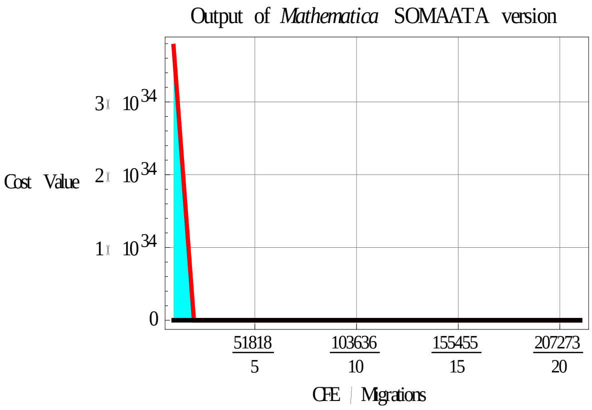


Figure 13.3. CF evolution by SOMA

The history evolution of parameters 'k_i' were also uncertainty in the first 3-6 migrations, and it reached the stability after that. Therefore, it can be stated that DE and SOMA were successful in finding the unknown parameters of response chaotic system.

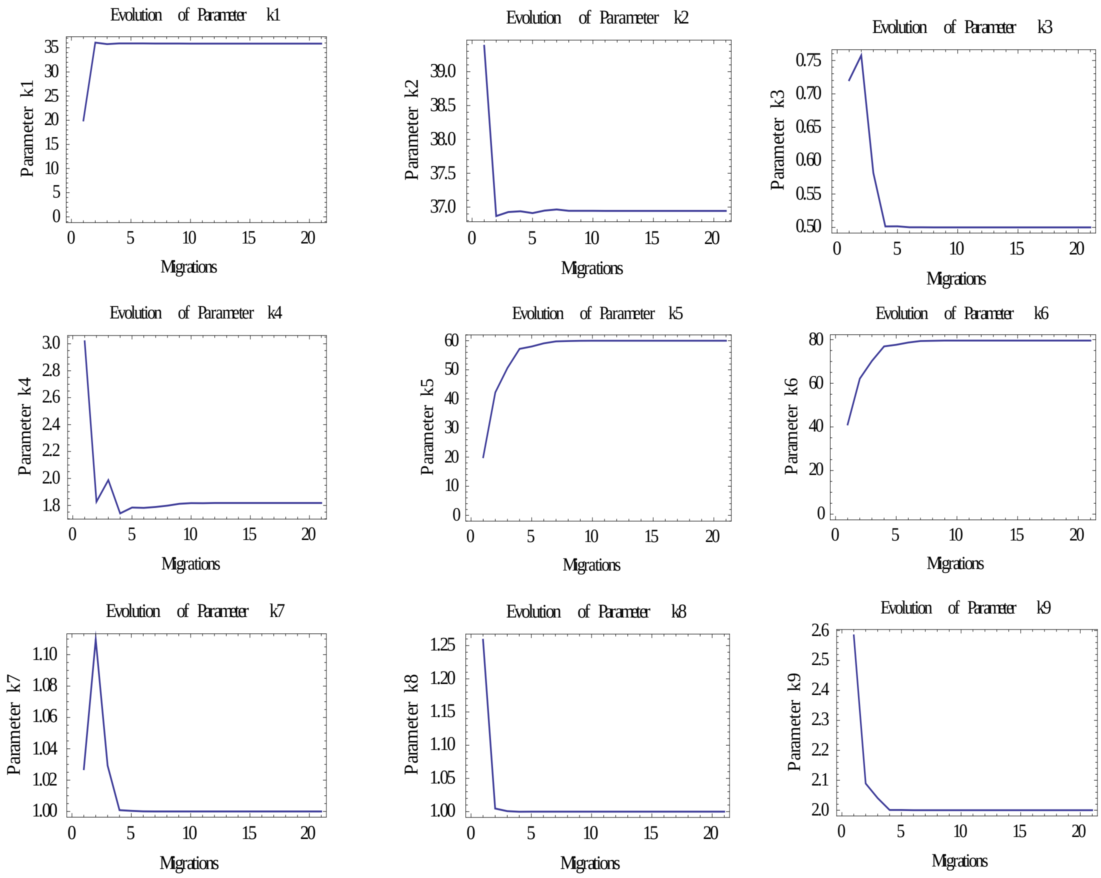


Figure 13.4. Evolution history of parameters by SOMAATA

As shown in Table 19 and Table 20, the estimated parameters always have the similar values together. From Figure 13.6 and Figure 13.7, it can be easily recognized that the parameters k_1, k_2, k_7, k_8 and k_9 are almost the same on 11 version simulations, while the difference of k_3, $k_{4,}$ k_5 and k_6 are significant. However, the value of cost functions always approached to minimum area, the cost function $CF_{SOMAATAA}$=0.320878 is smallest as shown in Figure 13.5. Therefore, the parameters estimated by SOMAATAA will be selected to ensure that the synchronization error approach to a minimum. Thus, the actual parameters were identified.

Table 19. Estimated parameters of control function and optimum CF by DE

Estimated values	DE Version						
	1	2	3	4	5	6	7
k_1	36.2710	35.5836	36.0742	35.7732	35.1467	36.8903	36.1310
k_2	37.0165	36.7626	36.8068	36.8398	36.3316	36.0588	37.1032
k_3	0.76080	0.63108	0.90326	1.36929	0.50151	1.20522	1.14046
k_4	1.42738	1.05672	1.51666	2.17205	2.82134	1.14962	1.52759
k_5	58.5680	51.0817	55.1871	59.4313	44.3674	58.2104	37.2125
k_6	78.1458	70.4942	75.3100	78.9930	64.3707	78.8263	56.7865
k_7	0.94133	0.88573	0.98272	0.92327	0.97340	1.04829	1.16730
k_8	0.97050	0.98817	0.98394	0.97234	0.97330	0.98099	1.03196
k_9	1.85698	1.89599	1.93564	2.02172	1.94910	2.14003	2.19639
CF	0.39792	0.43584	0.38481	0.39429	0.41833	0.41919	0.44581

Table 20. Estimated parameters of control function and optimum CF by SOMA

Estimated values	SOMA Version			
	8	9	10	11
k_1	36.1628	35.0725	35.3851	35.8622
k_2	36.8300	36.1058	36.9752	36.9433
k_3	0.56965	0.59059	0.50169	0.5
k_4	1.69162	2.9468	1.83717	1.81771
k_5	58.6038	47.9947	59.963	60.
k_6	78.2939	68.6717	79.5353	79.6101
k_7	0.96562	0.95246	1.00043	1
k_8	1.00015	0.99739	0.99997	1
k_9	1.98164	1.93714	2.00013	2
CF	0.33815	0.40354	0.32131	0.320878

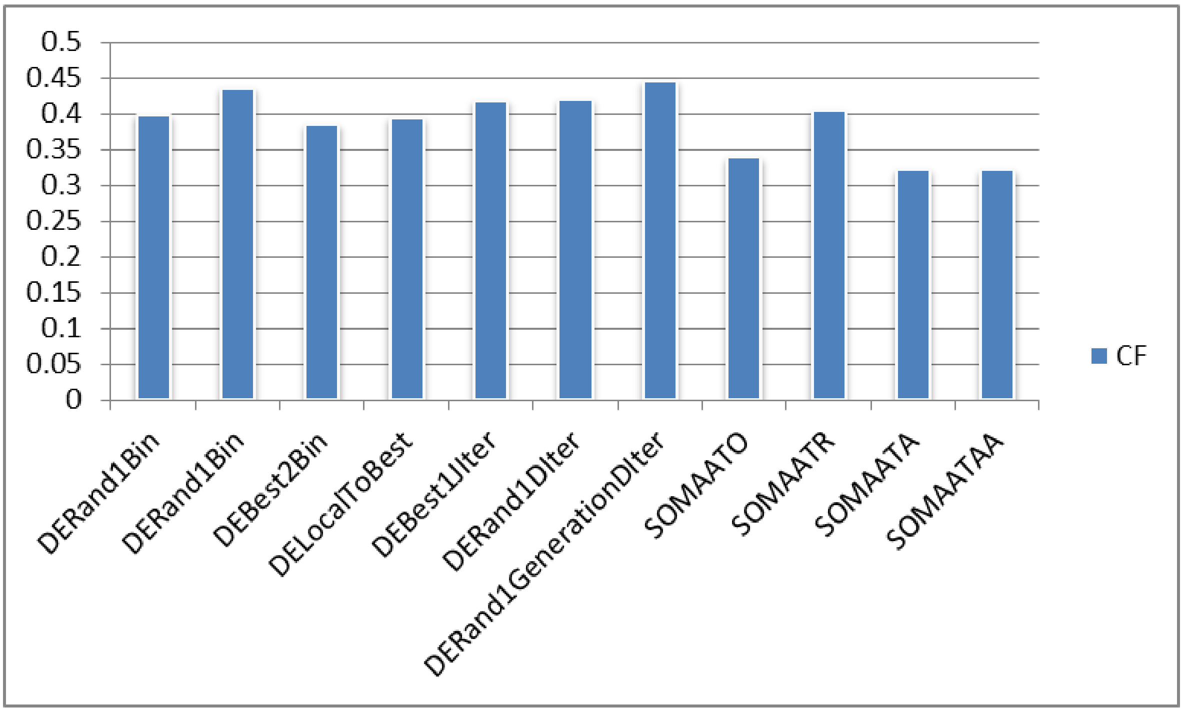


Figure 13.5. Comparison of cost function by EA versions

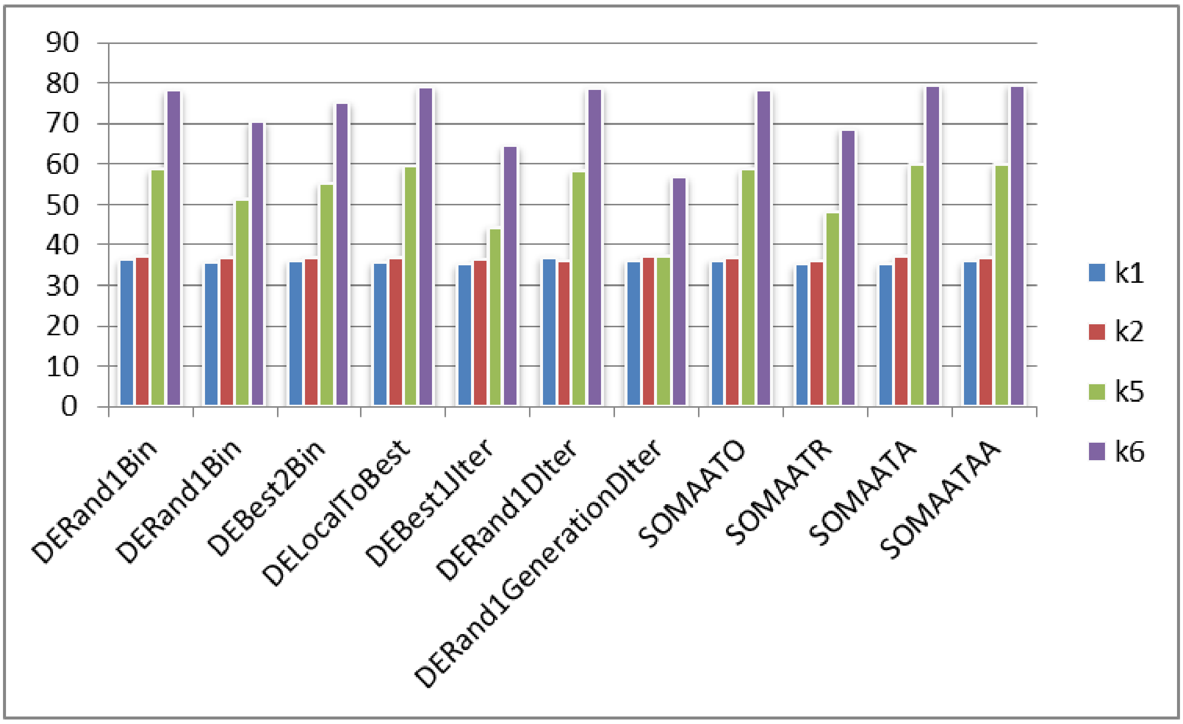


Figure 13.6. Comparison of estimated parameters k1,k2,k5,k6

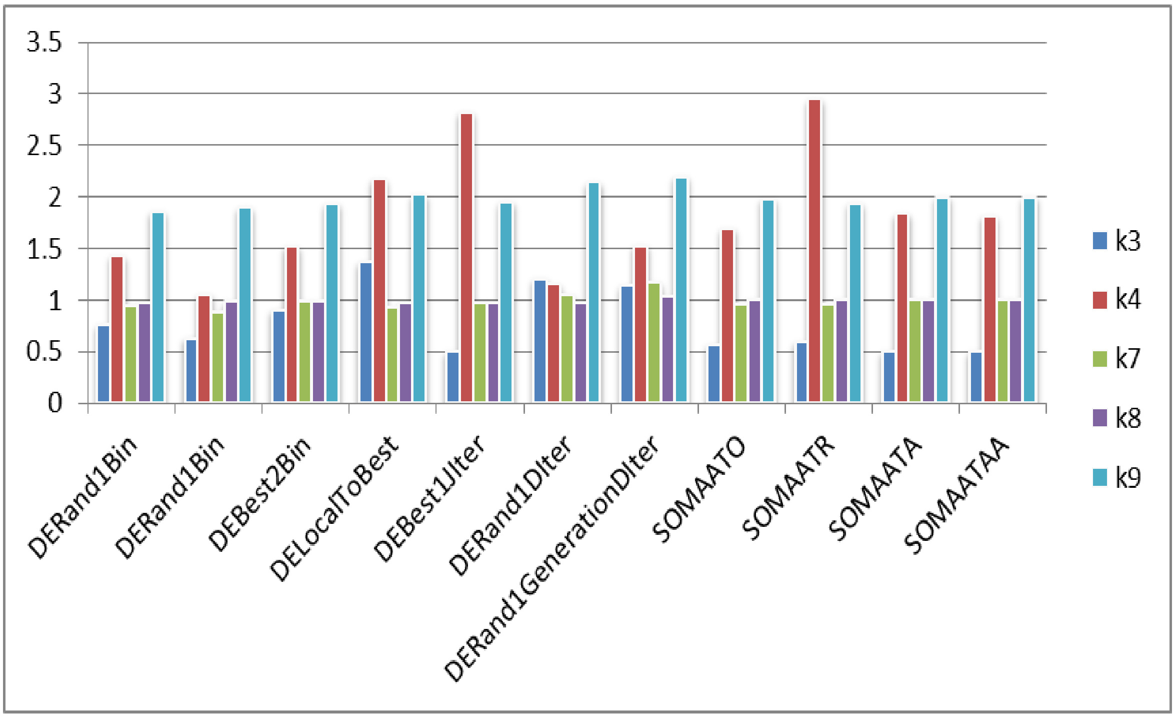


Figure 13.7. Comparison of estimated parameters k3,k4,k7,k8,k9

13.4. Synchronization with estimated parameters

Based on the estimated values, the control functions $u_1(t)$, $u_2(t)$, $u_3(t)$ were constructed. The effective of the control functions on the synchronization of driver systems Rössler and on response system Lü by control functions were demonstrated as shown in Figure 13.9. It can easily point out that the synchronization between of driver systems Rössler (thin line) and on response system Lü (dash line) did not exist in Figure 13.8.

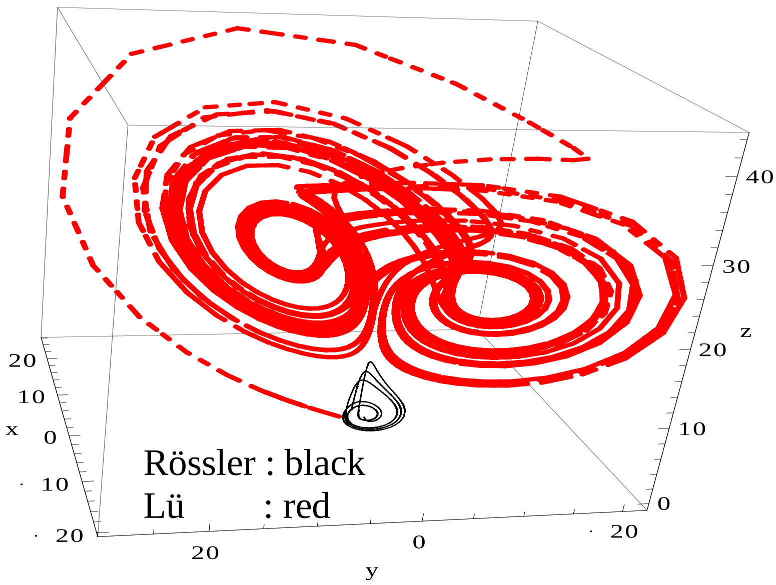


Figure 13.8. Non-synchronization of Rössler and Lü system

But when control functions were used, the synchronization was achieved between two systems although they were started under different initial values. Therefore, it demonstrated that the control functions are effective to synchronize for two different (Rössler and Lü) chaotic systems.

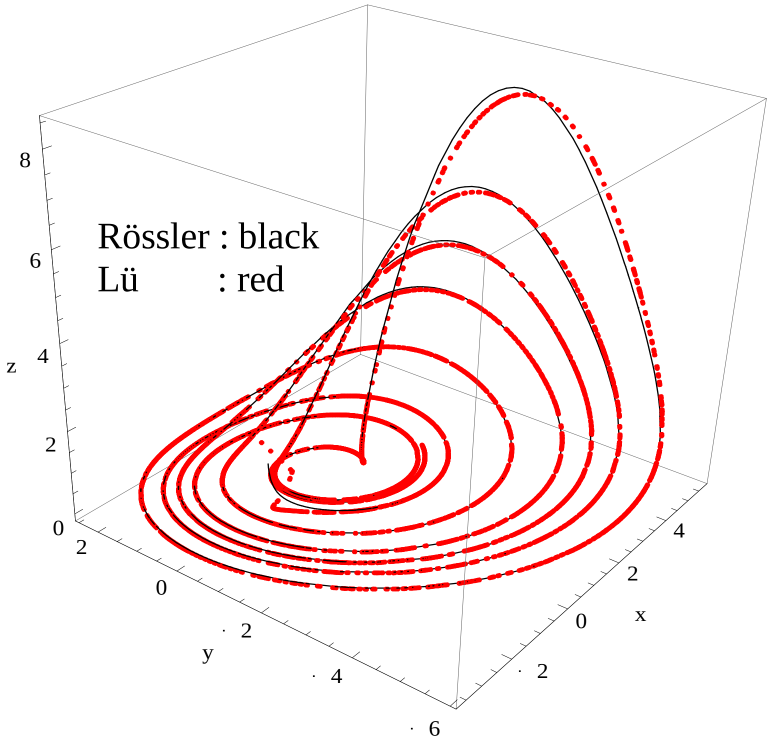


Figure 13.9. Synchronization of Rössler and Lü system

There are exist small synchronization errors between two systems. But when we compare the effect of estimated parameters k_i with other ones, which can be chosen randomly such as: k_1=36, k_2=37, k_3=1, k_4=1, k_5=20.45, k_6=40, k_7=1, k_8=1, k_9=2; the synchronization error of estimated values (black line) is smaller than that of the chosen ones (blue dash line) as shown in Figure 13.10. Further, the estimated parameters k_i were chosen from 11 version of EA, it indicated that the estimated parameters are optimal choice in this case.

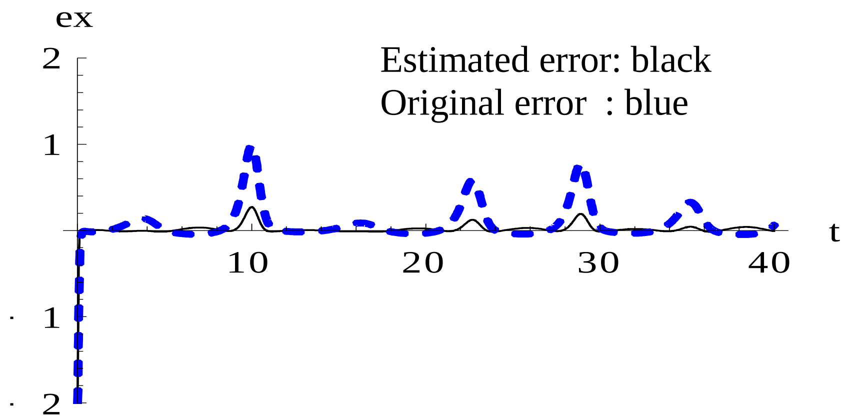


Figure 13.10. Comparison of synchronization errors

14. Application on Chaotic Secure Communication System

14.1. Application on encoding and decoding

Many chaotic encoding and decoding schemes have been investigated, which are used to encode messages on the chaotic waveform. Chaotic Masking Scheme (CMS) is one of the simplest methods in chaotic secure communication. A possible data encryption scheme is to add a small amplitude message to a larger amplitude chaotic carrier signal. The message is added into carrier signal before being sent to the receiver as the "hide" message. When a secret message is being encrypted, the encryption should be as complex as possible so that if anyone was to intercept the message, they would not be able to decrypt it.

$$\text{Transmitted signal} = \text{Message} + \text{Chaotic signal} \tag{42}$$

$$s(t) = m(t) + X(t)$$

A block diagram of a chaotic masking system is shown in Figure 3.3 where the information signal is recovered by subtracting the synchronized chaotic signal from the received waveform.

$$\text{Recovered message} = \text{Transmitted signal} - \text{Synchronization signal} \tag{43}$$

$$m'(t) = s(t) - Y(t)$$

$$= m(t) + X(t) - Y(t)$$

However, the message is corrupted by the synchronization errors e(t)=X(t)-Y(t) caused by the dissymmetry between the transmitter and the receiver in the presence of the encoded message. The performance of chaotic communications is directly concerned to the quality of synchronization. Because these synchronization errors are significant, the receiver cannot be perfectly synchronized to the transmitter in this system, the communication performance of the CMS is low.

To demonstrate the chaotic secure communication process, a signal is composed of two parts: a chaotic carrier signal and a message, Qi system is used for both the encoder and decoder. The active passive decomposition technique is applied to achieve the synchronization between two identical Qi systems. Figure14.1 shows the message $m(t)= 0.1\text{Sin}(10t+2\text{Cos}(3t))$, carrier chaotic signal x(t), encryption signal s(t), and Figure 14.2 shows the power spectrum of encryption signal through the CMS scheme.

Qi encoder:

$$X=\begin{cases}\dot{x}_1 = a(x_2 - x_1) + x_2x_3x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1x_3x_4 \\ \dot{x}_3 = -cx_3 + x_1x_2x_4 \\ \dot{x}_4 = -dx_4 + x_1x_2x_3 \\ s(t) = x_1(t) + m(t)\end{cases} \tag{44}$$

Qi decoder:

$$Y=\begin{cases}\dot{y}_1 = a(y_2 - y_1) + y_2y_3y_4 \\ \dot{y}_2 = b(y_1 + y_2) - y_1y_3y_4 \\ \dot{y}_3 = -cy_3 + y_1y_2y_4 \\ \dot{y}_4 = -dy_4 + y_1y_2y_3 \\ \mathrm{m}'(t) = s(t) - y_1(t)\end{cases} \tag{45}$$

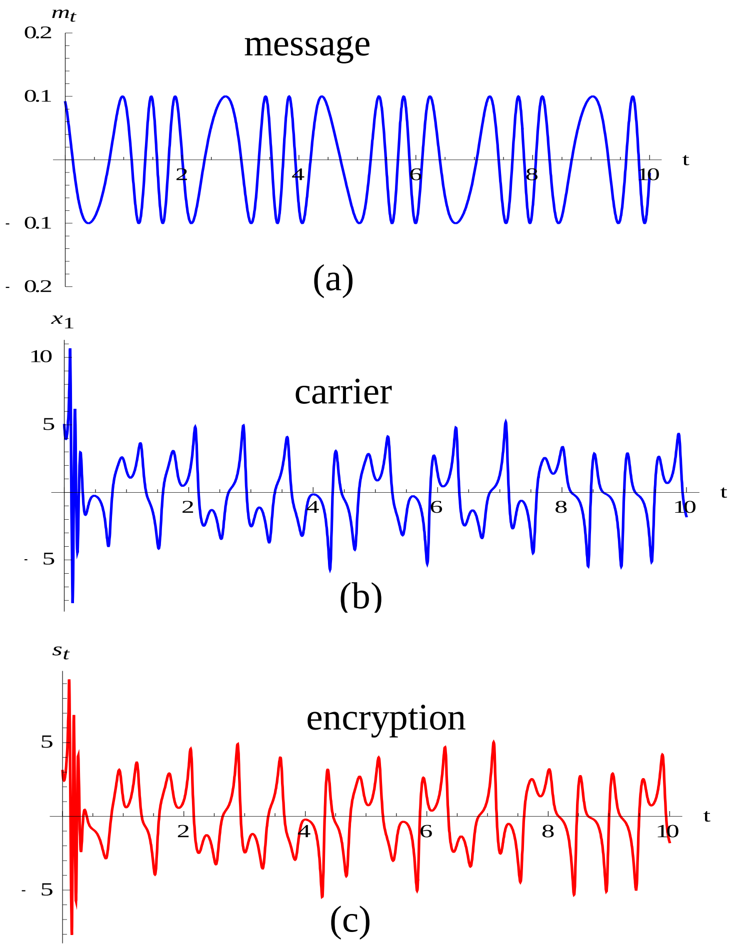


Figure14.1. The carrier (b) and the message (a) are added together to give the encryption signal (c)

In this scheme, the message is added on the chaotic signal after the waveform leaves the feedback loop, as can be seen from the setup in block diagram (Figure 3.3). The message is not injected into the dynamics that generates the chaotic waveform of the transmitter. The complexity of the chaotic waveform is not increased in the case of CMS. Therefore, the synchronization error between two identical Qi systems is also the synchronization error of CMS.

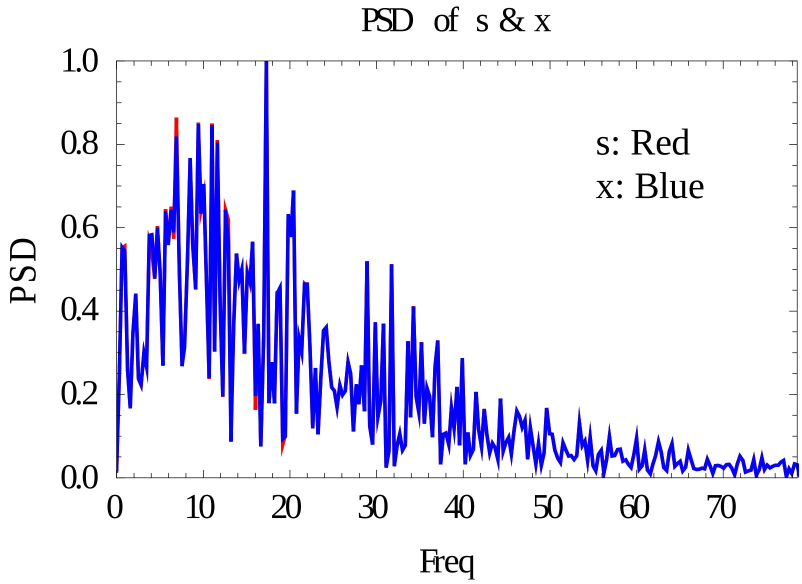


Figure 14.2. The power spectrum of carrier and encryption signal

14.2. Synchronization of 4D Qi chaos system with estimated parameters

By using values estimated by EA, the response system was constructed. The effective of the estimated value on the synchronization errors of driver systems X and response system Y via APD method were demonstrated as shown in Figure 14.5.

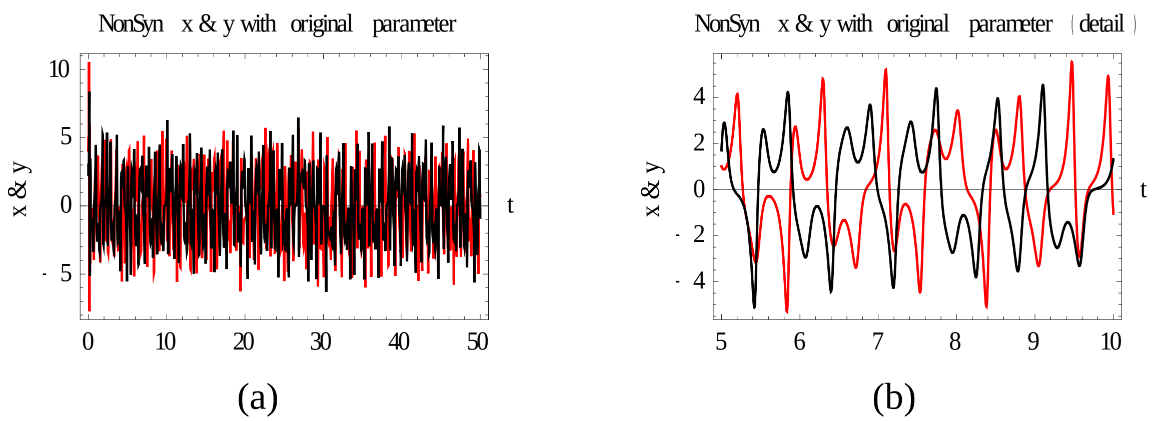
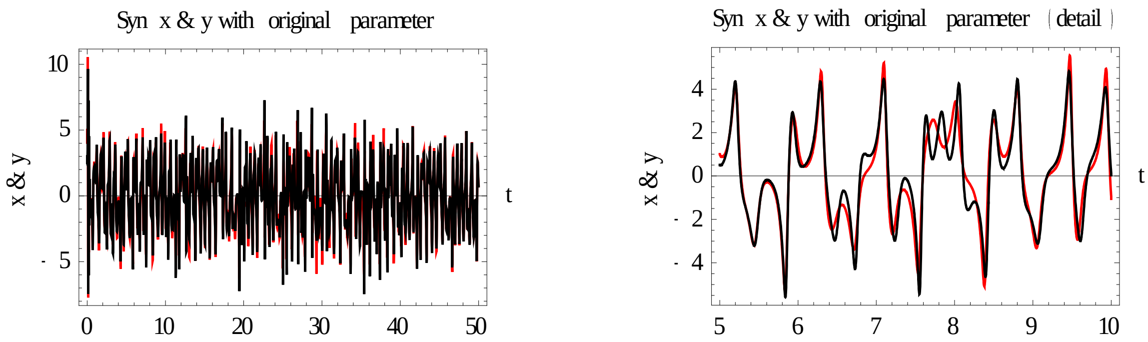
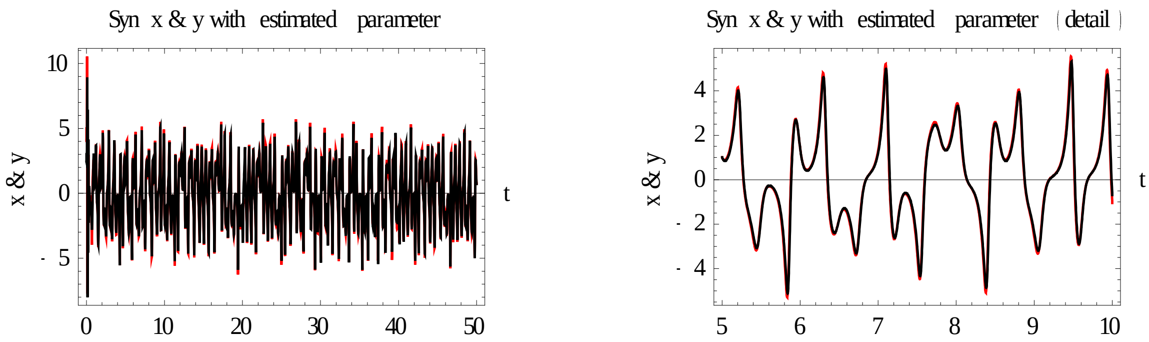


Figure 14.3. Non-synchronization of x (black) and y (red) and its detail



(a) (b)

Figure 14.4. Synchronization of x and y with original parameters and its detail



(a) (b)

Figure 14.5. Synchronization of x and y with estimated parameters and its detail

As shown in Figure 14.3, the synchronization between x and y at receiver were not identified. Figure 14.4 displays that the trajectories of 'x' converged to 'y' when APD was applied with original parameter values, the synchronization between 'x' and 'y' can be used to retrieve the information signal by subtracted from the received signal. However, the synchronization error is significant in this case. As shown in Figure 14.4.b, the quality of synchronization with original parameters is lower than that with estimated values, which was exhibited in Figure 14.5. The performance of the communication system highly relies upon the synchronization ability of chaotic systems.

As shown in the comparison between the transmitted signal and the synchronized chaotic signal y(t), which is constructed by the original parameters in Figure 14.6, the power density spectrums of transmitted signal and synchronized chaotic signal have a significant difference. That means the information, which is retrieved by subtracting the synchronized chaotic signal from the received waveform, will be achieved with very poor quality. So, it could not be suitable for using to extract the information in this communication system.

But it is much better when estimated parameters were applied as shown in Figure 14.7. The power spectrums of transmitted signal and the synchronized chaotic signal do not have a significant difference. The estimated chaotic synchronization signal could not the same with the carrier chaotic signal. But it clearly showed that the retrieved information signal will be better in this case.

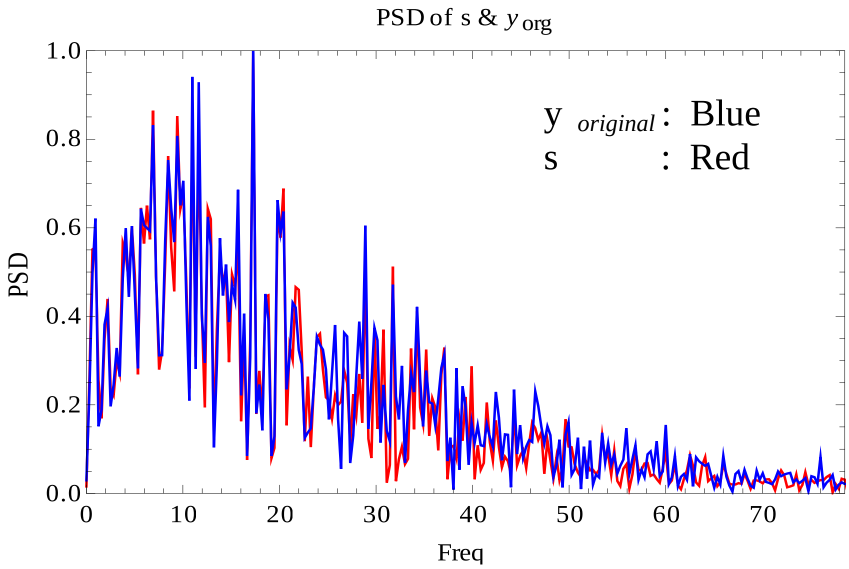


Figure 14.6. Comparison of PSD of transmitted signal and synchronized chaotic signal with original parameters.

Therefore, it has been proven that the estimated values were effective to retrieve the information signal in chaotic masking communication scheme. CMS by using estimated parameters is much better than that of original values. By this way, the performance of communication system is increased.

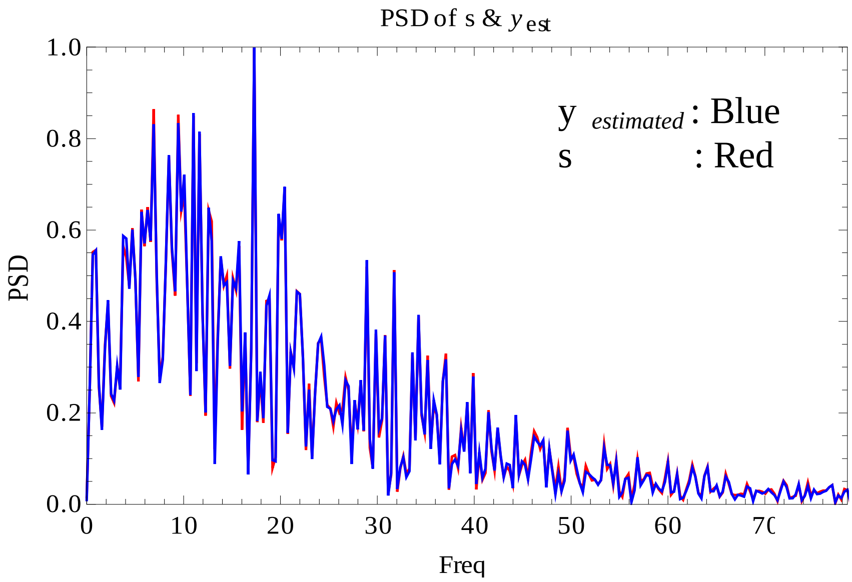


Figure 14.7. Comparison of PSD of transmitted signal and synchronized chaotic signal with estimated parameters.

15. Discussions and Conclusions

15.1. Discussions

The research was motivated by the many promises that the evolutionary algorithm offer for the chaotic secure communication. The system performance generally depends on the quality of chaos synchronization. It has been shown that the synchronization error always exist in the communication system. Therefore, application of evolutionary algorithms to improve the quality of communication chaos is feasible.

PC method, APD method and FB method were applied to synchronize two identical chaos systems. The synchronization errors were used to formulate the cost function of the optimization problem. Parameter estimation for chaotic synchronization system was formulated as a multidimensional optimization problem. SOMA and DE were used to find the unknown parameters by minimizing cost function.

All three methods (PC, APD and FB) were effective in synchronizing two chaotic systems under different initial conditions. We observed that PC method of chaos synchronization works clearly well for the chaotic systems in Chapter 8, 11, 12. However it requires dividing the original system into two stable subsystems. So that, in some case the synchronization could not achieve. The FB method is strongest and the easiest to synchronize two chaotic system. However, the quality of this method is low by the presence of parameter controls 'g'. APD is different from the PC method. While the PC method allows for a given chaotic system only a finite number of possible decompositions to produce synchronization, here the freedom to choose the driving signal makes the APD method very powerful and general, due to its extreme flexibility in applications.

Because of the irregular behavior of chaotic systems, there is a lot of local optimum in the landscape of cost function, but DE and SOMA easily escaped and achieved the global optimum parameters. The research results are believed to represent a practical basis for the application of evolutionary algorithm in minimizing the synchronization error in chaotic communication systems. SOMA and DE gave the positive results in most simulations.

In Chapter 8 we have studied the effect of PC method on identical chaotic synchronization and the performance of evolutionary algorithm such as DE and SOMA. Chapter 9 showed that the successful of EA on the synchronization via APD method, and the feedback method was executed in Chapter 10. Chapter 11 and Chapter 12 are the answer to the question of whether EA can be applied to those systems higher (5 and 6) dimensions do not.

The experimental results obtained in Chapter 13 showed that the synchronization of two different chaotic systems can be achieved with control function, which was designed by using EA. The enhancement of the synchronization in chaotic secure communication is confirmed in Chapter 14.

We have demonstrated that the synchronization qualities were achieved by estimated parameters is always better than that of original, except in Chapter 12, the estimated parameters have the same value with the original parameters. Thus, it can be stated that the synchronization qualities achieved by estimated parameters is the optimum.

15.2. Conclusions

This thesis has presented a method of improving the efficiency of chaotic communication schemes. While the several synchronization methods just based on the negative transverse Lyapunov exponents, this method is based on the application of evolutionary algorithm in chaotic communication systems. The parameters of chaotic system at receiver were found, and it is effective to synchronize the driver and response chaotic systems. SOMA and DE were successful in finding the optimum values of chaos synchronization errors, which ensure for the high quality synchronization between transmitter and receiver chaotic system. It was shown that simulations give satisfactory results. Thus, it can be stated from experimental results that SOMA and DE are strong enough for improving the quality of the chaotic secure communication.

15.3. Further Research

As the future subject, it can be extended to other synchronization method to find the more suitable method, which is much stronger of synchronization. It can be executed on the more complex systems (such as multi-scroll chaotic systems) to compare the ability of this method on finding the optimum of chaotic synchronization systems. It can also be extended to the other communication systems such as CSK, DCSK, ..., or mention the effects of noise, fading, offset, *etc*… in real world.

REFERENCES

[1] Schuster, H.G and Just, W., *Deterministic Chaos*, Wiley VCH, 2005.

[2] Hilborn R.C., *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*, Oxford University Press, 2000, ISBN: 0-19-850723-2

[3] Wai T, Francis L andChi T., *Digital communications with chaos.* Elsevier, 2006, ISBN: 0-08-045151-9.

[4] Zelinka I., *Real-time deterministic chaos control by means of selected evolutionary techniques*, Engineering Applications of Artificial Intelligence, 10, 2008.

[5] Pecora, L.M. and Carroll, T. L., *Synchronization in chaotic systems,* Phys. Rev. Let., 64(8), 1990, pp.821–824.

[6] Kocarev, L and Parlitz, U., *General Approach for Chaotic Synchronization with Applications to Communication*, Phys. Rev. Lett., 74, 1995,pp. 5028–5031.

[7] Ott E,Grebogi C, Yorke J A. *Controlling chaos*. Phys.Rev.Lett., 6411, 96-1199,1990.

[8] M. Ding and E. Ott, *Enhancing synchronism of chaotic systems*, Phys. Rev. E 49, R945, 1994.

[9] Chen M, Han Z. *Controlling and synchronizing chaotic Genesio system via nonlinear feedback control*. Chaos, Solitons and Fractals, 17709-716, 2003.

[10] Liao Teh-lu .*Adaptive Synchronization of Two Lorenz Systems*, Chaos Solitons and Fractals, 9, 1555-1561. 1998.

[11] Park J H, Kwon O M. *A novel criterion for delayed feedback control of time delay chaotic systems*. Chaos, Solitons and Fractals, 23495-501, 2005.

[12] Lü Jin-hu,Zhang Suo-chun, *Controlling Chen's chaotic attractor using backstepping design based on parameters identification*. Physics Letters A, 286, 148-152, 2001.

[13] Afraimovich. V. S., Verichev. N. N., *Stochastic synchronization of oscillation in dissipative systems*, Radiophysics and Quantum Electronics, Volume 29, Issue 9, 1986, pp.795-803.

[14] Kapitaniak T. *Synchronization of chaos using continuous control*. Phys Rev E Stat Phys Plasmas Fluids Relat Interdiscip Topics. Volume 50(2), 1994, pp1642-1644.

[15] Parltiz, U., *Estimating model parameters from time series by autosynchronization*, Phys Rev Lett, 76,1996,1232–5.

[16] Keisuke, Ito**.,** *Chaos in the Lotka-Volterra two-disc dynamo system*, Earth and Planetary Science Letters Vol. 51, 2, 1980, pp. 451-456.

[17] Millen, Mc., *The shape and dynamics of the Lotka-Volterra attractor*, The Nonlinear Journal Vol.1,1999, pp. 1-10.

[18] Stenflo L. *Generalized Lorenz equations for acoustic-gravity waves in the atmosphere*. Physica Scr 1996;53:83–4.

[19] Qi G, Chen Z, Du S, Yuan Z. *On a four-dimensional chaotic system*. Chaos, Solitons & Fractals 23, 2005,1671–1682.
[20] Roy D, Musielak ZE, *Generalized Lorenz models and their routes to chaos. II. Energy-conserving horizontal mode truncations*. Chaos, Solitons and Fractals. 31. 2007.747-756.
[21] Zelinka, I., *SOMA - Self-Organizing Migrating Algorithm*, In: B.V. Babu, G. Onwubolu Eds., New optimization techniques in engineering, Springer-Verlag, chapter 7, 2004.
[22] Zelinka, I., *SOMA- Self-Organizing Migrating Algorithm*, [Online]. [01.11.2010], URL: <http://www.ft.utb.cz/people/zelinka/soma/>.
[23] Onwubolu, G and Davendra, D., *Differential Evolution: A Handbook for Global Permutation-Based Combinatorial Optimization*. Studies in Computational Intelligence, Vol. 175, Springer,2009
[24] Storn, R. and Price, K., *Differential Evolution - a Simple and Efficient Adaptive Scheme for Global Optimization over Continuous Spaces*" , Technical Report TR-95-012, ICSI, March 1995,
[25] Hervé Dedieu., 1993, *Chaos shift keying: Modulation and Demodulation of a chaotic carrier using self-synchronizing Chua's circuits*, IEEE Transactions on Circuits and Systems, 1993.
[26] Liu, C.X.: *A new hyperchaotic dynamical system*. Chinese Physics 16 (2007).
[27] O. E. Rössler ., *An Equation for Continuous Chaos*. Physics Letters 57A (5): 397–398, 1976.
[28] Otto E. Rössler., Rössler_attractor, [Online].[01.11.2010], URL: <http://www.scholarpedia.org/article/Rössler _attractor>
[29] J. Lü, G. Chen and S. Zhang, *Dynamical analysis of a new chaotic attractor*. Int J Bifurcat Chaos, 12 (2002), pp. 1001–1015.
[30] Kennamer, K.: *Studies of the onset of chaos in the Lorenz and generalized Lorenz systems*. Master's thesis, University of Alabama in Huntsville (1995)
[31] Nguyen, T.D., Ivan Zelinka. *Chaos theory in secure communication*. Mendel 2009, In Proc. 15th International Conference on Soft Computing, Brno, Czech Republic, 24 - 26 June 2009, pages 147-153, ISBN: 978-80-214-3884-2.
[32] Nguyen, T.D., *Chaos synchronization in none-ideal channel by differential evolution algorithm*. Mendel 2010, In Proc. 16th International Conference on Soft Computing, Brno, Czech Republic, 23 -25 June 2010, pages 49-55, ISBN: 978-80-214-4120-0.
[33] Nguyen, T.D., Ivan Zelinka. *Using method of artificial intelligence to estimate parameters of chaotic synchronization system*. Mendel 2011, In Proc. 17th International Conference on Soft Computing, Brno, Czech Republic, 15 -17 June 2011, pages 22-29, ISSN 1803-3814.
[34] Nguyen, T.D., Ivan Zelinka. *Using Differential Evolution for Parameter Estimation in Five Dimensions Chaotic Synchronization Systems*. Odborný vědecký časopis Trilobit. Vol.2, 2011. ISSN 1804-1795. [Online]

http://trilobit.fai.utb.cz/using-differential-evolution-for-parameter-estimation-in-five-dimensions-chaotic-synchronization-systems.

[35] Nguyen T.D., Ivan Zelinka. *Applied Differential Evolution to Estimate Parameters in Four-Dimensional Chaotic Synchronization Systems*. Kybernetika-International journal published by Institute of Information Theory and Automation, Vol.X, p.xx-xx, 201x.(re-submitted)

[36] Nguyen T.D., Phan. T.T.D., and Roman Jasek. *Parameter Estimation in Five Dimensional Chaotic Synchronization Systems by Self-Organizing Migrating Algorithm*. WSEAS Transactions on Systems, Vol. 11, p.117-128, 2012, ISSN 1109-2777.

[37] Nguyen T.D., Ivan Zelinka. *Parameter Estimation in Five Dimensional Chaotic Synchronization Systems by Differential Evolution Algorithm*. Mendel 2012, In Proc. 18th International Conference on Soft Computing, Brno, Czech Republic, 27 -29 June 2012, p.52-57, ISSN 1803-3814.

[38] Nguyen T.D., Phan. T.T.D., and Ivan Zelinka. Application of Self-Organizing *Migrating Algorithm in Five Dimensional Chaotic Synchronization Systems via Active-Passive Decomposition*. Advances in Intelligent Systems and Computing, Vol. 192, Nostradamus: Modern Methods of Prediction, Modeling and Analysis of Nonlinear Systems, 2012, pages 203-213, ISSN 2194-5357.

[39] Nguyen T.D., Phan. T.T.D., and Ivan Zelinka. *Using Differential Evolution Algorithm in Six-Dimensional Chaotic Synchronization Systems*. Advances in Intelligent Systems and Computing, Vol. 192, Nostradamus: Modern Methods of Prediction, Modeling and Analysis of Nonlinear Systems, 2012, pages 215-224, ISSN 2194-5357.

[40] Blasius B, Huppert A, Stone L. *Complex dynamics and phase synchronization in spatially extended ecological system*. Nature *1999;399:354–9.*

[41] Zhou TS, Lu¨ JH, Chen GR, Tang Y. *Synchronization stability of three chaotic systems with linear coupling*. Phys Lett A 2002;*301:231–40.*

[42] Sun JT, Zhang YP. *Some simple global synchronization criterions for coupled time-varying chaotic systems*. Chaos, Solitons & Fractals 2004;19:93–8.

[43] Chen HK. *Global chaos synchronization of new chaotic systems via nonlinear control*. Chaos, Solitons & Fractals 2005;23:1245–51.

[44] Huang L, Feng R, Wang M. *Synchronization of chaotic systems via nonlinear control*. Phys Lett A 2004;320:271–5.

[45] Zhang J, Li CG, Zhang HB, Yu JB. *Chaos synchronization using single variable feedback based on backstepping method*. Chaos, Solitons & Fractals 2004;21:1183–93.

[46] Bai EW, Lonngren KE. *Synchronization of two Lorenz systems using active control*. Chaos, Solitons & Fractals 1997;8:51–8.

[47] Agiza HN, Yassen MT. *Synchronization of Rossler and chaotic dynamical systems using active control*. Phys Lett A 2001;278:191–7.

[48] Zhang H, Ma XK. *Synchronization of uncertain chaotic systems with parameters perturbation via active control*. Chaos, Solitons & Fractals 2004;21:39–47.
[49] Lei YM et al. *Global synchronization of two parametrically excited systems using active control*. Chaos, Solitons & Fractals 2006;28:428–36.
[50] Ho MC, Hung YC. *Synchronization of two different systems by using generalized active control*. Phys Lett A 2002;301:424–8.
[51] C.-L. Kuo, *Design of a fuzzy sliding-mode synchronization controller for two different chaos systems*, Comput. Math. Appl. 61 (2011) 2090–2095.
[52] N.-S. Pai, H.-T. Yau, C.-L. Kuo, *Fuzzy logic combining controller design for chaos control of a rod-type plasma torch system*, Expert Syst. Appl. 37 (2010)8278–8283.
[53] W. Guo, S. Chen, H. Zhou, *A simple adaptive-feedback controller for chaos synchronization*, Chaos Soliton Fract. 39 (2009) 316–321.
[54] J.M.V. Grzybowski, M. Rafikov, J.M. Balthazar, *Synchronization of the unified chaotic system and application in secure communication*, Commun.Nonlinear Sci. Numer. Simulat. 14 (2009) 2793–2806.
[55] H. Chen, G. Sheu, Y. Lin, C. Chen, *Chaos synchronization between two different chaotic systems via nonlinear feedback control*, Nonlinear Anal. 70(2009) 4393–4401.
[56] S.M. Lee, D.H. Ji, J.H. Park, S.C. Won, *H_∞ synchronization of chaotic systems via dynamic feedback approach*, Phys. Lett. A 372 (2008) 4905–4912.
[57] F. Jianwen, H. Ling, X. Chen, F. Austin, W. Geng, *Synchronizing the noise-perturbed Genesio chaotic system by sliding mode control*, Commun. Nonlinear Sci. Numer. Simulat. 15 (2010) 2546–2551.
[58] N. Cai, Y. Jing, S. Zhang, *Modified projective synchronization of chaotic systems with disturbances via active sliding mode control*, Commun. Nonlinear Sci. Numer. Simulat. 15 (2010) 1613–1620.
[59] J. Yan, Y. Yang, T. Chiang, C. Chen, *Robust synchronization of unified chaotic systems via sliding mode control*, Chaos Soliton Fract. 34 (2007) 947–954.
[60] H. Yau, *Design of adaptive sliding mode controller for chaos synchronization with uncertainties*, Chaos Soliton Fract. 22 (2004) 341–347.
[61] H. Wang, Z. Han, Q. Xie, W. Zhang, *Finite-time chaos synchronization of unified chaotic system with uncertain parameters*, Commun. Nonlinear Sci.Numer. Simulat. 14 (2009) 2239–2247.
[62] H. Yau, C. Shieh, *Chaos synchronization using fuzzy logic controller*, Nonlinear Anal. RWA 9 (2008) 1800–1810.
[63] C. Chen, *Quadratic optimal neural fuzzy control for synchronization of uncertain chaotic systems*, Expert Syst. Appl. 36 (2009) 11827–11835.
[64] C. Lin, Y. Peng, M. Lin, *CMAC-based adaptive backstepping synchronization of uncertain chaotic systems*, Chaos Soliton Fract. 42 (2009) 981–988.

[65] J. Lin, J. Yan, *Adaptive synchronization for two identical generalized Lorenz chaotic systems via a single controller*, Nonlinear Anal. RWA 10 (2009)1151–1159.

[66] J. Yan, M. Hung, T. Liao, *Adaptive sliding mode control for synchronization of chaotic gyros with fully unknown parameters*, J. Sound Vib. 298 (2006)298–306.

[67] J. Yan, M. Hung, T. Chiang, Y. Yang, *Robust synchronization of chaotic systems via adaptive sliding mode control*, Phys. Lett. A 356 (2006) 220–225.

[68] M. Pourmahmood, S. Khanmohammadi, G. Alizadeh, *Synchronization of two different uncertain chaotic systems with unknown parameters using a robust adaptive sliding mode controller*, Commun. Nonlinear Sci. Numer. Simulat. 16 (2011) 2853–2868.

[69] M.P. Aghababa, S. Khanmohammadi, G. Alizadeh, *Finite-time synchronization of two different chaotic systems with unknown parameters via sliding mode technique*, Appl. Math. Model. 35 (2011) 3080–3091.

[70] G. Zhang, Z. Liu, J. Zhang, *Adaptive synchronization of a class of continuous chaotic systems with uncertain parameters*, Phys. Lett. A 372 (2008) 447–450.

[71] X. Chen, J. Lu, *Adaptive synchronization of different chaotic systems with fully unknown parameters*, Phys. Lett. A 364 (2007) 123–128.

[72] H. Zhang, W. Huang, Z. Wang, T. Chai, *Adaptive synchronization between two different chaotic systems with unknown parameters*, Phys. Lett. A 350 (2006) 363–366.

[73] H. Salarieh, M. Shahrokhi, *Adaptive synchronization of two different chaotic systems with time varying unknown parameters*, Chaos Soliton Fract. 37(2008) 125–136.

LIST OF AUTHOR'S PUBLICATION ACTIVITIES

[1] Nguyen, T.D., Ivan Zelinka. *Chaos theory in secure communication*. Mendel 2009, In Proc. 15th International Conference on Soft Computing, Brno, Czech Republic, 24 - 26 June 2009, pages 147-153, ISBN: 978-80-214-3884-2.

[2] Nguyen, T.D., *Chaos synchronization in none-ideal channel by differential evolution algorithm.* Mendel 2010, In Proc. 16th International Conference on Soft Computing, Brno, Czech Republic, 23 -25 June 2010, pages 49-55, ISBN: 978-80-214-4120-0.

[3] Nguyen, T.D., Ivan Zelinka. *Using method of artificial intelligence to estimate parameters of chaotic synchronization system*. Mendel 2011, In Proc. 17th International Conference on Soft Computing, Brno, Czech Republic, 15 -17 June 2011, pages 22-29, ISSN 1803-3814.

[4] Nguyen, T.D., Ivan Zelinka. *Using Differential Evolution for Parameter Estimation in Five Dimensions Chaotic Synchronization Systems*. Odborný vědecký časopis Trilobit. Vol.2, 2011. ISSN 1804-1795. [Online] http://trilobit.fai.utb.cz/using-differential-evolution-for-parameter-estimation-in-five-dimensions-chaotic-synchronization-systems.

[5] Nguyen T.D., Ivan Zelinka. *Applied Differential Evolution to Estimate Parameters in Four-Dimensional Chaotic Synchronization Systems*. Kybernetika-International journal published by Institute of Information Theory and Automation, Vol.X, p.xx-xx, 201x.(re-submitted)

[6] Nguyen T.D., Phan. T.T.D., and Roman Jasek. *Parameter Estimation in Five Dimensional Chaotic Synchronization Systems by Self-Organizing Migrating Algorithm.* WSEAS Transactions on Systems, Vol. 11, p.117-128, 2012, ISSN 1109-2777.

[7] Nguyen T.D., Ivan Zelinka. *Parameter Estimation in Five Dimensional Chaotic Synchronization Systems by Differential Evolution Algorithm*. Mendel 2012, In Proc. 18th International Conference on Soft Computing, Brno, Czech Republic, 27 -29 June 2012, p.52-57, ISSN 1803-3814.

[8] Nguyen T.D., Phan. T.T.D., and Ivan Zelinka. *Application of Self-Organizing Migrating Algorithm in Five Dimensional Chaotic Synchronization Systems via Active-Passive Decomposition*. Advances in Intelligent Systems and Computing, Vol. 192, Nostradamus: Modern Methods of Prediction, Modeling and Analysis of Nonlinear Systems, 2012, pages 203-213, ISSN 2194-5357.

[9] Nguyen T.D., Phan. T.T.D., and Ivan Zelinka. *Using Differential Evolution Algorithm in Six-Dimensional Chaotic Synchronization Systems*. Advances in Intelligent Systems and Computing, Vol. 192, Nostradamus: Modern Methods of Prediction, Modeling and Analysis of Nonlinear Systems, 2012, pages 215-224, ISSN 2194-5357.

CURRICULUM VITAE

PERSONAL INFORMATION

Name	Nguyễn Thanh Dũng
Date of birth	19 April 1979
Present address	T.G.Masaryka 1281 760 01 Zlín
Marital status	Married
Contact	tel: +420 773 966 808, email:tnguyen@fai.utb.cz, thanhdungcatc@yahoo.com

EDUCATION

1994 – 1997	BenTre High School in BenTre, specialization: Mathematics, Physics, Chemistry.
1997 – 2002	University of Technical Education Ho Chi Minh City (UTE), Faculty of Electrical and Electronic Engineering (FEE), Engineer degree program Electrical and Electronic engineering.
2004 – 2007	University of Transport and Communications (UTC), Faculty of Electrical – Electronic Engineering (FEE), Master of Science degree program Electrical and Electronic engineering.
Since June 2008	Tomas Bata University in Zlín, Faculty of Applied Informatics (FAI), Student of a doctoral program in Technical Cybernetics in full-time study.

ATTENDENCE AT CONFERENCES

	2009	-Attendance at 15th International Conference on Soft Computing, Mendel 2009 in Brno, Czech Republic.
	2010	-Attendance at 16th International Conference on Soft Computing, Mendel 2010 in Brno, Czech Republic.
	2011	-Attendance at 17th International Conference on Soft Computing, Mendel 2011 in Brno, Czech Republic.

	2012	-Attendance at International conference Nostradamus 2012, Ostrava, Czech Republic. -Attendance at 18th International Conference on Soft Computing, Mendel 2012 in Brno, Czech Republic.

LANGUAGE KNOWLEDGE

Vietnamese language	native
English language	active – doctoral exam – May, 2010

EMPLOYMENT

2002 – 2003	Zodiac company, technical engineer.
2003 - 2008	Lecturer at Vietnam aviation academy (VAA), Faculty of AETE. Seminars and laboratories – Electronic circuit, Navigation system (NDB: Non-Directional Beacons).