An Introduction to the Special Issue: Recent Advances in Defense Systems: Applications, Methodology, Technology

CHRISTOS VOLOS [1], FILIPPO NERI [2]
[1] Department of Mathematics and Engineering Science, University of Military Education,
Hellenic Army Academy, Vari, GREECE
[2] Editor in Chief of WSEAS Transactions on Systems,
Department of Computer Science, University of Naples "Federico II", Naples, ITALY
chvolos@gmail.com, nerifil@gmail.com

The Special Issue “Recent Advances in Defense Systems: Applications, Methodology, Technology” is seeking to help professionals and researchers to understand the current trends to the advancement of defense systems modeling and simulation, technology, methodology, and theory. So, this Special Issue is addressed not only to scientists and engineers involved in battlefield defense capability but also to everybody who is interested in the development of the field of military science and engineering.

The major focus of this Special Issue was to support research in battlefield technology, amplify the cooperation between researchers and present the most recent achievements. The collection of equipment, vehicles, armour, structures and communication systems that are designed for use in warfare, were some of the subjects that this Special Issue had as an aim to highlight the most significant recent activities.

It is common for military technology to have been researched and developed by scientists and engineers specifically for use by the armed forces. However, in spite of the fact that many new technologies have come as a result of the military funding of science, they are not only used for military activities but also for civilian ones. So, it is very useful for the scientific community to know the research progress in various fields of military science and engineering.

In details, this Special Issue is a collection of four articles which are related with four crucial subjects in modern military operations. These are concerning the fields of autonomous mobile robots, the security of communication systems, the data encryption systems and the IT Service Management.

In recent years, unmanned vehicles (ground, aerial or surface) play a crucial role in many military missions all around the world. Especially, autonomous mobile robots have become a topic of great interest because of its ever-increasing applications in various military activities, which put human integrity in risk, such as the surveillance of terrains, the terrain exploration for explosives or dangerous materials and the patrolling for intrusion in military facilities.

So, in the first paper, the authors Christos Volos, Nikolaos Bardis, Ioannis Kyprianidis and Ioannis Stouboulos have studied the motion control of an autonomous mobile robot, which is based on a specific type of chaotic systems. These systems, which are known from the theory of nonlinear dynamical systems, produce the “double-scroll” chaotic attractors.

The aim of using nonlinear systems in the field of autonomous mobile robots is very popular due to the fact that the chaotic motion of these robots is a guarantee of success in exploration of a terrain for vigilance, search or de-mining tasks.

Therefore, this paper proposed a motion control strategy of an autonomous mobile robot, which is based on a chaotic path planning generator, in order to cover a terrain fast with unpredictable way. For choosing the system with the best appearance in regard of the terrain coverage, three different nonlinear dynamical systems with double-scroll chaotic behavior, the Chua oscillator, the Lorenz system, and a circuit with a nonlinear resistor having an current – voltage characteristic based on a saturation function, were used. The comparative study of the proposed double-scroll systems shows that the third system has significantly greater terrain coverage, among the three used dynamical systems.

Also, the subject of chaotic systems has many important applications in various engineering fields. One of them is the security of communication systems, which plays a very important role in the outcome of military operations.

So, in the second paper the authors Aceng Sambas, Mada Sanjaya and Halimatussadiyah proposed a secure communication system, which is based on the concept of “chaotic synchronization”. The chaotic synchronization is considered as the complete coincidence of the states of individual chaotic systems. This interesting behavior can result from an interaction between systems or subsystems, as well as from the influence of external noisy or regular fields. In this work, the system of two coupled nonlinear electronic circuits, in the development scheme of chaos-based secure communication system, has been used. The proposed electronic circuit implements the well-known Rossler nonlinear system. Simulation results, by using MATLAB and MultiSIM, demonstrate the chaotic synchronization of coupled chaotic Rossler circuits and the successful application of this scheme to signal masking secure communication system.

The third paper of author Nikolaos Doukas investigates aspects concerning privacy during the communication of low color depth images in encrypted form via low bit-rate, error prone channels. As it is known, cyber security and privacy are sources of increasing importance for the successful deployment of information and communication technology. It is a fact that in military operations the information systems and transmission networks, which are extended to the last soldier, has greatly increased the importance of managing the risk of some of the content traveling towards the command centers falling on hostile hands. So, communication of data and especially of image data is of paramount importance.

In details, this paper presents the existing approaches for region of interest determination in images, image encryption and image compression within this context. The problem is established and conflicts between the aims of data compression and data encryption are out-lined and theoretically founded. An innovative approach is hence presented that automatically selects regions of interest in low color depth images, while achieving an acceptable level of security without increasing the data volume of the resulting image. The technique is suitable for cases where the data being transmitted has a limited lifecycle period and the compressed and encrypted image data are likely to be corrupted, such as the transmission via channels that are not guaranteed error – free. An error correction add-on to the algorithm permits an increase on the average decrypted image quality. Initial crypt-analytic resilience results for the proposed scheme are given. The proposed scheme is intended as a means of facilitating the deployment of COTS technology in tactical situations, by increasing the level of security of the underlying infrastructure.

Authors Anel Tanovic and Fahrudin Orucevic, in the fourth paper, present a new ITIL framework. ITIL (Information Technology Infrastructure Library) is the most popular framework for the management of IT services, while ISO/IEC 20000 is the first IT Service Management standard. Today many researches from IT Service Management field are connected to the comparison of two or more frameworks or standards. The goal of these researches is to create a new universal framework or standard for the management of IT services which should be better than ITIL from 2011.

This paper is based on two different measurements of the system implementation: the first one is a measurement by using ITIL recommendations and the second one is a measurement by using recommendations of ISO/IEC 20000 standard. The aim is to see in which ITIL processes the result of measurement is bad, to find complementary ISO/IEC 20000 processes in which the result is good, and based on this to suggest a new model of ITIL framework for the design and implementation of the system for x-play services of Telecom operator. The scientific value of this paper is a new produced ITIL framework which could be used also for some other Telecom operator's systems.

The “Recent Advances in Defense Systems: Applications, Methodology, Technology” is created from researchers and scientists of various engineering fields, which study crucial issues of military operations. We hope this Special Issue will be the first step towards the development of closer cooperation between research groups working on the subject of defense systems. Also, we look forward to hearing reactions and learning from the reader of this Issue, who will ultimately judge this effort.

Motion Control of a Mobile Robot Based on Double-Scroll Chaotic Circuits

CHRISTOS K. VOLOS AND NIKOLAOS BARDIS
Department of Mathematics and Engineering Studies
University of Military Education - Hellenic Army Academy
Athens, GR-16673
GREECE
chvolos@gmail.com, bardis@itr.gr

IOANNIS M. KYPRIANIDIS AND IOANNIS N. STOUBOULOS
Department of Physics
Aristotle University of Thessaloniki
Thessaloniki, GR-54124
GREECE
imkypr@auth.gr, stouboulos@physics.auth.gr

Abstract: - In this paper, the motion control of a mobile robot, which is based on a specific type of chaotic systems, is studied. These systems produce the well-known from the nonlinear theory double-scroll chaotic attractors. So, the proposed motion control strategy of the mobile robot is based on a chaotic path planning generator in order to cover a terrain fast and with unpredictable way. For choosing the system with the best appearance in regard of the terrain coverage, three different nonlinear dynamical systems with double-scroll chaotic behavior, the Chua oscillator, the Lorenz system, and a circuit with a nonlinear resistor having an i-v characteristic based on a saturation function, were used. The comparative study of the proposed double-scroll systems shows that the third system has significantly greater terrain coverage, among the three used dynamical systems.

Key-Words: - Mobile robot, motion control, chaos, Chua circuit, Lorenz system, double-scroll chaotic attractors.

1 Introduction

In the last decades the research field of autonomous mobile robots has become a topic of great interest because of its ever-increasing applications in various activities. Industrial transportation, floor-cleaning devices and fire fighting devices have been developed accenting autonomous mobile robots as very useful tools in industrial and civil life [1-3]. Also, many military activities, which put human integrity in risk, such as the surveillance of terrains, the terrain exploration for explosives or dangerous materials and the patrolling for intrusion in military facilities, have driven to the development of intelligent robotic systems [4-6].

Especially, in these military missions robotic systems must have some very important features such as the perception and identification of the target, the positioning of the robot on the terrain and the updating of the terrain's map. However, the most useful feature, determining the success of these military missions, is the path planning. For this reason many research teams trying to find out the way to generate a trajectory, which will guarantee the surveillance of the entire terrain or the finding of the explosives. Furthermore, in the case of patrolling for intrusion, the path of the robot must be as much difficult to be predicted by the intruder as possible. So, the mission of patrolling a terrain with a mobile robot is an issue that has to do with finding a plan which must satisfy three major targets: the unpredictability of the trajectory, the scan of the entire terrain and the fast scanning of the robot's workplace. These are the basic requirements for selecting the most suitable autonomous mobile robots for the specific kind of missions.

These characteristics were the beginning of using nonlinear dynamical systems in the development of autonomous mobile robots, especially in the last decade [6-8]. As it is known, nonlinear systems have a very rich dynamic behavior, showing a variety of chaotic phenomena. This chaotic behavior is the reason for which nonlinear systems have been used in many other engineering fields such as communications, cryptography, random bits generators and neural networks [10-14].

The aim of using nonlinear systems in autonomous robots is achieved by designing controllers, which ensure chaotic motion. Signals, which are produced by chaotic systems or circuits, are used to guide autonomous robots for exploration of a terrain for vigilance, search or de-mining tasks. The main feature of chaotic systems, which is the unpredictability, is a necessary condition in the previous mentioned tasks. In the literature very known chaotic systems, such as Arnold dynamical system, Standard or Taylor-Chirikov map, Lorenz system and Chua circuit, have been used [4,5,15-18].

In this work, the motion control strategy of a mobile robot is studied, in order to generate the most unpredictable trajectory. This is implemented by using different chaotic path planning generators. The common feature of the used chaotic generators is the production of double-scroll chaotic attractors. The comparative study accents the chaotic system with the better results in regard to unpredictability of the trajectory and the coverage rate of the robot's workplace.

The rest of the paper is organized as follows. In the next section the basic features of chaotic systems are presented. The mathematical models of the nonlinear systems, which are adopted as robot's driver and the proposed model for the robot are described in Section 3. The simulation results and their analysis are presented in Section 4. Finally, Section 5 includes the conclusions of this work.

2 Chaotic Systems

The basic components of the chaotic robotic systems, which are developed nowadays, are microcontrollers or CPUs for controlling their chaotic motion [5]. Many researchers are trying to impart the main feature of chaotic systems to robots, which is the great sensitivity on initial conditions, so as to show unpredictable trajectories.

Nevertheless a nonlinear dynamical system, in order to be considered as chaotic, must fulfill the following three conditions [19].

1. It must be topologically mixing,
2. its chaotic orbits must be dense and
3. it must be very sensitive on initial conditions.

Firstly, the term *topologically mixing* means that the chaotic dynamical system, especially chaotic mobile robot, will move over time so that each designated area of the trajectory will eventually cover part of any particular region. This property of chaotic systems guarantees a complete scan of the entire working space environment.

The second feature of chaotic systems is that its chaotic orbits have to be dense. This means that, the trajectory of a dynamical system is dense, if it comes arbitrarily close to any point in the domain.

Finally, the most important feature of chaotic systems, as it is mentioned, is the sensitivity on initial conditions. This means that a small variation on a system's initial conditions will produce a totally different chaotic trajectory. This is the feature, which is contributed to the desired robot's unpredictable trajectory and makes the long-term prediction of this trajectory, based on finite-time measurements, practically impossible.

Therefore, based on these features of chaotic systems, a chaotic trajectory, from the perspective of an intruder, presents a complicated behavior, that does not exhibit any recurrent pattern and seems to be completely random. Nevertheless, these two approaches, chaotic and random, have a major and substantial difference. The chaotic motion in contrary to the random one, is based on determinism, which in the case of mobile robots is an advantage. This happens because the behavior of a robot can be predicted in advance only by the system designer. So, an autonomous chaotic mobile robot, with such characteristics, may be used successfully in many missions such as a patrol robot or as a de-mining device.

3 The Mobile Robot Model

Many works on kinematic control of chaotic robots is based on a typical differential motion with two degrees of freedom, composed by two active, parallel and independent wheels and a third passive wheel [4,20]. The active wheels are independently controlled on velocity and rotation sense. A well-known commercial model of this type of mobile robots is the mini-robot Khepera (Fig.1).

The above mentioned mechanism has been used to the kinematic control of the robot of this work. So, the proposed mobile robot's motion is described by the linear velocity v(t) [m/s], the angle θ(t) [rad] describing the orientation of the robot, and the angular velocity ω(t) [rad/s]. The linear velocity provides a linear motion of the medium point of the wheels axis, while the direction velocity provides a rotational motion of the robot's over the same point. In Fig.2 the description of the robot motion on a plane is shown. The robot's motion control is

Fig.1. The mobile robot Khepera.

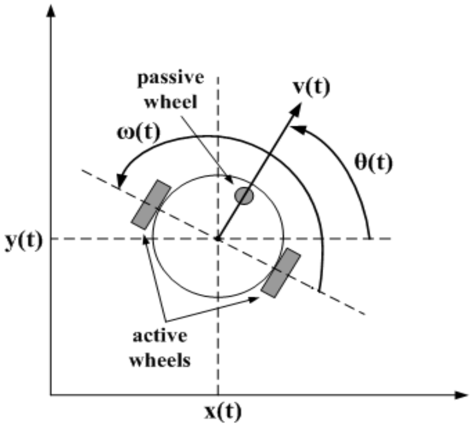


Fig.2. The description of the robot motion on a plane.

described by the following system equation (1).

$$\begin{pmatrix} \dot{x}(t) \\ \dot{y}(t) \\ \dot{\theta}(t) \end{pmatrix} = \begin{pmatrix} \cos\theta(t) & 0 \\ \sin\theta(t) & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} v(t) \\ \omega(t) \end{pmatrix} \qquad (1)$$

where, {x(t), y(t)} is the robot's position on the plane and θ(t) is the robot's orientation. Also, it must be mentioned that in the case in which the robot reaches the borders of the terrain, the robot stops and waits the next direction order to move.

Furthermore, in many cases, robots move in spaces with boundaries like walls or obstacles. So, many robots have sensors, like sonar or infrared devices (like Khepera), which provide the capability to detect the presence of obstacles or even more the recognition of the searched objects or intruders. In this work, for a better understanding of the robot's kinematic behavior we assume that the robot, by using the proposed control scheme, works in a smooth state space without any sensor. So, when the robot reaches to a boundary stops and waits the next motion order from the chaotic generator.

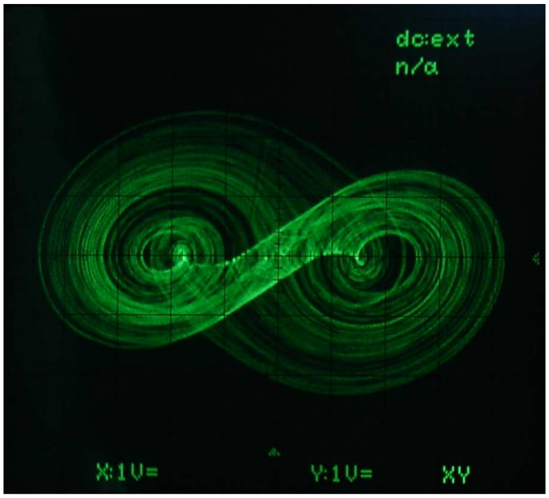


Fig.3. Experimental double-scroll chaotic attractor.

4 The Double-Scroll Systems

It has been known, that many nonlinear functions can generate chaos. Typical examples are piecewise-linear functions (e.g. Chua's circuit) [21-26], the smooth cubic function (e.g. the Duffing oscillator) [27-29], the smooth quadratic function (e.g. the Lorenz system) and the piecewise-quadratic function [30]. Among them Chua's circuit is a paradigm for chaos, being a simple nonlinear electrical circuit that exhibits double-scroll chaotic attractors (Fig.3). An alternative way for generating double-scroll like behavior was proposed by means of a simple circuit implementation [31].

Since there are many chaotic systems, which pattern is a good candidate to be chosen for use as a chaotic path planning generator? In general the criterion in many works is the largest possible coverage area through computer simulation.

In this work three of the most well-known double-scroll systems are used. These are the Chua and Lorenz systems, because they were used in previous works, as such a double-scroll chaotic system based on a saturated function proposed by Volos, Kyprianidis and Stouboulos (VKS) [32].

4.1 Chua Circuit

As it is mentioned, the first one is the dynamical system (2), which describes the most studied nonlinear circuit, the Chua circuit (Fig.4). This nonlinear circuit has been studied both theoretically and experimentally and a variety of phenomena, which are related with Chaos theory, such as the dependence of a system on initial conditions, the crisis of chaotic attractors and the

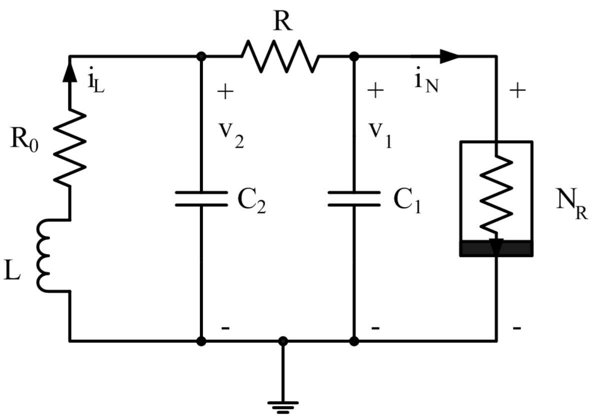


Fig.4. The Chua's circuit.

route to chaos through the period doubling, are observed [23-25].

Chua circuit has three equilibrium points. One of these equilibria is the origin, the other two usually referred as P^+ and P^{-}. These two latter points are located at the center of the two holes in Fig.3. A typical trajectory of the attractor rotates around one of these equilibrium points, getting further from it after each rotation until either it goes back to a point closer to the equilibrium or either repeats the process or directs toward the other equilibrium point and repeats a similar process, but around the other equilibrium point. In both cases the number of rotations is random. This unpredictability of double-scroll chaotic attractors is one of the peculiarities of deterministic chaos.

The state equations describing the Chua's circuit are as follows:

$$\begin{cases} \dfrac{dv_1}{dt} = \dfrac{1}{C_1} \cdot \left[\dfrac{1}{R} \cdot (v_2 - v_1) - g(v_1) \right] \\ \dfrac{dv_2}{dt} = \dfrac{1}{C_2} \cdot \left[\dfrac{1}{R} \cdot (v_1 - v_2) + i_L \right] \\ \dfrac{di_L}{dt} = \dfrac{1}{L} \cdot \left[-v_2 - R_0 \cdot i_L \right] \end{cases} \quad (2)$$

where, $g(v_1)$ is a piecewise-linear function. In this paper the nonlinear element N_R of this circuit implements the cubic function of the form:

$$g(v_1) = i_N = -k_1 \cdot v_1 + k_3 \cdot v_1^3 \quad (3)$$

where, k_1, $k_3 > 0$. The practical circuit for realizing the cubic polynomial of Eq.(3) is shown in Fig. 5 [26]. The two terminal nonlinear resistor N_R consists of one Op Amp (LF411), two analog multipliers (AD633JN) and five resistors.

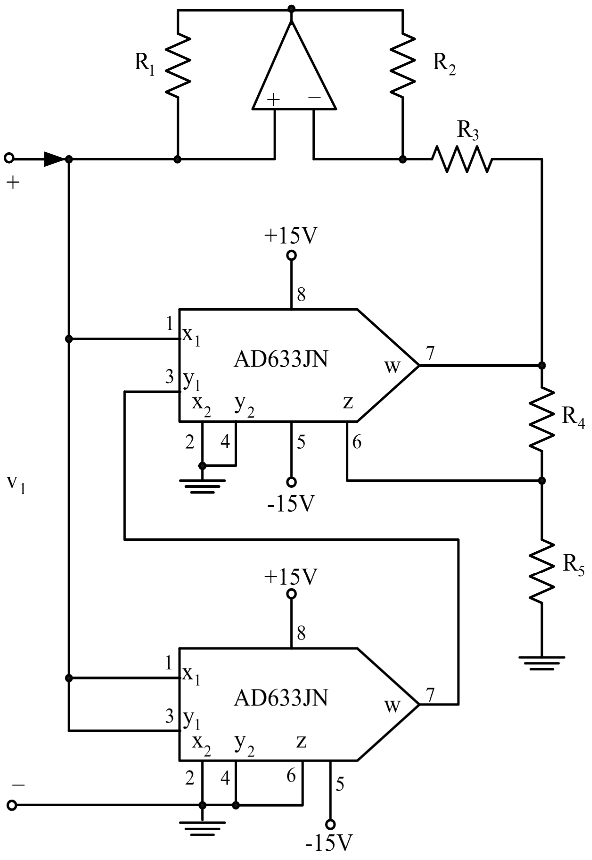


Fig.5. Practical circuit for realizing the cubic polynomial v-i characteristic.

Each multiplier implements the function:

$$w = \frac{(x_1 - x_2) \cdot (y_1 - y_2)}{10V} + z \quad (4)$$

where the factor 10V is an inherent scaling voltage in the multiplier. The connections of the Op-Amp and the resistors R_1, R_2 and R_3 form an equivalent negative resistor R_e, when $R_1 = R_2$ and the Op-Amp operates in its linear region, in order to obtain the desired coefficients k_1 and k_2. The voltages of the positive and negative electrical sources are ±15V. The driving point v-i characteristic of N_R is as below:

$$i_N = -\frac{1}{R_3} \cdot v_1 + \frac{R_4 + R_5}{R_3 \cdot R_4} \cdot \frac{1}{10V} \cdot \frac{1}{10V} \cdot v_1^3 \quad (5)$$

where,

$$k_1 = \frac{1}{R_3} \text{ and } k_3 = \frac{R_4 + R_5}{R_3 \cdot R_4} \cdot \frac{1}{10V} \cdot \frac{1}{10V}.$$

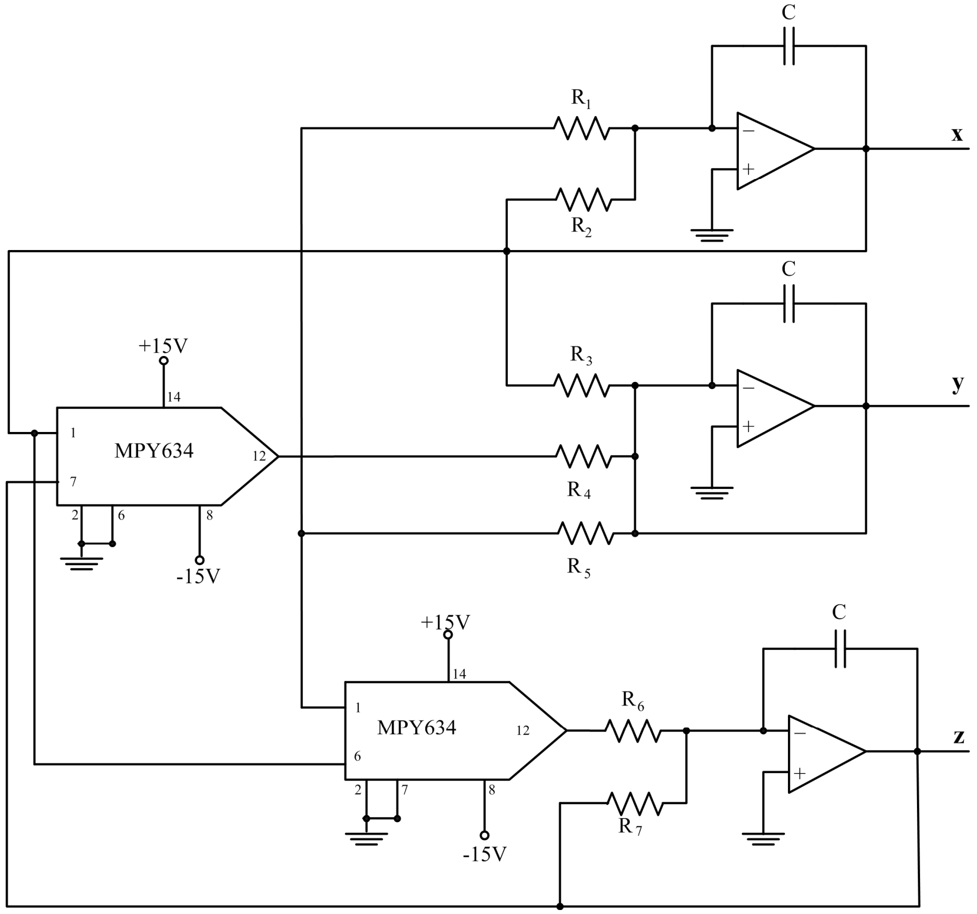


Fig.6. The Lorenz circuit.

4.2 Lorenz System

In 1963 the meteorologist Edward Lorenz published his famous set of coupled nonlinear first-order ordinary differential equations. They are relatively simple, but the resulting behavior is wonderfully complex. In this system the control parameters are the Rayleigh number r, the Prandtl number σ, and the geometric factor b. The equations are:

$$\begin{cases} \dfrac{dx}{d\tau} = \sigma \cdot (-x + y) \\ \dfrac{dy}{d\tau} = r \cdot x - y - x \cdot z \\ \dfrac{dz}{d\tau} = -b \cdot z + x \cdot y \end{cases} \qquad (6)$$

Since today a great number of different implementations of Lorenz equation have been proposed. In this work a simple implementation with just 3 Op-Amps (LF411) and two analog multipliers (MPY634) have been used (Fig.6).

4.3 VKS Circuit

Finally, the third dynamical circuit (Fig.7) is described by the dimensionless system (7).

$$\begin{cases} \dfrac{dx}{d\tau} = y \\ \dfrac{dy}{d\tau} = z \\ \dfrac{dz}{d\tau} = -\alpha \cdot (x + y + z) + b \cdot f(x) \end{cases} \qquad (7)$$

where, α and b are the circuit parameters and are defined as follows:

$$\alpha = (R \cdot C)^{-1}, b = (R_X \cdot C)^{-1} \qquad (8)$$

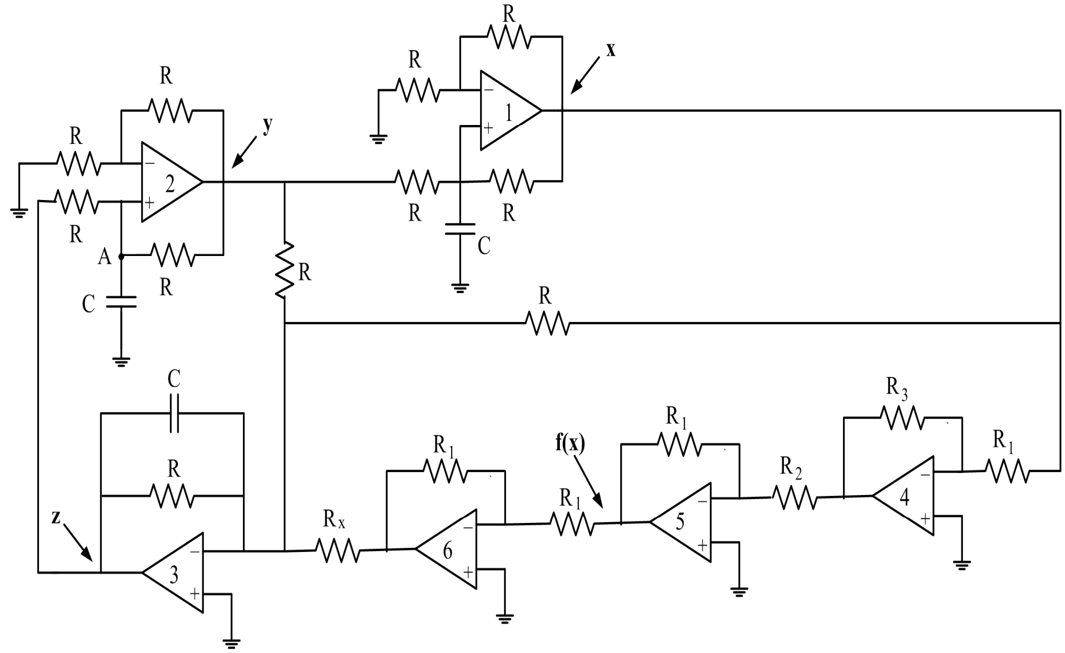


Fig.7. The VKS circuit.

The state parameters x, y, and z represent the voltages at the outputs of the operational amplifiers numbered as “1”, “2” and “3” respectively, as shown in Fig.7.

Function f(x) (Eq.9) is a saturation function, which is calculated in such a way that the saturation plateaus are ±1 and the slope of the intermediate linear region is $k = R_3/R_2$.

$$f(x) = \begin{cases} 1, & \text{if} \quad x > \frac{R_2}{R_3}\cdot 1V \\ \frac{R_3}{R_2}\cdot x, & \text{if} \quad -\frac{R_2}{R_3}\cdot 1V \le x \le \frac{R_2}{R_3}\cdot 1V \\ -1, & \text{if} \quad x < -\frac{R_2}{R_3}\cdot 1V \end{cases} \quad (9)$$

Furthermore, all the Op-Amps were of the type LF411 and the voltages of the positive and negative power supplies were set ±15V.

5 Numerical Simulations

In this work for integrating the three dynamical systems into the proposed robot’s controller a known strategy is used. In all systems the parameter z will be the angular position θ.

So, the angular velocity of the robot will be:

$$\omega = \frac{d\theta}{d\tau} = \frac{dz}{d\tau} \quad (10)$$

Also, by adding into systems (2), (6) and (9) the two following equations (11), which correspond to mobile robot’s motion, three five-dimension systems are created.

$$\begin{cases} \frac{dX}{d\tau} = v\cdot\cos(n\cdot z) \\ \frac{dY}{d\tau} = v\cdot\sin(n\cdot z) \end{cases} \quad (11)$$

In the above system (X, Y) are the coordinates of the robot’s position on terrain and v is a constant velocity of the mobile robot. Furthermore, n is a factor of normalization so parameter z of each system has the same magnitude. With this technique the three control dynamical systems give comparable results.

To test the proposed control strategy of a mobile robot the results of the numerical simulations are presented in details in this paragraph. For this reason the terrain coverage, using the known coverage rate (C), which represents the effectiveness, as the amount of the total surface covered by the robot running the algorithm, is used.

The coverage rate (C) is given by the following equation:

$$C = \frac{1}{M} \cdot \sum_{i=1}^{M} I(i) \qquad (12)$$

where, I(i) is the coverage situation for each cell in which the terrain has been divided [33]. This is defined by the following equation

$$I(i) = \begin{cases} 1, & \text{when the cell i is covered} \\ 0, & \text{when the cell i is not covered} \end{cases} \qquad (13)$$

where, i = 1, 2, ..., M. The robot's workplace is supposed to be a square terrain with dimensions $M = 20m \times 20m = 400m^2$ in normalized unit cells. Furthermore, a second interesting evaluation criterion is the coverage time of the system, which is the total time for the system to cover the entire terrain.

In this work, the three proposed dynamical systems were solved numerically by using the fourth order Runge-Kutta algorithm. Searching for sets of optimal parameters for the three dynamical systems for generating the best possible patterns is a very time-consuming task. Therefore, for convenience, we retain their original parameters of these systems as used in the literature. So, the parameters, the initial conditions and the factor n of each system, which were chosen in order to appear double-scroll chaotic attractors, are:

- The values of parameters of Chua's circuit are: R_0 = 30Ω, R = 1960Ω, R_1 = R_2 = 2kΩ, R_3 = 1.671kΩ, R_4 = 3.01kΩ, R_5 = 7.887kΩ, C_1=7.4nF, C_2 = 95.8nF. Also, the set of initial conditions is: (x_0, y_0, z_0) = (0.8, -0.2, 0.4) and n = 4.4.

- The values of parameters of Lorenz's circuit are: R_1 = R_2 = 100kΩ, R_3 = 35.7kΩ, R_4 = 10kΩ, R_5 = 1MΩ, R_6 = 10kΩ, R_7 = 374kΩ C_1 = 0.1μF. So, the set of the normalized parameters and initial conditions are: {σ, r, b} = {5, 28, 0.375},(x_0, y_0, z_0) = (1, -1, 2), and n = 1.

- The values of parameters of VKS's circuit are: R = 20kΩ, R_1 = 1kΩ, R_2 = 14.3kΩ, R_3 = 28.6kΩ, R_X = 10kΩ and C = 1nF. So, the set of the normalized parameters and initial conditions are: {α, b, k} = {0.5, 1, 2}, (x_0, y_0, z_0) = (0.5, 0.2, 0.1) and n = 14.7.

Table 1. Coverage rate of each system.

System	Coverage Rate
Chua	11.5 %
Lorenz	23.0 %
VKS	40.0 %

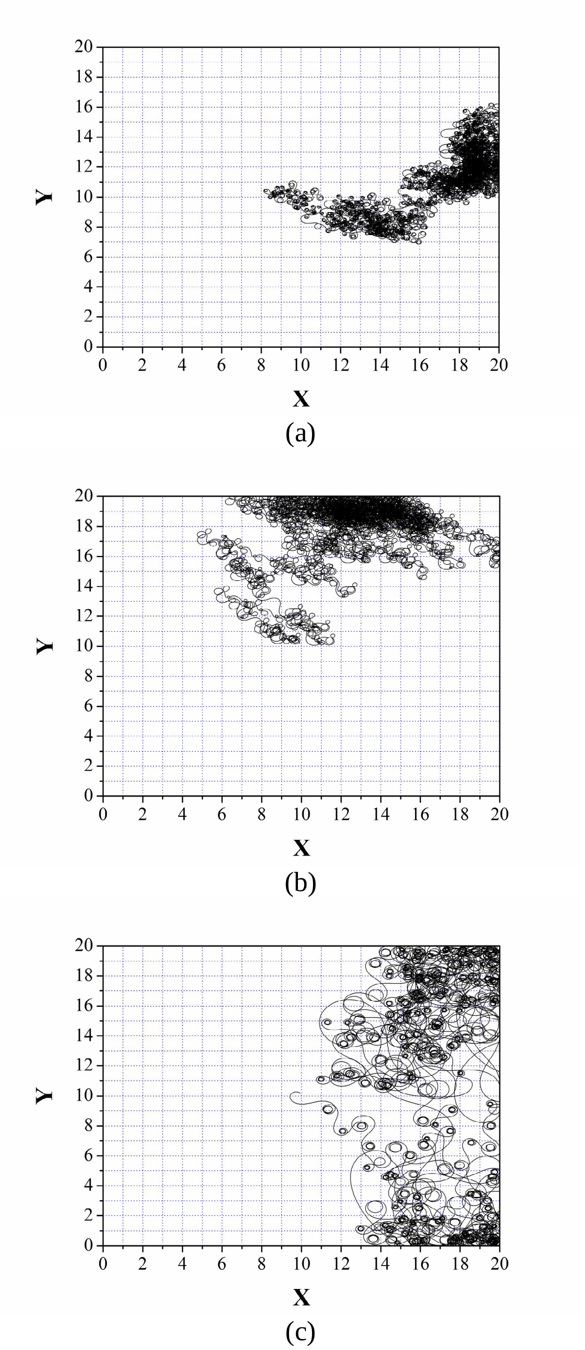
Also, in this work the initial position and velocity of the robot were chosen to be: (X, Y) = (10, 10) and v = 1m/s. Duration for run-time for simulation in this paper was 1000s.

Comparison results of the three proposed dynamical systems, are shown in Figs.8(a)-(c). In these figures simulations of the mobile robot's behavior of each system are presented. Also, in Table 1 the coverage rate for the three systems are compared. As it is shown, Chua circuit appears the smaller value of coverage rate among the systems. Lorenz system has two times the coverage rate of Chua circuit. Finally, VKS system shows significantly higher value of coverage rate as regards to the other systems. So, from the three proposed dynamical systems, VKS has the better performance, which is obvious in Fig.4(c) where the 40% of the terrain shows to be covered by the robot. This happens because the VKS system produces a mobile robot's orbit which is constituted by spiral curves that abstain longer distances concerning the other two systems, as it appears in Fig.8(c).

Finally, by choosing the system with the best results, that is VKS system, we run the simulation until the mobile robot covers the whole terrain. Also, the set of initial conditions have been changed, (x_0, y_0, z_0) = (0.8, -0.2, 0.4), so as to be proved that the chaotic motion of the robot is different but independent of the choice of systems initial conditions. The mobile's robot motion path is shown in Fig.9. As it is obvious the terrain has been covered by the robot in 99.25% (only three cells have not been covered) in time of 5000s.

6 Conclusion

In this work a comparative study of three different chaotic circuits which are used for the driving strategy of a mobile robot was presented. For the aim of this approach the most well-known double-scroll chaotic systems were chosen. The first one



(a)

(b)

(c)

Fig.8. The mobile robot's motion path with (a) Chua, (b) Lorenz and (c) VKS system.

was the Chua circuit while the second was a circuit which implements the Lorenz equation. The third one was a circuit (VSK) which its nonlinear element has a saturation function for i-v charactreristic.

This approach is followed in order to generate the most unpredictable trajectory, as well as the trajectory with the higher coverage rate of a specific terrain. The results of the comparative study show that the VSK system has significantly higher terrain

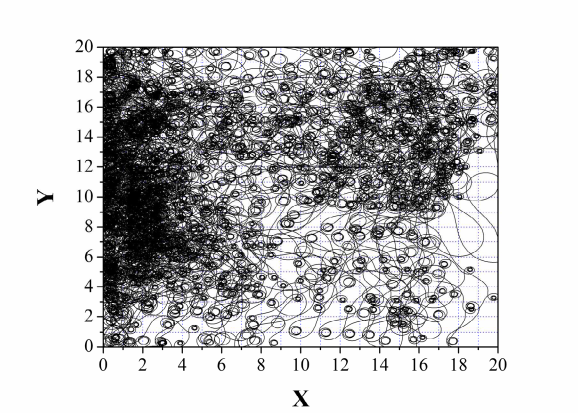


Fig.9. The mobile robot's motion path with VKS system, after 5000s.

coverage, which is the criterion of success of such robot's mission, among the proposed dynamical systems. This result was produced because of the nature of the double-scroll chaotic attractors, which were produced by the VSK system. Finally, the coverage of the whole terrain in a very satisfactory time, with the VSK system, was proved.

References:

[1] J. Palacin, J. A. Salse, I. Valganon, and X. Clua, Building a Mobile Robot for a Floor-Cleaning Operation in Domestic Environments, *IEEE Trans. Instrum. Meas.*, Vol. 53, 2004, pp. 1418–1424.

[2] M. J. M. Tavera, M. S. Dutra, E. Y. V. Diaz, and O. Lengerke, Implementation of Chaotic Behaviour on a Fire Fighting Robot, *In Proc. of the 20th Int. Congress of Mechanical Engineering*, Gramado, Brazil, November 2009.

[3] L. B. Yu, Q. X. Cao, Trajectory Planning based on Hand Operation for the Un-Redundant Arm of Service Robot, *WSEAS Trans. Syst.*, vol. 7, pp.759–768.

[4] L. S. Martins-Filho and E. E. N. Macau, *Trajectory Planning for Surveillance Missions of Mobile Robots*, Studies in Computational Intelligence, Springer-Verlag, Berlin Heidelberg, 2007, pp. 109–117.

[5] P. Sooraksa and K. Klomkarn, No-CPU Chaotic Robots: From Classroom to Commerce, *IEEE Circuits Syst. Mag.*, Vol. 10, 2010, pp. 46–53.

[6] E. Krotkov and J. Blitch, The Defence Advanced Research Projects Agency (DARPA) Tactical Mobile Robotics Program, *Int. J. Rob. Res.*, Vol. 18, 1999, pp. 769–776.

[7] O. Castillo and P. Melin, Automated Mathematical Modelling, Simulation and Behavior Identification of Robotic Dynamic Systems using a New Fuzzy-Fractal-Genetic Approach, *Robot. Auton. Syst.*, Vol. 28, 1999, pp. 19–30.

[8] S. Aoi and K. Tsuchiya, Bifurcation and Chaos of a Simple Walking Model Driven by a Rhythmic Signal, *Int. J. Nonlinear Mech.*, Vol. 41, 2006, pp. 438–446.

[9] A. T. Safa, M. G. Saadat, and M. Naraghi, Passive Dynamic of the Simplest Walking Model: Replacing Ramps with Stairs, *Mech. Mach. Theory*, Vol. 42, 2007, pp. 1314–1325.

[10] S. G. Stavrinides, A. N. Anagnostopoulos, A. N. Miliou, A. Valaristos, L. Magafas, K. Kosmatopoulos, and S. Papaioannou, Digital Chaotic Synchronized Communication System, *J. Eng. Sci. Techn. Rev.*, Vol. 2, 2009, pp. 82–86.

[11] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, Experimental Demonstration of a Chaotic Cryptographic Scheme, *WSEAS Trans. Circ. Syst.*, Vol. 5, 2006, pp. 1654–1661.

[12] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, Chaotic Cryptosystem Based on Inverse Duffing Circuit, *In Proc. of the 5th International Conference on Non – linear Analysis, Non – linear Systems and Chaos (NOLASC 2006)*, 2006, pp 92–97.

[13] M. E. Yalcin, A. K. Suykens, and J. Vandewalle, True Random Bit Generation from a Double-Scroll Attractor, *IEEE Trans. Circ. Syst. I*, Vol. 51, 2004, pp. 1395–1404.

[14] M. Ebner and S. Hameroff, Modelling of Robust Figure/Ground Separation, *In Proc. of the 3rd International Conference on Biocomputational Systems and Biotechnologies*, 2011, pp. 67–72.

[15] Y. Nakamura and A. Sekiguchi, The Chaotic Mobile Robot, *IEEE Trans. Robot. Autom.*, Vol. 17, 2001, 898–904.

[16] A. Jansri, K. Klomkarn, and P. Sooraksa, On Comparison of Attractors for Chaotic Mobile Robots, *In Proc. of the 30th IEEE Annual Conference of Industrial Electronics Society*, Vol. 3, Busan, Korea, November 2004, pp. 2536–2541.

[17] L. S. Martins-Filho and E. E. N. Macau, Patrol Mobile Robots and Chaotic Trajectories, *Math. Probl. Eng.*, Vol. 2007, 2007, p. 1.

[18] D. I. Curiac and C. Volosencu, Developing 2D Trajectories for Monitoring an Area with Two Points of Interest, *In Proc. of the 10th WSEAS Int. Conference on Automation and Information*, 2009, pp. 366–369.

[19] B. Hasselblatt and A. Katok, *A First Course in Dynamics: With a Panorama of Recent Developments*, Cambridge University Press, 2003.

[20] R. Sieqwart and I. R. Nourbakhsh, *Introduction to Autonomous Mobile Robots*, MIT Press, Cambridge, Mass, USA, 2004.

[21] L. O. Chua, C. W. Wu, A. Huang, and G. Q. Zhong, A Universal Circuit for Studying and Generating Chaos-Part I: Routes to Chaos, *IEEE Trans Circ Sys I*, Vol. 40, 1993, pp. 732–744.

[22] E. Kurt, Nonlinearities a non-autonomous chaotic circuit with a non-autonomous model of Chuas diode, *Physica Scripta*, Vol. 74, 2006, pp. 22–27.

[23] T. Matsumoto, A Chaotic Attractor from Chua's Circuit, *IEEE Trans. Circuits Syst.*, Vol. 31, 1984, pp. 1055–1058.

[24] G. Q. Zhong and F. Ayron, Global Unfolding of Chua's Circuit, *Int. J. Circuit Theory Applic.*, Vol. 13, 1985, pp. 93–98.

[25] R. Madan, Special Issue on Chua's Circuit: A paradigm for Chaos, Part I: Introduction and applications, *J. Circuit Syst. Comput.*, Vol. 3, 1993.

[26] G. Q. Zhong, Implementation of Chua's Circuit with a Cubic Nonlinearity, *IEEE Trans. Circuits Syst.*, Vol. 41, 1994, pp. 934–941.

[27] I. M. Kyprianidis, Ch. K. Volos, and I. N. Stouboulos, Experimental Study of a Nonlinear Circuit Described by Duffing's Equation, *In Proc. of I Interdisciplinary Chaos Symposium*, Vol. 4, 2006, pp. 45–54.

[28] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, Designing of Coupling Scheme between Two Chaotic Duffing – type Electrical Oscillators, *WSEAS Trans. Circuits Syst.*, Vol. 5, 2006, pp. 985–992.

[29] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, Bidirectional Coupling of Two Duffing – type Circuits, *In. Proc. of the 7th WSEAS International Conference on Systems Theory and Scientific Computation*, 2007, pp. 145–150.

[30] K. S. Tsang and K. F. Man, Generating Chaos via x|x|, *IEEE Trans. Circ. Syst. I*, Vol. 48, 2001, pp. 635–641.

[31] A. S. Elwakil, K. N. Salama, and M. P. Kennedy, A System for Chaos Generation and its Implementation in Monolithic Form, *In Proc. of IEEE Int. Symp. Circ. Syst.*, Vol. V, 2000, pp. 217–220.

[32] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, Experimental Study of the Dynamic Behaviour of a Double Scroll Circuit, *J. Appl. Funct. Anal.*, Vol. 4, 2008, pp. 703–711.

[33] S. Choset, Coverage for Robotics - A Survey of Recent Results, *Ann. Math. Artif. Intel.*, Vol. 31, 2006, pp. 113–126.

Proposal of a new model for ITIL framework based on comparison with ISO/IEC 20000 standard

ANEL TANOVIC*, FAHRUDIN ORUCEVIC **
* Department for IT development of multimedia services, BH Telecom d.d. Sarajevo
Obala Kulina Bana 8, Sarajevo 71000, Bosnia and Herzegovina
** Department of Computer Science and Informatics University of Sarajevo, Faculty of Electrical Engineering
Zmaja od Bosne bb, Sarajevo 71000, Bosnia and Herzegovina
anel.tanovic@bhtelecom.ba, forucevic@etf.unsa.ba

Abstract: - ITIL is the most popular framework for the management of IT services, while ISO/IEC 20000 is the first IT Service Management standard. Many today's researches from IT Service Management field are connected to the comparison of two or more frameworks or standards. The goal of this researches is to create a new universal framework or standard for the management of IT services which should be better than ITIL from 2011. This paper is based on two different measurements of the Billing system implementation: the first one is a measurement by using ITIL recommendations and the second one is a measurement by using recommendations of ISO/IEC 20000 standard. The aim is to see in which ITIL processes the result of measurement is bad, to find complementary ISO/IEC 20000 processes in which the result is good, and based on this to suggest a new model of ITIL framework for the design and implementation of the Billing system for x-play services of Telecom operator. The scientific value of this paper is a new produced ITIL framework which could be used also for some other Telecom operator's systems.

Key-Words: - ITIL 2011, ISO/IEC 20000, Billing system, Budgeting and Accounting services, Incident and Service Request Management, Problem Management.

1 Introduction

Information Technology Infrastructure Library or ITIL represents the best environment for the practice of a company which offer IT services as their main business function. ITIL poses a tool for implementing a service which one organization will be able to fully use with realization of the implementation of all the processes or partially use through the implementation of just a few of their processes which are considered to be helpful in developing their business results [6], [7], [8], [9], [10]. According to last version from 2011, ITIL has 5 life cycle stages: Service Strategy (which is responsible for the definition of the strategy of the organization) [6], Service Design (which is responsible for the definition of contracts with users and suppliers and for the definition of information security level) [7], Service Transition (which is responsible for the design and implementation of a new service) [8], Service Operation (which is responsible for handling with incidents and problems after a releasing into a production of a new service) [9] and Continual Service Improvement (which is responsible for continuous fully or partially improvement of IT services) [10]. Figure 1. shows ITIL 2011 with all 5 phases and 26 processes.

ISO/IEC 20000 is the first international standard for the IT Service Management [2], [3]. The goal of this standard is to integrate a set of 'best practises' into any business environment [1], [2], [5]. According to last version from 2011, ISO/IEC 20000 has 4 phases of processes: Service Delivery process (which are responsible for management of finances, for definition of contracts with suppliers and customers and for the definition of information security level), Relationship processes (which are responsible for the improvement of internal business processes for the management of suppliers), Resolution processes (which are responsible for handling and solving user's incidents and problems) and Control processes (which are responsible for the management of changes) [1], [4]. Figure 2. shows ISO/IEC 20000 standard with all 4 processes phases and 13 processes.

Section 2 of the paper describes previous research papers from this area. Section 3 of the paper presents test environment for the development of a new ITIL framework which is basically Billing system for x-play services of Telecom operator. Section 4 of the paper presents a methodology which is used for measurements covered in this paper. Section 5 of the paper presents measurements for all 26 processes of ITIL framework which are done during the design and implementation of Billing system. Section 6 of the paper shows measurements for all 13 processes of ISO/IEC 20000 standard which are done during the design and implementation of Billing system. Section 7 is the comparison between measurements which are done in section 5 and section 6. Based on this comparison, it is proposed a new model for ITIL framework which covers all Telecom operator Billing systems.

2 Previous research

The most interesting paper from this research area is the paper [22]. Several frameworks and standards are included in IT management systems in many organizations. But, they are not comprehensive enough to serve as efficient IT management system. This paper proposes a new model for ITIL framework based on comparison with CobiT framework and ISO/IEC 27002 standard. This new model of ITIL framework is universal and it could be used in every company. This new model contains a set of ‘best practices’ from IT governance which is taken from CobiT framework and a set of ‘best practises’ from information security which is taken from ISO/IEC 27002 standard. This model also contains a set of metric parameters like Key Performance Indicators and Critical Success Factors which could be used for measurements for a new model of ITIL framework. Very interesting paper similar to this is [23] in which authors have developed a new ‘maturity ITIL’ model based on research in four different Portugal organizations. The authors developed a maturity model to assess an ITIL implementation and provide a roadmap for improvement based on priorities, dependencies, and guidelines. They also demonstrated a practical application of the proposed model with a questionnaire to assess the ITIL Incident Management process that was evaluated in 2 real world organizations. Finally, in paper [24] ITIL maturity to business IT strategic alignment is validated by Strategic Alignment Maturity model. Focusing on how ITIL covers business-IT alignment maturity criteria of the model, the maturity of ITIL strategic alignment practises is assessed which makes it possible to recognize conceptual and practical competencies of ITIL to aligning business and IT in strategic level. Applying ITIL to the strategic alignment maturity model identifies opportunities to improvement in ITIL alignment perspective.

Previous research from this area is also the paper [19] which is based on description of differences between ITIL 2007 and ITIL 2011. This paper has shown how much is better ITIL 2011 than ITIL 2007 and in which processes from ITIL 2011 are needed corrections. Paper [16] presents a new model for ITIL which has only 6 processes during the implementation of IP Multimedia Subsystem in one Telecom operator in Bosnia and Herzegovina. This paper covers only processes from Service Transition phase. Paper [15] is very important for the measurements which are done here: this paper has showed that a good implemented ITIL process in some system is that process which is implemented with 75% recommendations. This research is done in test environment of IPTV/VoIP system of Telecom operator, and it is primary based on description of Supplier Management implementation. Paper [12] has introduced a new technique which is called Balanced Scorecard and which is today the most important technique for the measurement of ITIL implementation. Very similar technique to this technique is Gap analysis which was used as the main technique in this paper [10]. Paper [20] presents the difference between ITIL framework and ISO/IEC 20000 standard and shows what are disadvantages of ITIL implementation and in the same time advantages of ISO/IEC 20000 implementations in the same business environments. This paper is the introduction into research covered in this paper. The research covered is the continuous of previous research papers in improvement of actual version of ITIL [22], [23], [24], but also the first paper which gives a new model of ITIL framework from ISO/IEC 20000 standard.

In paper [25] is presented ITIL framework and its importance for the business today. Paper [12] presents Balanced Scorecard as the most popular technique for the measurement of ITIL processes. One similar technique which is called Gap analysis will be used in measurements in this paper. In paper [26] is described the usage of business process tools for modeling requirements on system changes. Paper [27] describes advantages of using some IT Service Management methodology or standard in the implementation of some cloud system. In paper [28] is described the spiral model development concept for one multimedia application.

3 Test environment

Telecom Operator, which Billing system is shown in this document as the test environment, has a total of 4 packets of x-play service: Phone (it includes IPTV and VoIP), Net (it includes IPTV and Internet), Full (it includes IPTV, VoIP and Internet) and Premi (it includes IPTV, VoIP, Internet and Mobile Telephony) [16]. Services with additional charge include: Video on Demand (VoD), PayPerView (Live) and combination of VoD service and Live service (Product). Figure 3 shows the basic components of this Billing system. These components are: IPTV service and VoIP service as the main x-play service components and 3 additional components: Video on Demand, Live and Product [16].

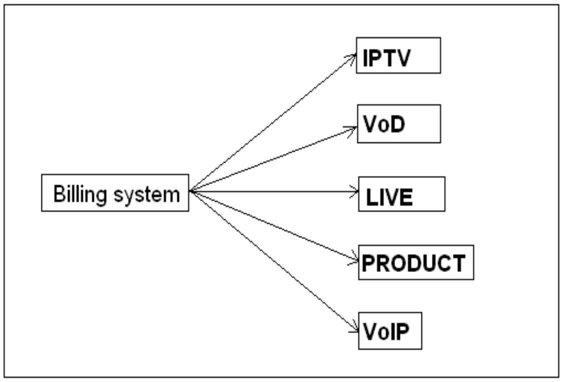


Fig. 3 - Components of Billing system for x-play services

Figure 4 presents Entity Relationship Diagram for x-play services of Telecom operator. Most important tables are signed with a red color. These tables are: table *Subscriber* which keeps all information about users, table *Cdr* which keeps information about users purchase of VoD, Live and Product contents, table *Iptvvod* which transforms data from Cdr table into final Billing tables, table *Billingvod* which makes a final consumption of VoD, Live and Product contents and finally table *Billingiptv* which makes a final consumption sum of x-play services [11], [13], [14].

4 Methodology for research

Gap analysis is a business assessment tool enabling an organization to compare where it is currently and where it wants to go in the future. This provides the organization with insight to areas which have room for improvement. This can be used to determine the gap between ‘What do we want?’ and ‘What do we need?’ for example. In last two papers [18] and [19], we have chosen Balanced Scorecard as the technique for the measurement of the implementation of ITIL processes. By using a Gap analysis technique in this paper, we want to show that this technique is also adequate for the measurement of ITIL implementations, the same as Balanced Scorecard technique [12].

The process involves determining, documenting and approving the variance between business requirements and current capabilities. Gap analysis naturally flows from benchmarking or other assessments such as service or process maturity assessments. Once the general expectation of performance is understood then it is possible to compare that expectation with the level of performance at which the company currently functions. This comparison becomes the gap analysis. Such analysis can be performed at the strategic, tactical or operational level of an organization.

Gap analysis can be conducted from different perspectives such as [10]:

- Organization (e.g. human resources)
- Business direction
- Business processes
- Information technology.

All these perspectives are shown through Key Performance Indicators for 26 ITIL processes and 13 ISO/IEC 20000 processes in next two sections of the paper.

We will use two different parameters for measurements in this paper: Key Performance Indicators (KPI) and Critical Success Factors (CSF). Each ITIL or ISO/IEC 20000 process has a few significant KPI values which are needed for the measurement of the implementation of each process. Each KPI has an assigned value, which represents the desired value for that KPI, and which is called CSF [10]. All measurements in next two sections are done by using these two formulas:

1. *Result of the KPI implementation = (KPI Measured value/CSF)*100*, if KPI is presented by numeric value
2. *Result of the KPI implementation = CSF - KPI Measured value*, if KPI is presented by percentage value.

5 Measurements of the implementation of Billing system by using key performance indicators for ITIL framework

Table 1 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Strategy Management for IT services process. The final result shows the implementation of 80% recommendations of Key Performance Indicators for this process [6], [16], [17].

Table 1 - Key performance indicators for the process: Strategy Management for IT services

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
The average number of internal factors	5	80%
The average number of external factors	8	85%
The average number of recommendations for the process: Financial Management for IT services	12	65%
The average number of recommendations for the process: Business Relationship Management	10	80%
The average number of recommendations for the process: Demand Management	6	90%
The average number of recommendations for the process: Service Portfolio Management	9	80%

Table 2 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Financial Management for IT services process. The final result shows the implementation of 70% recommendations of Key Performance Indicators for this process [6], [16], [17].

Table 2 - Key performance indicators for the process: Financial Management for IT services

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Adherence to Budgeting Process	72%	64%
Cost-/ Benefit Estimation	68%	55%
Post Implementation Review	80%	68%
Adherence to Approved Budget	82%	75%
Adherence to Project Resources	90%	77%
Proposals for Cost Optimization	85%	78%

Table 3 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Demand Management process. The final result shows the implementation of 89% recommendations of Key Performance Indicators for this process [6], [16], [17].

Table 3 - Key performance indicators for the process: Demand Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of requests for a new service by user	6000	82%
Percentage of implemented user requests for a new service	95%	88%
Number of requests for a new service from the organization	10	95%
Percentage of implemented organizational requests for a new service	15	86%
Number of requests for a new service from suppliers	45	92%

Table 4 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Service Portfolio Management process. The final result shows the implementation of 65% recommendations of Key Performance Indicators for this process [6], [16], [17].

Table 4 - Key performance indicators for the process: Service Portfolio Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Planned New Services	5	20%
Number of Unplanned New Services	5	40%
Number of Strategic Initiatives	4	100%
Number of New Customers	20000	75%
Number of Lost Customers	2000	90%

Table 5 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Business Relationship Management process. The final result shows the implementation of 82% recommendations of Key Performance Indicators for this process [6], [16], [17]. The best implemented Key Performance Indicator is The average of test users (86%) and the least implemented Key Performance Indicator is Percentage of satisfied users (78%). The possible improvements for this process are needed in the future.

Table 5 - Key performance indicators for the process: Business Relationship Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
The average number of test users	500	86%
The percentage of completed questionnaires	90%	82%
Percentage of satisfied users	90%	78%

Table 6 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Design Coordination process. The final result shows the implementation of 88% recommendations for this process [7], [16], [17].

Table 6 - Key performance indicators for the process: Design Coordination

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
The time of production of IT service design packages	20 days	98%
The number of improved IT services	2	100%
The number of created policies and procedures	8	86%
The average number of work teams for a single process	6	83%
The average time for the planning of design	8 days	74%

Table 7 shows KPIs and results of the KPIs implementation in the test environment of Billing System for Service Catalogue Management process. The final result shows the implementation of 84% recommendations.

Table 7 - Key performance indicators for the process: Service Catalogue Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
The number of implemented service catalogues	6	94%
The time needed for the implementation of service catalogue	8 days	85%
The time required to maintain the service catalogue	15 days	67%
The percentage of successfully inserted content	90%	88%
The percentage of unused service catal.	95	87%

Table 8 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Service Level Management process. The final result shows the implementation of 81% recommendations of Key Performance Indicators for this process [7], [16], [17].

Table 8 - Key performance indicators for the process: Service Level Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Services covered by SLAs	3	74%
Services covered by OLAs	3	82%
Monitored SLAs	5	90%
SLAs under Review	2	82%
Fulfillment of Service Levels	3	85%
Number of Service Issues	7	73%

Table 9 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Capacity Management process. The final result shows the implementation of 86% recommendations of Key Performance Indicators for this process [7], [16], [17].

Table 9 - Key performance indicators for the process: Capacity Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Incidents due to Capacity Shortages	7	87%
Exactness of Capacity Forecast	12	78%
Capacity Adjustments	5	80%
Resolution Time of Capacity Shortage	12h	83%
Capacity Reserves	90%	90%
Percentage of Capacity Monitoring	99%	98%

Table 10 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Availability Management process. The final result shows the implementation of 85% recommendations of Key Performance Indicators for this process [7], [16], [17]. The best implemented Key Performance Indicator is Service Availability (91%) and the least implemented Key Performance Indicator is Number of Service Interruptions (with the percentage of the implementation of 77%).

Table 10 - Key performance indicators for the process: Availability Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Service Availability	95%	91%
Number of Service Interruptions	3	77%
Duration of Service Interruptions	3h	82%
Availability Monitoring	100%	89%
Availability Measures	5	84%

Table 11 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for IT Service Continuity Management process. The final result shows the implementation of 85% recommendations of Key Performance Indicators for this process [7], [16], [17].

Table 11 - Key performance indicators for the process: IT Service Continuity Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Business Processes with Continuity Agreements	90%	65%
Gaps in Disaster Preparation	15	78%
Implementation Duration	5 days	70%
Number of Disaster Practices	10	95%
Number of Identified Shortcomings during Disaster Practices	6	88%
Business Processes with Continuity Agreements	13	94%

Table 12 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Information Security Management process. The final result shows the implementation of 87% recommendations of Key Performance Indicators for this process [7], [16], [17]. Information Security Management defines administration roles and levels of information security in Billing system. The best implemented Key Performance Indicator is Number of implemented preventive measures (94% of successful implementation) and the least implemented Key Performance Indicator is Number of Identified Shortcomings during Security Tests (85% of successful implementation). Table 12 shows a good level of successful implemented KPIs for Information Security Management.

Table 12 - Key performance indicators for the process: Information Security Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Implemented Preventive Measures	14	94%
Implementation Duration	9 days	87%
Number of Major Security Incidents	12	85%
Number of Security Tests	20	92%
Number of Identified Shortcomings during Security Tests	5	85%

Table 13 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Supplier Management process. The final result shows the implementation of 92% recommendations of Key Performance Indicators for this process [7], [16], [17].

Table 13 - Key performance indicators for the process: Supplier Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Agreed Contracts	7	92%
Number of Contract Reviews	10	88%
Number of Identified Contract Breaches	8	95%

Table 14 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Transition Planning and Support process. The final result shows the implementation of 86% recommendations of Key Performance Indicators for this process [8], [16], [17].

Table 14 - Key performance indicators for the process: Transition Planning and Support

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
The percentage of implemented plans	98%	95%
The number of IT services versions	9	86%
The percentage deviation from the expected real goals	85%	78%
The percentage of satisfied users	92%	91%
The number of reduced deviation	10	80%

Table 15 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Change Management process. The final result shows the implementation of 79% recommendations of Key Performance Indicators for this process [8], [16], [17].

Table 15 - Key performance indicators for the process: Change Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Number of Major Changes	20	85%
Time for Change Clearance	48h	70%
Change Acceptance Rate	95%	82%
Number of Urgent Changes	25	80%

Table 16 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Service Asset and Configuration Management process. The final result shows the implementation of 78% recommendations of Key Performance Indicators for this process [8], [16], [17].

Table 16 - Key performance indicators for the process: Service Asset and Configuration Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Verification Frequency	7 days	84%
Verification Duration	3 days	78%
Effort for CMS Verifications	48h	90%
Automatic CMS Update	36h	68%
Number of CMS Errors	7	72%

Table 17 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Release and Deployment Management process. The final result shows the implementation of 84% recommendations of Key Performance Indicators for this process [8], [16], [17]. The best implemented Key Performance Indicator is Proportion of Automatic Release Distribution (91% of successful implemented KPI) and the least implemented Key Performance Indicator is Number of release backouts (78% of successful implemented Key Performance Indicators). The result of 84% shows that improvement for this process are possible.

Table 17 - Key performance indicators for the process: Release and Deployment Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Number of Releases	15	82%
Duration of Major Deployments	3 days	86%
Number of Release Backouts	10	78%
Proportion of Automatic Release Distribution	12h	91%

Table 18 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Service Validation and Testing process. The final result shows the implementation of 81% recommendations of Key Performance Indicators for this process [8], [16], [17].

Table 18 - Key performance indicators for the process: Service Validation and Testing

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Percentage of Failed Release Component Acceptance Tests	91%	84%
Number of Identified Errors	6	74%
Time for Error Fixing	12h	90%
Incidents Caused by New Releases	10	81%
Percentage of Failed Service Acceptance Tests	86%	75%

Table 19 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Change Evaluation process. The final result shows the implementation of 73% recommendations of KPIs for this process [8], [16], [17].

Table 19 - Key performance indicators for the process: Change Evaluation

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
The percentage of a new services which are released into production	80%	78%
The percentage of implemented changes which are released in the production	82%	68%
The average number of interactions with the Change Management process	30	75%
The average number of IT services that are immediately put into production	4	72%

Table 20 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Knowledge Management process. The final result shows the implementation of 84% recommendations of Key Performance Indicators for this process [8], [16], [17].

Table 20 - Key performance indicators for the process: Knowledge Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
The percentage of employees who finished the training	95%	87%
The average number of trainings during one year	15	84%
The percentage of time that is reduced in the maintenance of the system	92%	90%
The number of correct action in the maintenance of the system after the training	14	75%

Table 21 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Event Management process. The final result shows the implementation of 78% recommendations of Key Performance Indicators for this process [9], [16], [17].

Table 21 - Key performance indicators for the process: Event Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
The number and the percentage of events which are connected to incidents	400	78%
The number and the percentage of events which are connected to problems	30	81%
The number and the percentage of events which are connected to changes	20	79%
The number and the percentage of recurring events	12	74%
The number and the percentage of significant events for the performance	18	78%

Table 22 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Incident Management process. The final result shows the implementation of 67% recommendations of Key Performance Indicators for this process [9], [16], [17].

Table 22 - Key performance indicators for the process: Incident Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Number of Repeated Incidents	36	68%
Remotely Resolved Incidents	95%	72%
Number of Escalations	5	65%
Incident Resolution Time	3h	80%
First Time Resolution Rate	2h	58%
Resolution within SLA	2h	58%

Table 23 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Request Fulfillment process. The final result shows the implementation of 71% recommendations of Key Performance Indicators for this process [9], [16], [17].

Table 23 - Key performance indicators for the process: Request Fulfillment

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
The time resolution of requests for the service	6h	70%
Requests for services completed in accordance with the time	95%	68%
Cost of requests for the service	92%	75%
The percentage of satisfied users	90%	70%

Table 24 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Problem Management process. The final result shows the implementation of 69% recommendations of Key Performance Indicators for this process [9], [16], [17]. The best implemented Key Performance Indicator is Time until Problem identification (only 84% of successful implemented KPI) and the best implemented Key Performance Indicator is Number of incident per problem (55% of successful implemented Key Performance Indicator). The process is pretty bad implemented and the improvements are needed.

Table 24 - Key performance indicators for the process: Problem Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Problems	14	68%
Problem Resolution Time	24h	70%
Number of Incidents per Problem	7	69%
Number of Incidents per Known Problem	11	55%
Time until Problem Identification	6h	84%

Table 25 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Access Management process. The final result shows the implementation of 82% recommendations of Key Performance Indicators for this process [9], [16], [17].

Table 25 - Key performance indicators for the process: Access Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
The number of requests for the access	120	86%
The number of unsuccessful applications for a daily access	14	75%
The number of unsuccessful requests for access in one year	20	78%
The number of unsuccessful requests for access in one month	2	84%
The percentage of incidents which is caused by the wrong approach	92%	89%

Table 26 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Continual Service Improvement process. The final result shows the implementation of 85% recommendations of Key Performance Indicators for this process [10], [16], [17]. Key Performance Indicator which is the most implemented is Number of Identified Weaknesses (97%), and Key Performance Indicator: Number of completed improvement initiatives is least implemented (79%). Results for this process have shown and the phase of Continual Service Improvement is pretty good implemented in this system so improvements are needed in some other ITIL phases (especially in Service Operation phase).

Table 26 - Key performance indicators for the process: Continual Service Improvement Process

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Process Benchmarkings, Maturity Assessments, and Audits	12	82%
Number of Process Evaluations	30	84%
Number of Identified Weaknesses	50	97%
Number of Improvement Initiatives	25	84%
Number of Completed Improvement Initiatives	20	79%

6 Measurements of the implementation of Billing system by using key performance indicators for ISO/IEC 20000 standard

Table 27 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Capacity Management process. The final result shows the implementation of 88% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 27 - Key performance indicators for the process: Capacity Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Incidents due to Capacity Shortages	12	98%
Exactness of Capacity Forecast	95%	62%
Capacity Adjustments	95%	90%
Resolution Time of Capacity Shortage	12h	98%
Percentage of Capacity Monitoring	100%	94%

Table 28 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Service Continuity and Availability Management process. The final result shows the implementation of 93% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21]. The best implemented KPI is The percentage of IT services which is implemented in compliance with the availability and continuity plans (96% of successful implemented Key Performance Indicators).

Table 28 - Key performance indicators for the process: Service Continuity and Availability Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Availability of IT services	100%	98%
The number of service interruptions	15	95%
Duration of service interruption	6h	92%
Monitoring the availability of services	98%	97%
Measuring the availability of services	96%	88%
The number of business processes with continuity plan	18	91%
The percentage of service continuity plan which is implemented	96%	90%
The percentage of IT services which is implemented in compliance with the availability and continuity plans	99%	96%

Table 29 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Service Level Management process. The final result shows the implementation of 89% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 29 - Key performance indicators for the process: Service Level Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Services covered by SLAs	90%	86%
Services covered by OLAs	95%	88%
Monitored SLAs	90%	94%
SLAs under Review	90%	86%
Fulfilment of Service Levels	92%	90%
Number of Service Issues	95%	88%

Table 30 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Service Reporting process. The final result shows the implementation of 80% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 30 - Key performance indicators for the process: Service Reporting

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
The number of reports in one month	3	80%
The percentage of reports which are submitted properly	90%	84%
The percentage of satisfied managers	92%	78%
The percentage of documented processes	87%	79%

Table 31 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Information Security Management process. The final result shows the implementation of 89% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 31 - Key performance indicators for the process: Information Security Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Implemented Preventive Measures	12	92%
Implementation Duration	4 days	85%
Number of Major Security Incidents	8	78%
Number of Security Tests	6	84%
Number of Identified Shortcomings during Security Tests	10	98%
Number of Implemented Preventive Measures	8	95%

Table 32 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Budgeting and Accounting services process. The final result shows the implementation of 93% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21]. This result shows a good level of Budgeting and Accounting services process so that this process can be a replacement for some similar ITIL process. The least implemented KPI is The percentage of successfully implemented procurements (90%).

Table 32 - Key performance indicators for the process: Budgeting and Accounting services

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
The average annual income	350.000.000 E	94%
The average annual expenditure	610.000.000 E	92%
The average annual earnings	150.000.000 E	95%
The average annual investment	110.000.000 E	90%
The average daily consumption and earnings	500.000 E	96%
The percentage of Increasing the budget of the organization	95%	92%
The percentage of successfully implemented procurements	98%	90%

Table 33 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Business Relationship Management process. The final result shows the implementation of 87% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 33 - Key performance indicators for the process: Business Relationship Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
The average number of test users	2000	95%
The percentage of completed questionnaires	90%	84%
Percentage of satisfied users	85%	82%

Table 34 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Supplier Management process. The final result shows the implementation of 91% recommendations of KPIs for this ISO/IEC 20000 process [20], [21].

Table 34 - Key performance indicators for the process: Supplier Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implement ation
Number of Agreed Contracts	7	100%
Number of Contract Reviews	15	87%
Number of Identified Contract Breaches	10	86%

Table 35 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Incident and Service Request Management process. The final result shows the implementation of 90% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 35 - Key performance indicators for the process: Incident and Service Request Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Repeated Incidents	12	97%
Remotely Resolved Incidents	20	88%
Number of Escalations	15	91%
Incident Resolution Time	6h	88%
First Time Resolution Rate	2h	85%
Resolution within SLA	2h	90%
The time resolution of requests for the service	2h	88%
Requests for services completed in accordance with the time	95%	93%
Cost of requests for the service	95%	88%
The percentage of satisfied users	95%	90%

Table 36 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Problem Management process. The final result shows the implementation of 88% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 36 - Key performance indicators for the process: Problem Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Problems	15	87%
Problem Resolution Time	24h	85%
Number of Incidents per Problem	8	92%
Number of Incidents per Known Problem	8	90%
Time until Problem Identification	12h	86%

Table 37 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Problem Management process. The final result shows the implementation of 82% recommendations of Key

Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 37 - Key performance indicators for the process: Configuration Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Coverage of system configuration management	90%	87%
Automatic change of system configuration management	92%	85%
Number of errors in system configuration management during the period of one month	8	75%
Number of errors in the system for configuration management during the period of one year	35	82%
Number of units in the configuration of IT service	12	85%
Reduced number of incidents	95%	80%

Table 38 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Change Management process. The final result shows the implementation of 80% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21].

Table 38 - Key performance indicators for the process: Change Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Major Changes	7	87%
Time for Change Clearance	12h	82%
Change Acceptance Rate	92%	84%
Number of Urgent Changes	3	67%

Table 39 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for Release and Deployment Management process. The final result shows the implementation of 86% recommendations of Key Performance Indicators for this ISO/IEC 20000 process [20], [21]. The least implemented Key Performance Indicator is Number of reelase backouts (78% of successful implemented KPI for this recommendation).

Table 39 - Key performance indicators for the process: Release and Deployment Management

Key Performance Indicator (KPI)	Critical Success Factor (CSF)	Result of the KPI implementation
Number of Releases	15	84%
Duration of Major Deployments	5 days	90%
Number of Release Backouts	12	78%
Proportion of Automatic Release Distribution	18h	90%

7 Comparison between the implementation of ITIL framework and ISO/IEC 20000 standard

Table 40 shows the list of complementary processes of the ITIL framework in ISO/IEC 20000 standard. The list of these complementary processes is shown in book [4], in which are described differences between ITIL framework and ISO/EC 20000 standard. As we can see from this table, 14 ITIL processes has complementary processes in ISO/IEC 20000 standard. Processes from all 5 ITIL phases are placed in this table [20].

Table 40 - Complementary processes of the ITIL framework in ISO/IEC 20000 standard

ITIL process	Complementary process in ISO/IEC 20000 standard
Capacity Management	Capacity Management
IT Service Continuity Management	Service Continuity and Availability Management
Availability Management	Service Continuity and Availability Management
Service Level Management	Service Level Management
Information Security Management	Information Security Management
Financial Management for IT services	Budgeting and Accounting services
Business Relationship Management	Business Relationship Management
Supplier Management	Supplier Management
Incident Management	Incident and Service Request Management
Request Fulfillment	Incident and Service Request Management
Problem Management	Problem Management
Service Asset and Configuration Management	Configuration Management
Change Management	Change Management
Release and deployment Management	Release and deployment Management

Measurements from section 4. show that only 6 processes are implemented with the percentage of KPI implementation smaller than 75%. These processes are: Financial Management for IT services (total KPI implementation: 70%), Service Portfolio Management (total KPI implementation: 65%), Change Evaluation (total KPI implementation: 73%), Incident Management (total KPI implementation: 67%), Request Fulfillment (total KPI implementation: 71%) and Problem Management (total KPI implementation: 69%). Table 41. shows complementary ISO/IEC 20000 processes for all these ITIL processes. Only Service Portfolio Management and Change Evaluation don't have complementary ISO/IEC 20000 processes. For other 4 processes (Financial Management for IT services, Incident Management, Request Fulfillment and Problem Management), we will do the same measurements as in section IV, only now we will use a set of new Key Performance Indicators. Incident Management and Request Fulfillment will be treated as the same process Incident and Service Request Management [4], [20].

Table 41 - Replacement of ITIL processes which have achieved poor results with complementary processes from ISO/IEC 20000 standard

ITIL process	**Complementary process in ISO/IEC 20000 standard**
Financial Management for IT services	Budgeting and Accounting services
Service Portfolio Management	No process
Change Evaluation	No process
Incident Management	Incident and Service Request Management
Request Fulfillment	Incident and Service Request Management
Problem Management	Problem Management

Table 42 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for a new process: Budgeting and Accounting services. The final result shows the implementation of 84% recommendations of KPIs for this process [20].

Table 42 - Key performance indicators for the process: Budgeting and Accounting services

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
The average annual income	350.000.000 E	80%
The average annual expenditure	610.000.000 E	84%
The average annual earnings	150.000.000 E	86%
The average annual investment	110.000.000 E	85%
The average daily consumption and earnings	500.000 E	82%
The percentage of Increasing the budget of the organization	95%	86%
The percentage of successfully implemented procurements	98%	84%

Table 43 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for a new process: Incident and Service Request Management. The final result shows the implementation of 84% recommendations of Key Performance Indicators for this process [20].

Table 43 - Key performance indicators for the process: Incident and Service Request Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Number of Repeated Incidents	12	88%
Remotely Resolved Incidents	20	82%
Number of Escalations	15	86%
Incident Resolution Time	6h	82%
First Time Resolution Rate	2h	79%
Resolution within SLA	2h	82%
The time resolution of requests for the service	2h	90%
Requests for services completed in accordance with the time	95%	85%
Cost of requests for the service	95%	79%
The percentage of satisfied users	95%	83%

Table 44 shows Key Performance Indicators (KPIs) and results of the KPIs implementation in the test environment of Billing System for a new Problem Management process. The final result shows the implementation of 79% recommendations of Key Performance Indicators for this process [20]. The best implemented Key Performance Indicator is Problem Resolution time (81%) and the least implemented Key Performance Indicator is Time until Problem identification (74%).

Table 44 - Key performance indicators for the process: Problem Management

Key Performance Indicator (KPI)	**Critical Success Factor (CSF)**	**Result of the KPI implementation**
Number of Problems	15	79%
Problem Resolution Time	24h	81%
Number of Incidents per Problem	8	80%
Number of Incidents per Known Problem	8	80%
Time until Problem Identification	12h	74%

8 Conclusion

All these three measurements which are described in chapter VII have achieved good results according to paper [15]. Based on this, we propose a new model for ITIL 2011 framework which contains all these three processes. Changes are only present in two ITIL phases: Service Strategy and Service Operation. Processes that are placed in Service Strategy phase are now: Strategy Management for IT services, Budgeting and Accounting Services (a new process), Demand Management, Service Portfolio Management and Business Relationship Management. Processes that are placed now in Service Operation phase are: Event Management, Incident and Service Request Management (a new process), Problem Management (a new process with a new set ok Key Performance Indicators) and Access Management. A new proposed model for ITIL framework contains now 25 process (one process less than actual ITIL framework). In this new model of ITIL framework, only two processes are implemented with a less than 75% of Key Performance Indicators in the implementation of Billing system for dual play, triple play and quad play services of Telecom operator. Figure 5. shows a new model for ITIL framework.

Future research of authors in this area is connected to the improvement of ITIL framework based on comparison with other ITSM frameworks: PRINCE2 and CobiT and ITSM standards: eTOM, ISO/IEC 27001 and ISO/IEC 27002. This project is working on University of Sarajevo, on Faculty of Electrical Engineering in test environment of IPTV/VoIP service. The aim is to create a new model of ITIL framework which should contain a set of parameters from all other ITSM frameworks and standards. The aim of this model is also to increase the level of implementation of Key Performance Indicators in two rest ITIL processes which don’t have complementary processes in ISO/IEC 20000 [20]: Service Portfolio Management and Change Evaluation.

Acknowledgment

The authors wish to thank experts from 2 Telecom Operators from Bosnia and Herzegovina (BH Telecom and HT Eronet) for the realisation of this project. The authors wish also to thank the colleagues from University of Sarajevo (Faculty of Electrical Engineering) for advices in the realisation of this paper.

References:

[1] Van Haren Publishing, *Implementing ISO/IEC 20000 Certification – The Roadmap (ITSM Library)*, February 2008.

[2] J. Dugmore and S. Lacy, *The Differences Between BS 15000 and ISO/IEC 20000*, The Institution of Engineering and Technology, January 2007.

[3] L. Cooper, *A Guide to the New ISO/IEC 20000-1: The Differences Between the 2005 and the 2011 Editions*, BSI British Standards Institution, June 2011.

[4] Van Haren Publishing, *Implementing IT Service Management Aligning with ITIL and ISO/IEC 20000*, June 2011.

[5] M. Kunas, *Implementing Service Quality based on ISO/IEC 20000*, IT Governance Publishing, May 2011.

[6] S. Taylor, M. Iqbal, and M. Nieves, *ITIL Version 3 Service Strategy*, The Office of Government Commerce, July 2011.

[7] S. Taylor, V. Lloyd, and C. Rudd, *ITIL Version 3 Service Design*, The Office of Government Commerce, July 2011.

[8] S. Taylor, S. Lacy, and I. Macfarlane, *ITIL Version 3 Service Transition*, The Office of Government Commerce, July 2011.

[9] S. Taylor, D. Cannon, and D. Wheeldon, *ITIL Version 3 Service Operation*, The Office of Government Commerce, July 2011.

[10] S. Taylor, G.Case, and G.Spalding, *ITIL Version 3 Continual Service Improvement*, The Office of Government Commerce, July 2011.

[11] R. Martinez, D. Torres, M. Madrigal, and L. Guardado, Digital Domestic Meter for the Measurement and Billing of Electricity in Mexico, *11th WSEAS International Conference on Circuits (CSCC’07)*, pp. 1-6, July 2007.

[12] Dz. Dzonko and I. Traljic, Continual Service Improvement Using Balanced Scorecard, *8th International Conference on Telecommunications and Informatics (TELE-INFO ‘09)*, pp. 157-162, June 2009.

[13] C. Zhao, H. Gan, and F. Gao, A Study on the Process Model for IT Service Management, *3rd International Conference on Computer Engineering and Applications (CEA ‘09)*, pp. 206-210, January 2009.

[14] M. Jansen, What does it Service Management look like in the cloud ? – An ITIL based approach, *International WSEAS Journal: Recent Advances in Computers, Communications, Applied Social Science and Mathematics*, pp. 87-92, September 2011.

[15] A. Tanovic and F. Orucevic, Comparative Analysis of the Practice of Telecom Operators in the Realization of IPTV Systems Based on ITIL V3 Reccomendations for the Supplier Management Process, *IEEE International Conference on Service-Oriented Computing and Applications (SOCA),* pp. 1-8, December 2010.

[16] A. Tanovic, I. Androulidakis, and F. Orucevic, Design and implementation of the IP Multimedia Subsystem by using ITIL V3 recommendations, *11th WSEAS International Conference on Applications of Computer Engineering (ACE'12),* pp. 39-48, March 2012.

[17] A. Tanovic, I. Androulidakis, and F. Orucevic, Advantages of the new ITIL V3 model in the implementation of the IMS system, *11th WSEAS International Conference on Applications of Computer Engineering (ACE'12),* pp. 183-191, March 2012.

[18] A. Tanovic, I. Androulidakis and F. Orucevic, Results of the implementation of IP Multimedia Subsystem in one Telecom operator for the ITIL Incident Management and Problem Management process, paper accepted for *WSEAS Journal of Computers and Communications*, April 2012.

[19] A. Tanovic, I. Androulidakis, and F. Orucevic, Differences in results of measurement of ITIL 2007 and ITIL 2011 model for the IMS system, paper accepted for *WSEAS Journal of Computers and Communications*, April 2012.

[20] M. Brenner, T. Schaaf, and A. Scherer, Towards an information model for ITIL and ISO/IEC 20000 processes, *International Symposium on Integrated Network Management (IM'09),* pp. 113-116, June 2009.

[21] A. Nance, D. Underwood, K.S. Franklin, G. Malkani and M. Talukder, Essential ISO/IEC 20000 Managers' Executive's Guide, *ITpreneurs Nederland B.V.,* November 2007.

[22] S. Sahibudin, M. Sharifi, and M. Ayat, Combining ITIL, CobiT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations, *2nd Asia International Conference on Modeling & Simulation (AICMS 2008),* pp. 749-753, May 2008.

[23] R.F. de Sousa Pereira and M.M. da Silva, A Maturity Model for Implementing ITIL v3, *6th World Congress on Services (SERVICES-1),* pp. 399-406, July 2010.

[24] H.B. Esmaili, H. Gardesh, and S.S. Sikari, Validating ITIL maturity to strategic business-IT alignment, *2nd International Conference on Computer Technology and Development (ICCDT),* pp. 556-561, November 2010.

[25] Zhao, H. Gan and F. Gao, A Study on the Process Model for IT Service Management, *3rd WSEAS International Conference on Computer Engineering and Applications (CEA '09),* pp. 206-210, January 2009.

[26] S. Simonova and I. Zavadilova, Usage of business process tools for modelling requirements on system changes, *WSEAS International Conference on Development, Energy, Environment, Economics (DEEE'10),* pp. 321-326, November 2010.

[27] M. Jansen, What does it Service Management look like in the cloud, *WSEAS International Conference on Computers, digital communications and computing (ICDCC'11)* , pp. 87-92, September 2011.

[28] Z. Balantic, Spiral Model Development Concept of Multimedia Application, *10th WSEAS International Conference on Computers*, pp. 317-320, July 2006.

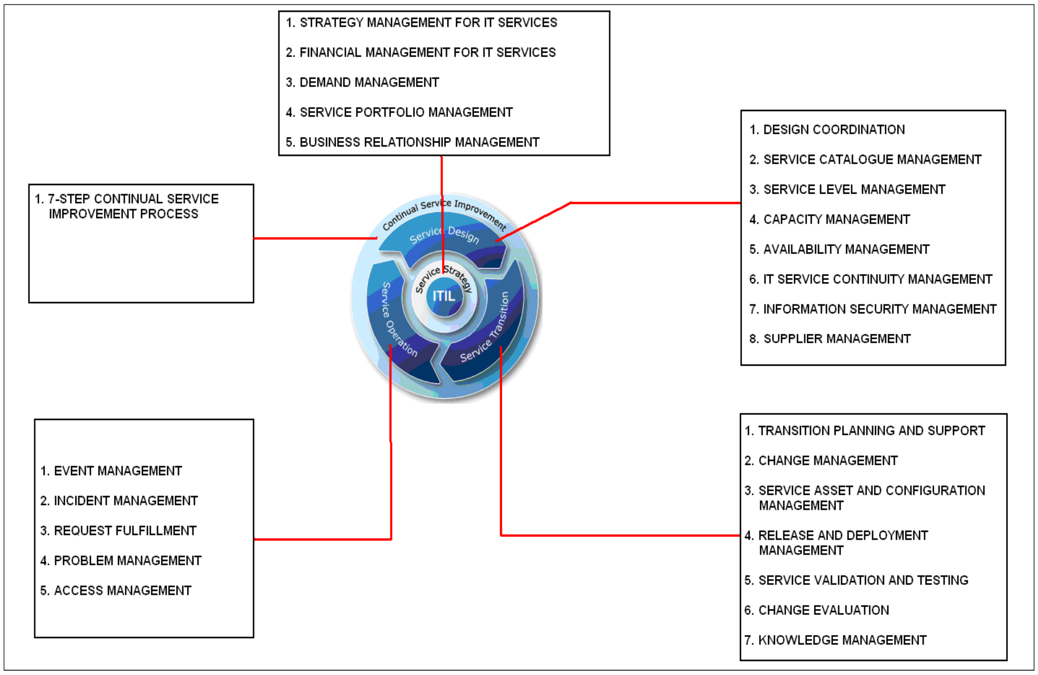

1. STRATEGY MANAGEMENT FOR IT SERVICES
2. FINANCIAL MANAGEMENT FOR IT SERVICES
3. DEMAND MANAGEMENT
4. SERVICE PORTFOLIO MANAGEMENT
5. BUSINESS RELATIONSHIP MANAGEMENT
1. 7-STEP CONTINUAL SERVICE IMPROVEMENT PROCESS
Continual Service Improvement
Service Design
Service Strategy
ITIL
Service Operation
Service Transition
1. DESIGN COORDINATION
2. SERVICE CATALOGUE MANAGEMENT
3. SERVICE LEVEL MANAGEMENT
4. CAPACITY MANAGEMENT
5. AVAILABILITY MANAGEMENT
6. IT SERVICE CONTINUITY MANAGEMENT
7. INFORMATION SECURITY MANAGEMENT
8. SUPPLIER MANAGEMENT
1. EVENT MANAGEMENT
2. INCIDENT MANAGEMENT
3. REQUEST FULFILLMENT
4. PROBLEM MANAGEMENT
5. ACCESS MANAGEMENT
1. TRANSITION PLANNING AND SUPPORT
2. CHANGE MANAGEMENT
3. SERVICE ASSET AND CONFIGURATION MANAGEMENT
4. RELEASE AND DEPLOYMENT MANAGEMENT
5. SERVICE VALIDATION AND TESTING
6. CHANGE EVALUATION
7. KNOWLEDGE MANAGEMENT

Fig. 1 - ITIL Framework

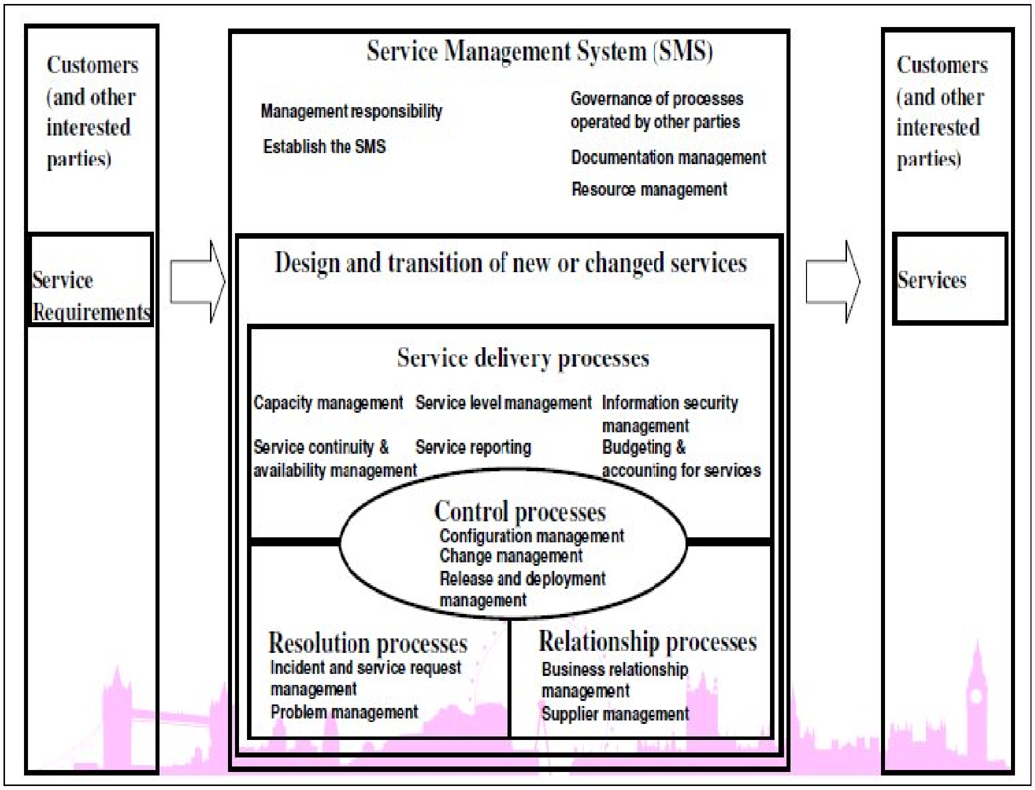

Customers (and other interested parties)
Service Requirements
Service Management System (SMS)
Management responsibility
Establish the SMS
Governance of processes operated by other parties
Documentation management
Resource management
Design and transition of new or changed services
Service delivery processes
Capacity management
Service level management
Information security management
Service continuity & availability management
Service reporting
Budgeting & accounting for services
Control processes
Configuration management
Change management
Release and deployment management
Resolution processes
Incident and service request management
Problem management
Relationship processes
Business relationship management
Supplier management
Customers (and other interested parties)
Services

Fig. 2 - ISO/IEC 20000 standard

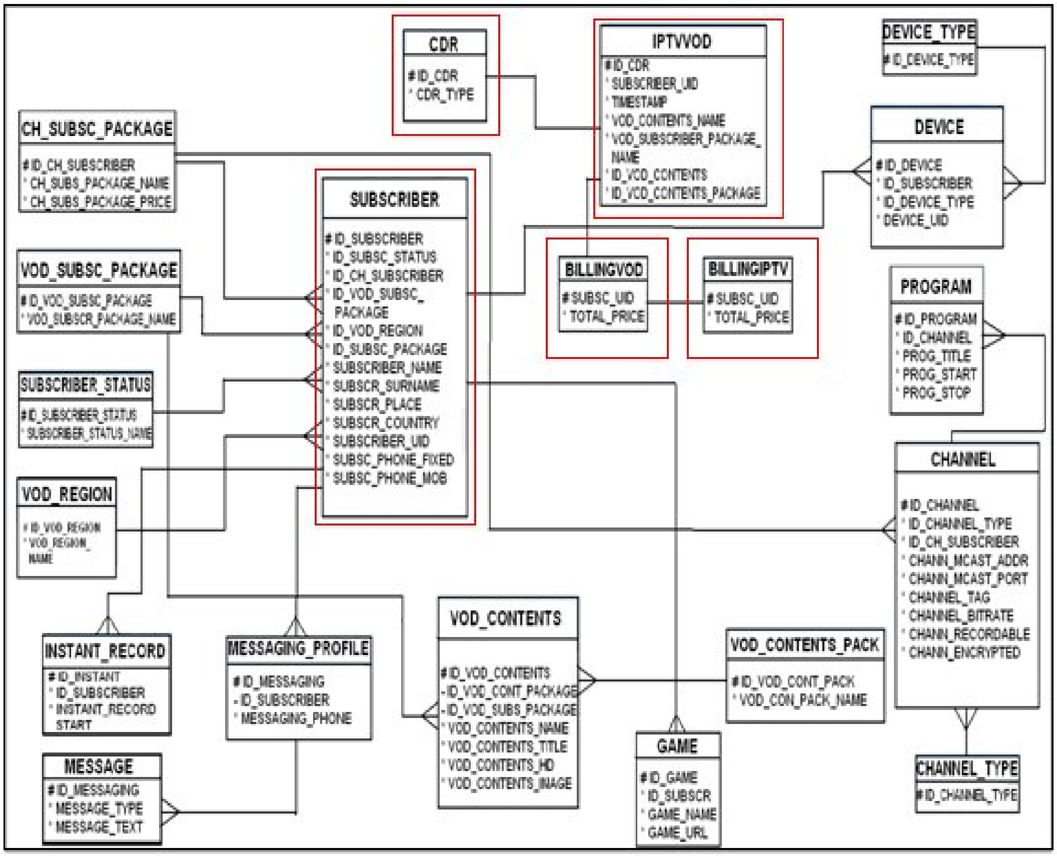


Fig. 4 - Entity Relationship Diagram for Billing system

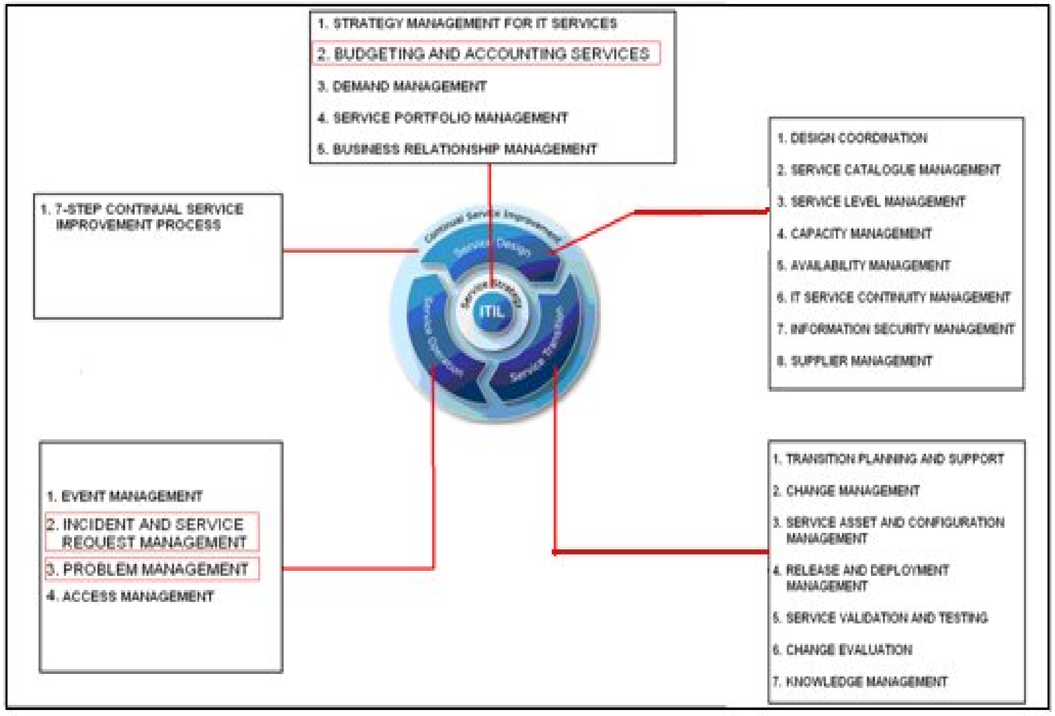

1. STRATEGY MANAGEMENT FOR IT SERVICES
2. BUDGETING AND ACCOUNTING SERVICES
3. DEMAND MANAGEMENT
4. SERVICE PORTFOLIO MANAGEMENT
5. BUSINESS RELATIONSHIP MANAGEMENT
1. 7-STEP CONTINUAL SERVICE IMPROVEMENT PROCESS
Continual Service Improvement
Service Design
Service Strategy
ITIL
Service Operation
Service Transition
1. DESIGN COORDINATION
2. SERVICE CATALOGUE MANAGEMENT
3. SERVICE LEVEL MANAGEMENT
4. CAPACITY MANAGEMENT
5. AVAILABILITY MANAGEMENT
6. IT SERVICE CONTINUITY MANAGEMENT
7. INFORMATION SECURITY MANAGEMENT
8. SUPPLIER MANAGEMENT
1. EVENT MANAGEMENT
2. INCIDENT AND SERVICE REQUEST MANAGEMENT
3. PROBLEM MANAGEMENT
4. ACCESS MANAGEMENT
1. TRANSITION PLANNING AND SUPPORT
2. CHANGE MANAGEMENT
3. SERVICE ASSET AND CONFIGURATION MANAGEMENT
4. RELEASE AND DEPLOYMENT MANAGEMENT
5. SERVICE VALIDATION AND TESTING
6. CHANGE EVALUATION
7. KNOWLEDGE MANAGEMENT

Fig. 5 - New model for ITIL framework

Unidirectional Chaotic Synchronization of Rossler Circuit and Its Application for Secure Communication

ACENG SAMBAS[1], MADA SANJAYA WS[2], HALIMATUSSADIYAH
Department of Physics, Faculty of Science and Technology
Universitas Islam Negeri Sunan Gunung Djati, Bandung
Bolabot Techno Robotic School, Sanjaya Star Group, Bandung
Jl. A.H. Nasution No. 105, Bandung
INDONESIA
acenx.bts@gmail.com[1] madasws@gmail.com[2] http://www.bolabot.com

Abstract: - Synchronization is considered as the complete coincidence of the states of individual systems. Such a regime can result from an interaction between systems or subsystems, as well as from the influence of external noisy or regular fields. In this paper, we have performed the design and numerical simulation of the synchronization between two identical coupled Rossler circuits and applied to a security system of communication. We have demonstrated in simulations that chaotic systems can be synchronized and this technique can be applied to signal masking communications by using MATLAB and MultiSIM programs. All simulations results performed on Rossler system, verify the applicable of secure communication

Key-Words: - Chaos, Chaotic synchronization, Unidirectional coupling, Rossler circuit, Secure communication, Numerical simulation.

1 Introduction

Chaotic behaviour has been found in many typical iterated maps such as the logistic map [1] and Henon map etc[2]. In various electronic circuit systems, including the Duffing oscillator [3], Double-Bell circuit [4] and hyper chaotic Rossler system [5]. Chaos has been widely applied to many scientific disciplines: biology [6], ecology [7], financial markets [8], psychology [9] and robotics [10].

One of the pioneers of synchronization is probably the Dutch scientist Christiaan Huygens. In the 17th century he described an observation of two pendulum clocks, both attached to the same beam that was supported by two chairs, that always end up swinging in opposite direction independent of their starting positions, Even when he applied a disturbance the two clocks showed *anti-phase* synchronized motion within half an hour [11-12].

Besides synchronization of pendulum clocks, a vast number of examples of synchronization of coupled oscillators can be found in nature, especially amongst living animals. Great examples are the simultaneous chirping of crickets and the synchronous flashing of fireflies on banks of rivers in Malaysia, Thailand and New Guinea. With this flashing in unison male fireflies try to attract female species on the other side of the river. Synchronization does also occur in brain dynamics where individual neurons are firing their action potentials at the same time [11].

Synchronization of chaotic oscillators in particular became popular when Pecora and Carroll published their observations of synchronization in unidirectionally coupled chaotic systems [13]. Their results were remarkable since chaos can be seen as a form of instability while synchronization implies stability of the error dynamics [12]. The research in synchronization of couple chaotic circuits is carried out intensively and some interesting applications such as cryptography, communications with chaos have come out of that research [14].

In this paper, a simple electronic system of two coupled circuits in the development scheme of chaos-based secure communication system has been used. First, we examine separately each oscillator circuit to study the dynamic behaviour when varying one parameter, which it has been done before. Furthermore, the unidirectional coupling method is applied to synchronize Rossler circuit. Finally, chaotic masking communication circuits and their simulations of the Rossler circuit are realized also MATLAB and MultiSIM.

2 Mathematical Model of Chaotic Rossler Circuit

One of the most well-known autonomous nonlinear systems [15-18]. The one nonlinearity in the circuit is a piecewise linear function made from op amp U4A with diode, 3 resistors and a diode.

The Rossler electronic circuits are describe by the following equations [15]:

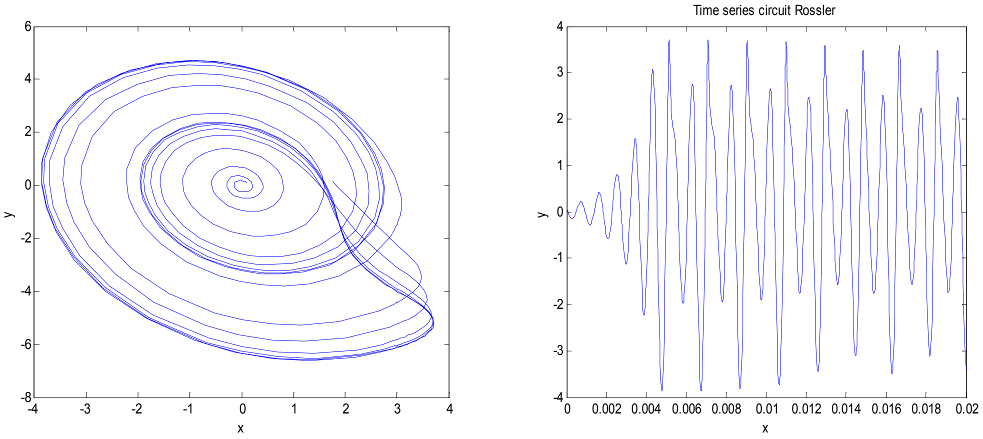
$$\left.\begin{aligned} \frac{dx}{dt} &= -\alpha(\Gamma x + \beta y + \lambda z) \\ \frac{dy}{dt} &= -\alpha(-x - \gamma y + 0.02z) \\ \frac{dz}{dt} &= -\alpha(-g(x) + z) \end{aligned}\right\} \qquad (1)$$

The piecewise linear function $g(x)$is defined by:

$$g(x) = \begin{Bmatrix} 0 & x \leq 3 \\ \mu(x-3) & x > 3 \end{Bmatrix} \qquad (2)$$

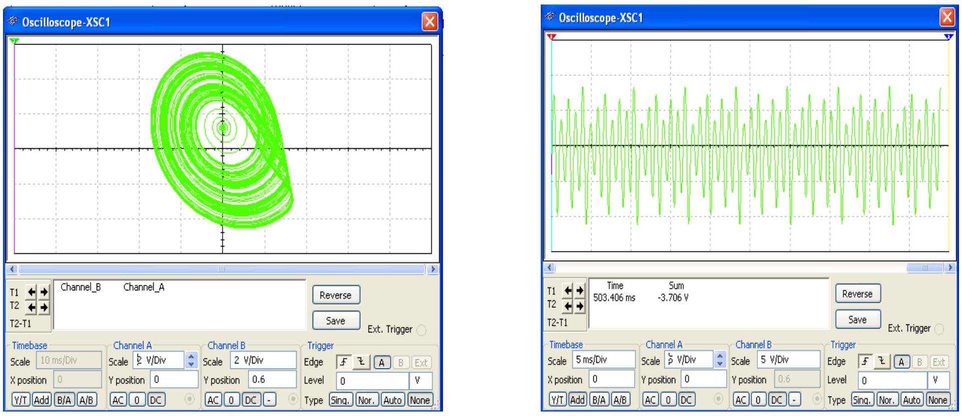
Where time factor α is $10^4\ s^{-1}$, Γ is 0.05, β is 0.5, λ is 1, μ is 15 and the circuit contains a variable resistor that can be used to change the value of γ. The relation between the value R_0 of the variable resistor and γ is R/R_0, with R=10kΩ. R_0=R_6 is a control parameter which exhibit bifurcation and chaotic dynamics.

The complete implementation of the Rossler chaotic circuit design using MultiSIM software is shown in Fig. 3. The function of nonlinear resistor as see in Fig. 3, are implemented with the analog operational amplifier. By comparing Fig. 1, and Fig. 2 a good qualitative agreement between the numerical integration of (1) and (2) by using MATLAB, and the circuits simulation by using MultiSIM, can be concluded.



(a) Phase Portrait of y versus x (b) Time-series of signal y

Fig.1 Numerical simulation results for Rc = 50 kΩ, with MATLAB



Channel_B Channel_A

Timebase: Scale 10 ms/Div; X position 0
Channel A: Scale 5 V/Div; Y position 0
Channel B: Scale 2 V/Div; Y position 0.6
Trigger: Edge A; Level 0 V

Time 503.406 ms Sum -3.706 V

Timebase: Scale 5 ms/Div; X position 0
Channel A: Scale 5 V/Div; Y position 0
Channel B: Scale 5 V/Div; Y position 0.6
Trigger: Edge A; Level 0 V

(a) Phase Portrait of y versus x (b) Time-series of signal y

Fig.2 Numerical simulation results for Rc = 50 kΩ, with MultiSIM

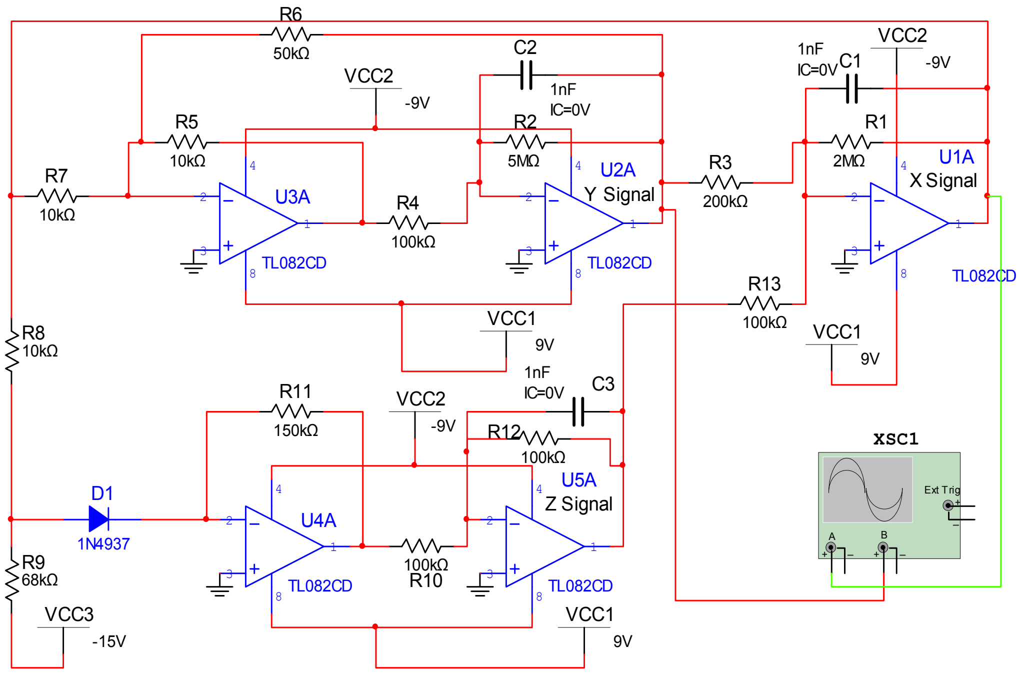


Fig. 3. Schematic of the proposed Rossler circuit

3 Unidirectional Chaotic Synchronization and Circuit's Analysis

There are two main forms of coupling. In the case of unidirectional or Master-Slave scheme, the master is the guide or reference system and the slave is driven system which is dependent on the master. In the case of bidirectional coupling two systems interact and are coupled with each other creating a mutual synchronization.

In this work, the overall system consists of two subsystems coupled by a configuration master-slave type. This implies that the slave system behaviour depends on the behaviour of the master, while the latter is not influenced by the behaviour of the slave system. As a result, the slave system is forced to follow the dynamics (or a specific function of the dynamics) of the master. In other words, when evolution of one of the two systems is not altered by coupling the resulting configuration is a unidirectional coupling.

Based on systems (3) and (4), a master systems in function of (x_1,y_1,z_1) and a slave systems in function of (x_2,y_2,z_2), can be designed. The slave systems, once it is coupled, it will be in function of (x_2, y_2, z_2, x_1). The state equations that describe the systems master and slave, both of them coupled, are

$$\left.\begin{aligned}
&\textit{Master}\\
&\frac{dx_1}{dt} = -\alpha\,(\Gamma x_1 + \beta y_1 + \lambda z_1)\\
&\frac{dy_1}{dt} = -\alpha\,(-x_1 - \gamma y_1 + 0.02\,z_1)\\
&\frac{dz_1}{dt} = -\alpha\,(-g(x_1) + z_1)\\
&g(x_1) = \begin{cases} 0 & x_1 \le 3 \\ \mu(x_1-3) & x_1 > 3 \end{cases}
\end{aligned}\right\} \tag{3}$$

$$\left.\begin{aligned}
&\textit{Slave}\\
&\frac{dx_2}{dt} = -\alpha(\Gamma x_2 + \beta y_2 + \lambda z_2) + g_c(x_1 - x_2)\\
&\frac{dy_2}{dt} = -\alpha(-x_2 - \gamma y_2 + 0.02 z_2)\\
&\frac{dz_2}{dt} = -\alpha(-g(x_2) + z_2)\\
&g(x_2) = \begin{cases} 0 & x_2 \le 3 \\ \mu(x_2-3) & x_2 > 3 \end{cases}
\end{aligned}\right\} \tag{4}$$

where $g_c = 1/Rc.C$ is the coupling strength , $Rc = R_1$ is the variable resistor and C is Capacitance in x signal , (Fig. 5). The asymptotic synchronized situation is defined as:

$$\lim_{t\to\infty} |x_1(t) - x_2(t)| = 0$$

The dynamic error system is defined as follows:

$$\left.\begin{aligned} e_x &= x_1 - x_2 \\ e_y &= y_1 - y_2 \\ e_z &= z_1 - z_2 \end{aligned}\right\} \qquad (5)$$

The time derivative of this error signal is

$$\left.\begin{aligned} \dot{e}_x &= \dot{x}_1 - \dot{x}_2 \\ \dot{e}_y &= \dot{y}_1 - \dot{y}_2 \\ \dot{e}_z &= \dot{z}_1 - \dot{z}_2 \end{aligned}\right\} \qquad (6)$$

By substituting (3) and (4) into (6), we have the following error dynamics:

$$\begin{aligned} \dot{e}_x &= -\alpha(\Gamma x_1 + \beta y_1 + \lambda z_1) - (-\alpha(\Gamma x_2 + \beta y_2 + \lambda z_2)) + g_c(x_1 - x_2) \\ &= -\alpha\Gamma x_1 - \alpha\beta y_1 - \alpha\lambda z_1 + \alpha\Gamma x_2 + \alpha\beta y_2 + \alpha\lambda z_2)) + g_c(x_1 - x_2) \\ &= -\alpha\Gamma(x_1 - x_2) - \alpha\beta(y_1 - y_2) - \alpha\lambda(z_1 - z_2) + g_c(x_1 - x_2) \\ &= (-\alpha\Gamma + g_c)e_x - \alpha\beta e_y - \alpha\lambda e_z \qquad (7) \\ \dot{e}_y &= -\alpha(-x_1 - \gamma y_1 + 0.02 z_1) - (-\alpha(-x_2 - \gamma y_2 + 0.02 z_2)) \\ &= \alpha x_1 + \alpha\gamma y_1 - \alpha 0.02 z_1 - \alpha x_2 - \alpha\gamma y_2 + \alpha 0.02 z_2 \\ &= \alpha e_x + \alpha\gamma e_y - \alpha 0.02 e_z \\ \dot{e}_z &= -\alpha(-g(x_1) + z_1) - (-\alpha(-g(x_2) + z_2)) \\ &= \alpha g(x_1) - \alpha z_1 - \alpha g(x_2) + \alpha z_2)) \\ &= -\alpha e_z + \alpha e_g \end{aligned}$$

Where $e_g = g(x_1) - g(x_2)$

With the objective to demonstrate synchronization, we analyze the stability of dynamic error system. Thus, we propose the following candidate function to Lyapunov function

$$V = \frac{1}{2}(e_x{}^2 + e_y{}^2 + e_z{}^2) \qquad (8)$$

Derive equation (8), is obtained:

$$\begin{aligned} \dot{V} &= e_x\dot{e}_x + e_y\dot{e}_y + e_z\dot{e}_z) \\ &= (-\alpha\Gamma + g_c)e_x - \alpha\beta e_y - \alpha\lambda e_z)e_x \\ &\quad + (\alpha e_x + \alpha\gamma e_y - \alpha 0.02 e_z)e_y \\ &\quad (-\alpha e_z + \alpha e_g)e_z \end{aligned}$$

$$\dot{V} = \begin{bmatrix} e_x \\ e_y \\ e_z \end{bmatrix}^T \begin{bmatrix} \alpha\Gamma - g_c & \alpha\beta & \alpha\lambda \\ -\alpha & -\alpha\gamma & 0.02\alpha \\ -\alpha\mu & 0 & \alpha \end{bmatrix} \begin{bmatrix} e_x \\ e_y \\ e_z \end{bmatrix}$$

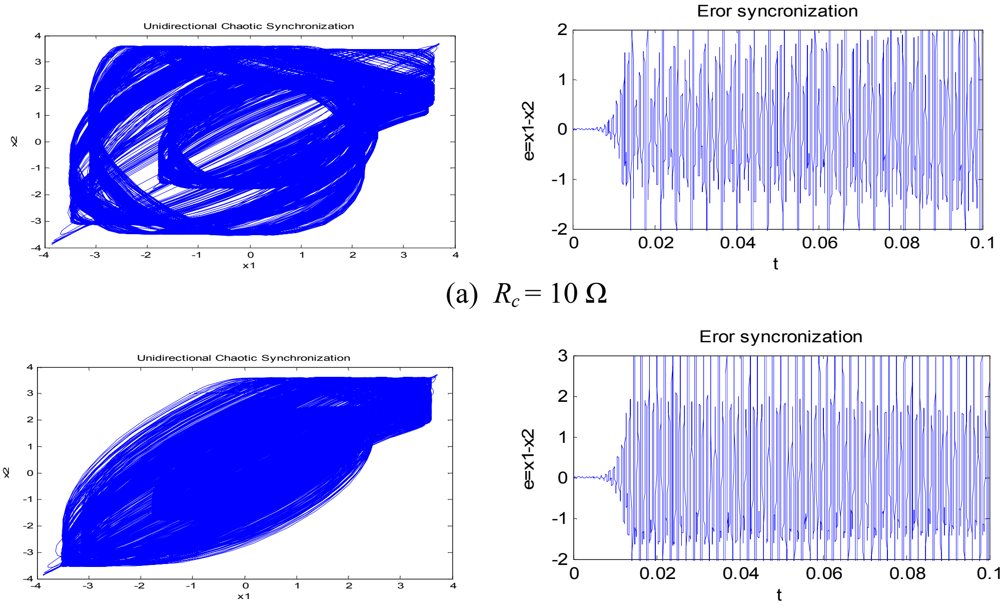
$$\dot{V} = -e^T A e < 0$$

Which is a negative definite function. It means that the dynamic error system (7) is asymptotically stable and, therefore, each one of synchronization errors, e_x, e_y and e_z, tends to zero as t tends to infinite. If synchronization errors tends to zero, then the states from slave system tend to those from master system, which means that they synchronize.

4 Numerical Simulations

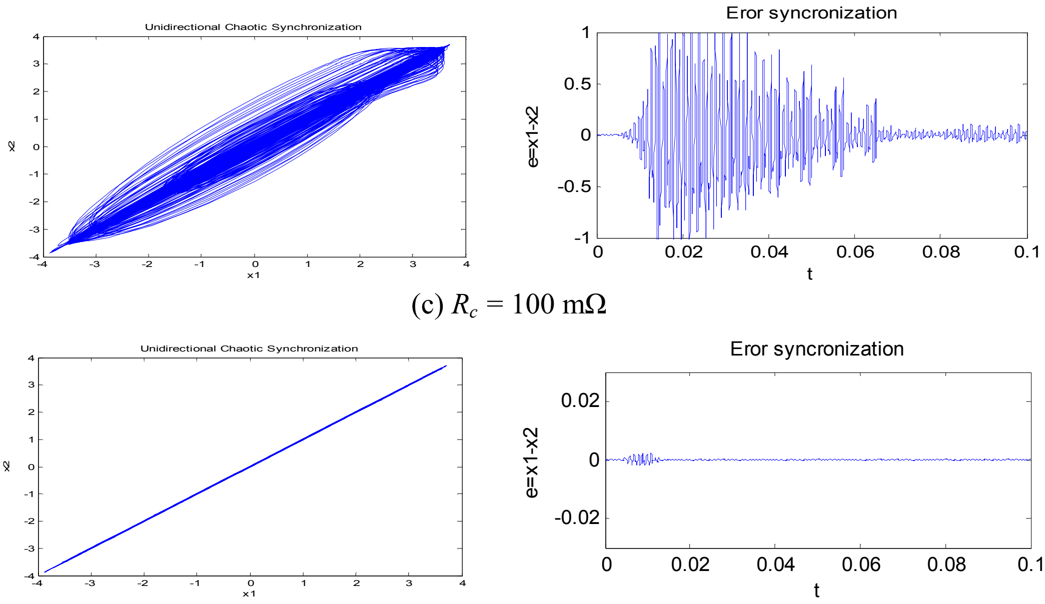
4.1 Simulation in MATLAB

First synchronization between identical systems is considered. We consider coupling through $g_c = 1/R_c$.C It can be seen in Fig. 4. That synchronization occurs if R_c does not exceed 10 mΩ.



(a) $R_c = 10\ \Omega$

(b) $R_c = 1\ \Omega$



(c) R_c = 100 mΩ

(d) R_c =10 mΩ

Fig. 4. Numerical results of unidirectional coupling, with MATLAB

Synchronization numerically appears for a coupling strength $R_c \leq$ 10 mΩ as shown in Fig. 4(d). For different initial condition, if the resistance coupling strength R_c >10 mΩ, the synchronization cannot occur as shown in Fig. 4 (a)-(c). The synchronization occurs when $R_c \leq$ 10 mΩ with errors $e_x = x_1 - x_2 \rightarrow 0$ which implies the complete synchronization for this resistance coupling strength as shown in Fig. 4 (d).

4.2 Analog Circuit Simulation in MultiSIM

Simulation results show that the two systems synchronize well. Fig. 5 shows the circuit schematic for implementing the unidirectional synchronization of coupled Rossler systems. We use 741 op-amps, appropriate valued resistors, one diode and capacitors for MultiSIM simulations. Fig. 6 also shows MultiSIM simulation results of this circuit.

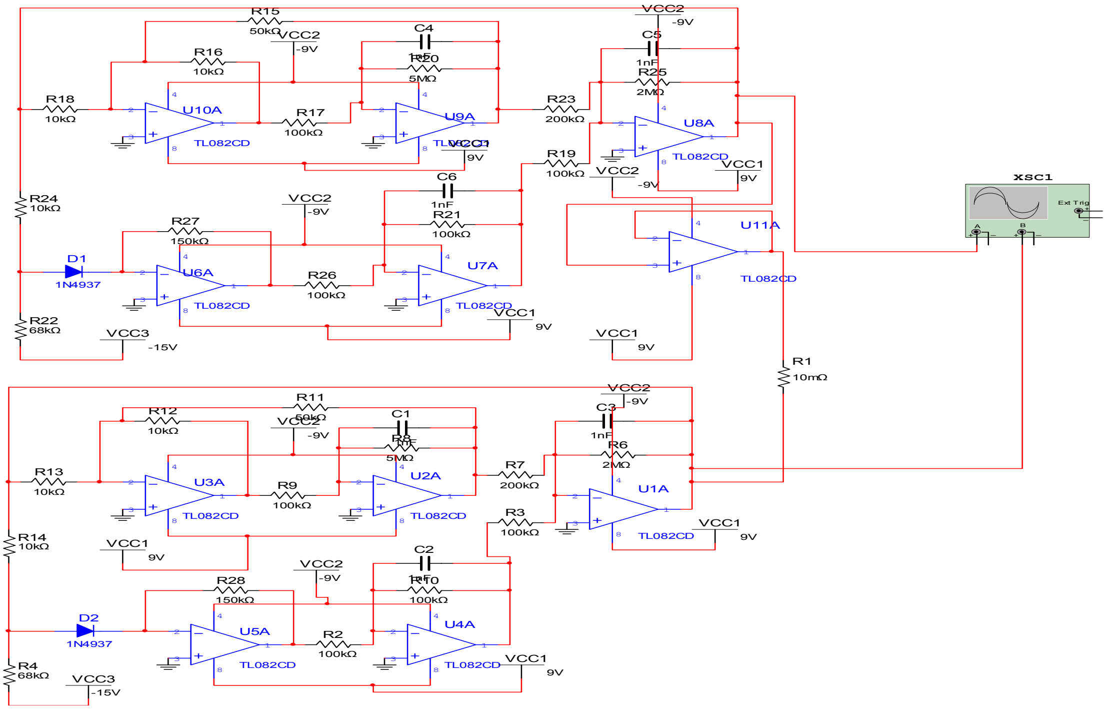
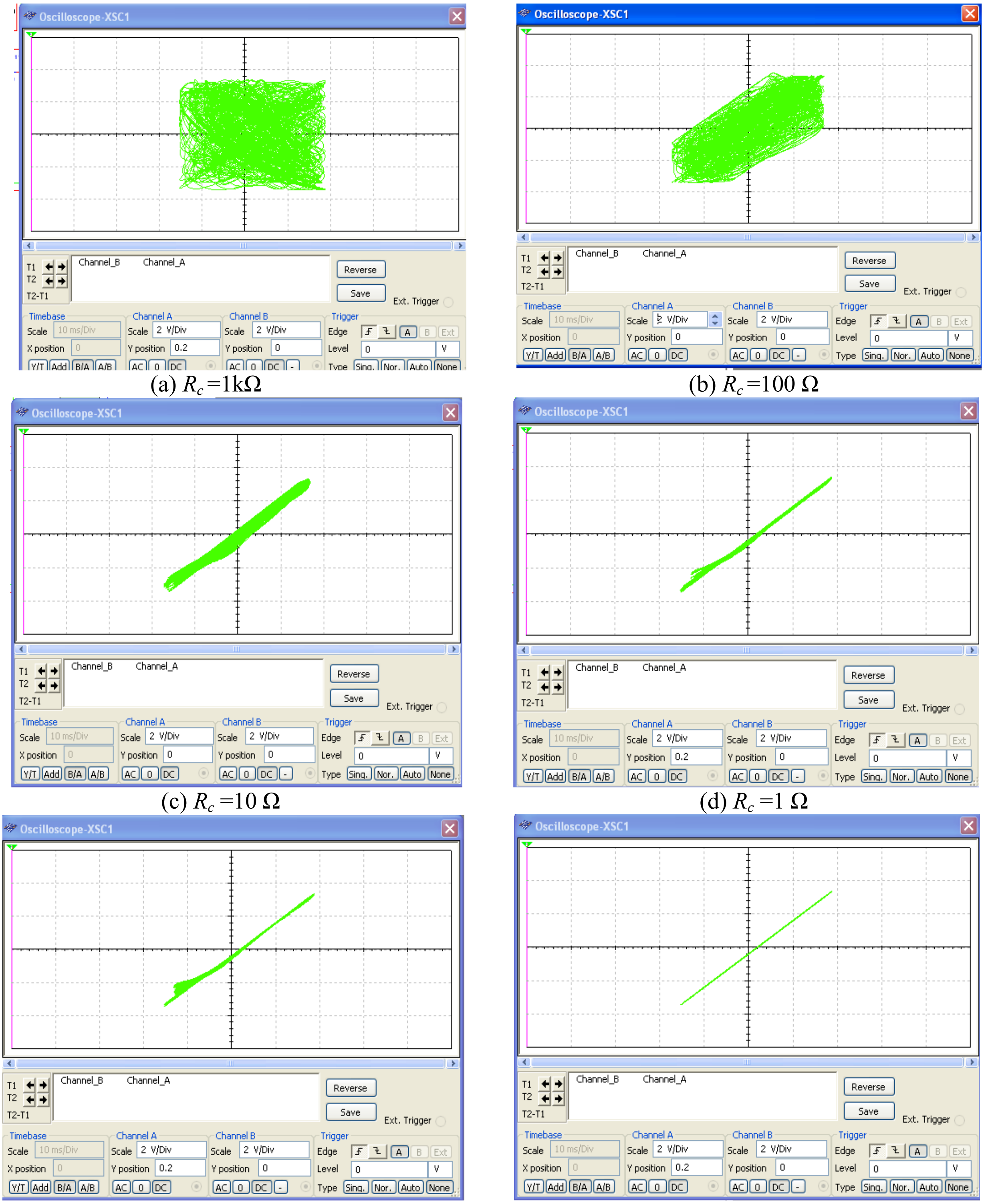


Fig. 5. Unidirectional chaotic synchronization Rossler circuit



(a) R_c=1kΩ

Timebase Scale 10 ms/Div, X position 0; Channel A Scale 2 V/Div, Y position 0.2; Channel B Scale 2 V/Div, Y position 0; Trigger Level 0 V

(b) R_c=100 Ω

Timebase Scale 10 ms/Div, X position 0; Channel A Scale 2 V/Div, Y position 0; Channel B Scale 2 V/Div, Y position 0; Trigger Level 0 V

(c) R_c =10 Ω

Timebase Scale 10 ms/Div, X position 0; Channel A Scale 2 V/Div, Y position 0; Channel B Scale 2 V/Div, Y position 0; Trigger Level 0 V

(d) R_c =1 Ω

Timebase Scale 10 ms/Div, X position 0; Channel A Scale 2 V/Div, Y position 0.2; Channel B Scale 2 V/Div, Y position 0; Trigger Level 0 V

(e) R_c =100 mΩ

Timebase Scale 10 ms/Div, X position 0; Channel A Scale 2 V/Div, Y position 0.2; Channel B Scale 2 V/Div, Y position 0; Trigger Level 0 V

(f) R_c =10 mΩ

Timebase Scale 10 ms/Div, X position 0; Channel A Scale 2 V/Div, Y position 0.2; Channel B Scale 2 V/Div, Y position 0; Trigger Level 0 V

Fig. 6. Phase portraits in the case of unidirectional coupling by using MultiSIM

Synchronization with MultiSIM simulation appears for a coupling strength $R_c \le 10$ mΩ as shown in Fig. 6 (f) For different initial conditions, if the resistance coupling strength $R_c > 10$ mΩ. The synchronization cannot occur as shown in Fig. 6 (a)-(e), the synchronization occurs when $R_c \le 10$ mΩ with errors $e_x = x_1 - x_2 \to 0$ which implies the complete synchronization for this resistance coupling strength as shown in Fig. 6 (f)

5 Application to Secure Communication Systems

5.1 Simulation in MATLAB

Consider the rescaled Rossler system as the transmitter:

Transmitter

$$\left.\begin{aligned}\frac{dx_1}{dt} &= -\alpha(\Gamma x_1 + \beta y_1 + \lambda z_1)\\ \frac{dy_1}{dt} &= -\alpha(-x_1 - \gamma y_1 + 0.02 z_1)\\ \frac{dz_1}{dt} &= -\alpha(-g(x_1) + z_1)\end{aligned}\right\} \qquad (9)$$

$$g(x_1) = \begin{cases} 0 & x_1 \le 3 \\ \mu(x_1 - 3) & x_1 > 3 \end{cases}$$

Receiver

$$\left.\begin{aligned}\frac{dx_2}{dt} &= -\alpha(\Gamma x_2 + \beta y_2 + \lambda z_2) + g_c(x_1 - x_2)\\ \frac{dy_2}{dt} &= -\alpha(-x_2 - \gamma y_2 + 0.02 z_2)\\ \frac{dz_2}{dt} &= -\alpha(-g(x_2) + z_2)\end{aligned}\right\} \qquad (10)$$

$$g(x_2) = \begin{cases} 0 & x_2 \le 3 \\ \mu(x_2 - 3) & x_2 > 3 \end{cases}$$

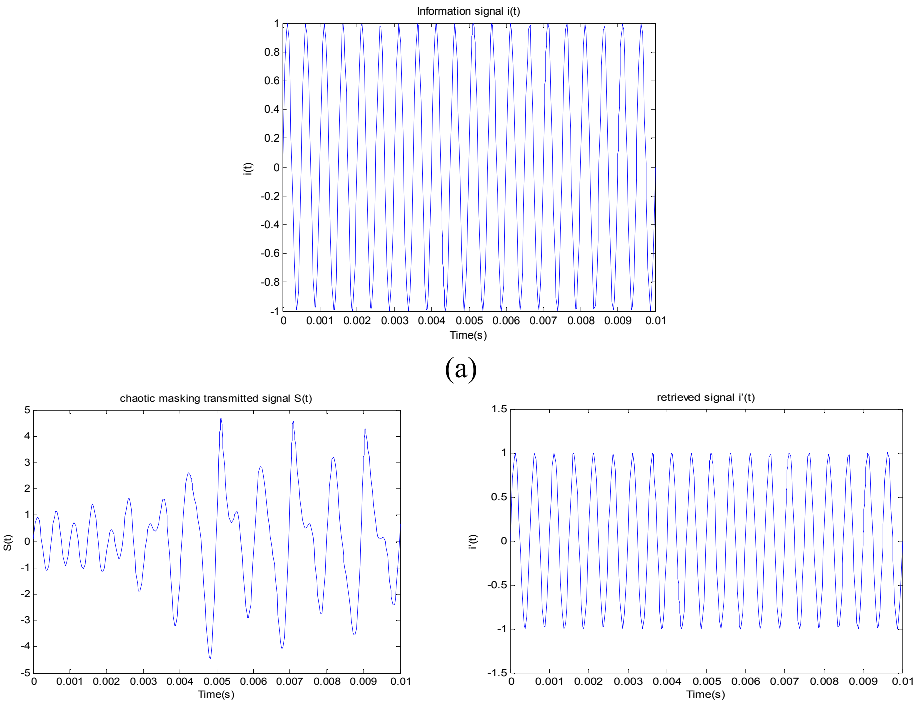
Sinusoidal wave signal recovery. To study the effectiveness of signal masking approach in the Rossler system, we first set the information-bearing signal *i(t)* in the form of sinusoidal wave

$$i(t) = A \sin(\ 2\pi f\ )t$$

Where A and f are the amplitude and the frequency of the sinusoidal wave signal. Respectively [19].

Due to the fact that output signal can recover input signal, it indicates that it is possible to implement secure communication scheme with the proposed chaotic system. The presence of the chaotic signal between the transmitter and receiver has proposed the use of chaos in secure communication systems [20].

The sinusoidal wave signals of amplitude 1 V and frequency 2 kHz is added to the generated chaotic x signal and the $S(t) = x + i(t)$ is feed into the receiver. The chaotic x signal is regenerated allowing a single subtraction to retrieve the transmitted signal, $[x + i(t)] - xr = i'(t)$, If $x = xr$. Fig. 7 (a-c) shows the MATLAB numerical simulation results for chaotic masking communication



(a)

(b) (c)

Fig. 7 MATLAB simulation of Rossler circuit masking communication system (a) Information signal *i*(*t*), (b) Chaotic masking transmitted signal *S*(*t*), (c) Retrieved signal *i'*(*t*).

5.2 Analog Circuit Simulation

In chaos-based secure communication schemes, information signals are masked or modulated (encrypted) by chaotic signals at the transmitter and the resulting encrypted signals are sent to the corresponding receiver across a public channel (unsafe channel). Perfect chaos synchronization is usually expected to recover the original information signals. In other words, the recovery of the information signals requires the receiver's own copy of the chaotic signals which are synchronized with the transmitter ones. Thus, chaos synchronization is the key technique throughout this whole process [20]. Fig. 8 shows the circuit schematic of implementing the Rossler circuit Chaotic Masking Communication. MultiSIM simulation results for several different frequencies are shown in Fig. 9. Fig. 9 shows the MultiSIM simulation results for masking signal communication system by varying the input signal's frequency. The red signal describes the wave information signal *i* (t), the green signal describes the transmitted chaotic masking signal *S* (t) and the purple signal describes the retrieved signal *i'*(*t*).

The simulation results shows that circuit autonomous Rossler is an excellent for chaotic masking communication when the frequency information is at intervals of 0.2 kHz – 9kHz. Otherwise, when the frequency information is more than 9 kHz or less than 0.2 kHz, the chaotic masking communication is not occur.

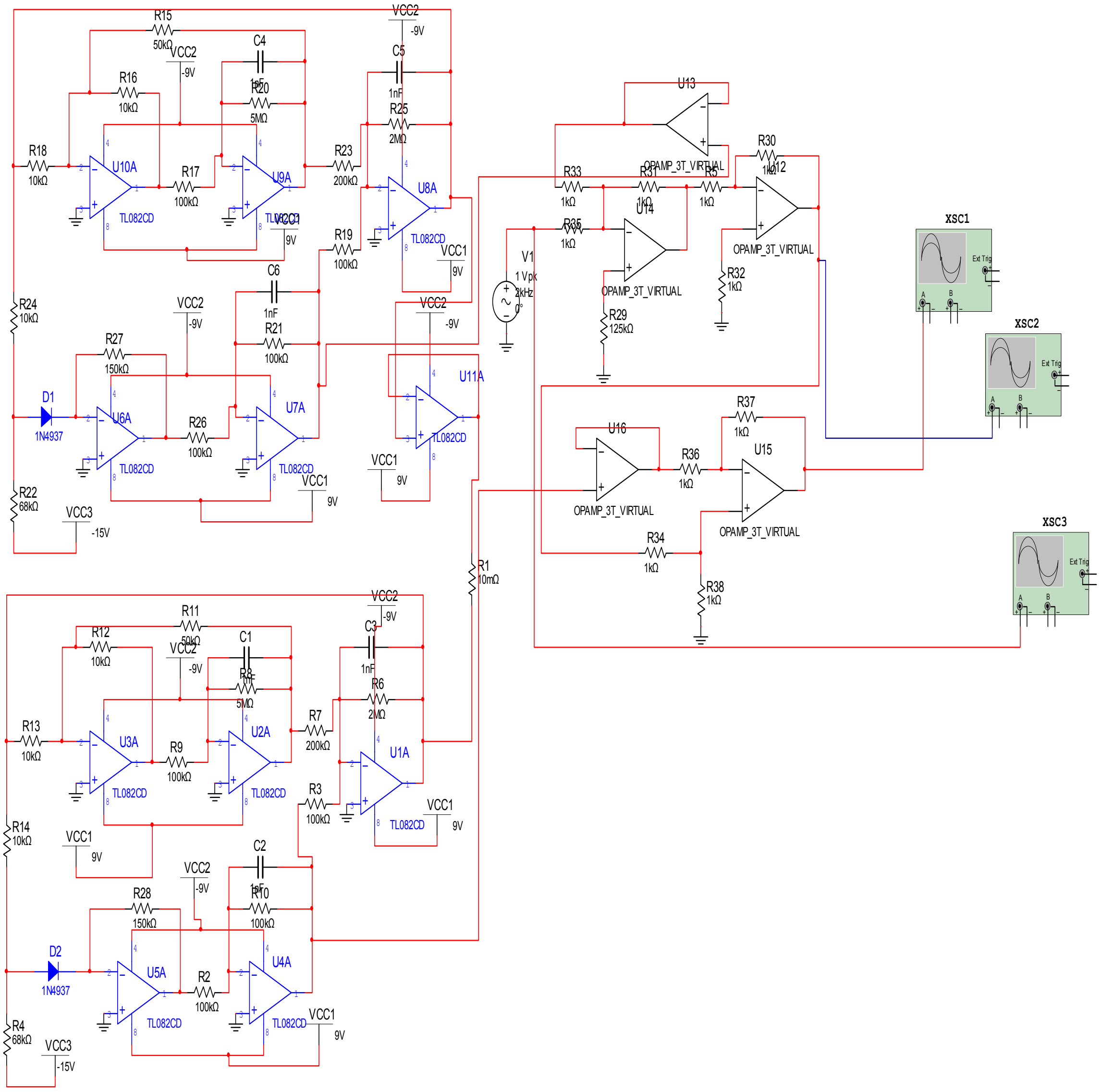
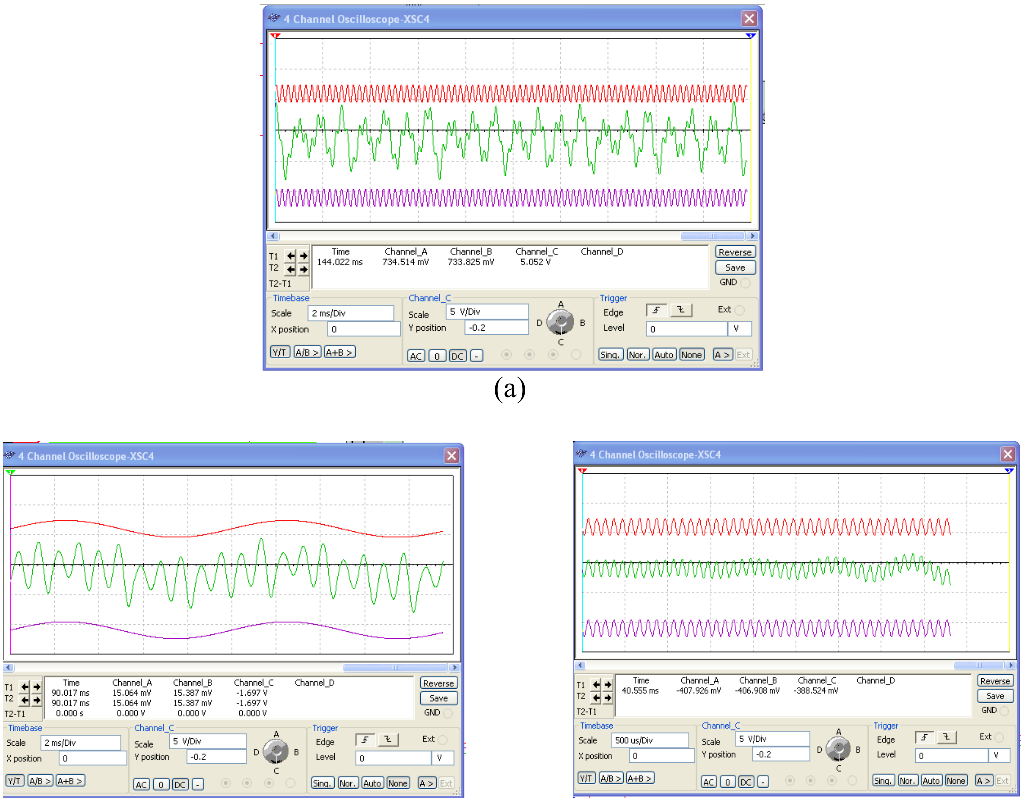


Fig. 8. Rossler circuit masking communication circuit.



```
Time         Channel_A    Channel_B    Channel_C    Channel_D
144.022 ms   734.514 mV   733.825 mV   5.052 V
```

Timebase Scale 2 ms/Div, X position 0; Channel_C Scale 5 V/Div, Y position -0.2; Trigger Level 0 V

(a)

```
Time         Channel_A    Channel_B    Channel_C    Channel_D
90.017 ms    15.064 mV    15.387 mV    -1.697 V
90.017 ms    15.064 mV    15.387 mV    -1.697 V
0.000 s      0.000 V      0.000 V      0.000 V
```

Timebase Scale 2 ms/Div, X position 0; Channel_C Scale 5 V/Div, Y position -0.2; Trigger Level 0 V

(b)

```
Time         Channel_A     Channel_B     Channel_C     Channel_D
40.555 ms    -407.926 mV   -406.908 mV   -388.524 mV
```

Timebase Scale 500 us/Div, X position 0; Channel_C Scale 5 V/Div, Y position -0.2; Trigger Level 0 V

(c)

Fig. 9. MultiSIM outputs of Rossler circuit masking communication systems
(a) Information frequency 4 kHz, (b) Information frequency 0.1 kHz (c) Information frequency 10 kHz

6 Conclusion

We propose a communication scheme for secure communications based on synchronization of chaotic systems. The scheme implies the use of two system variables, the one serves for chaos synchronization and the other is used for signal transmission and recovering. We show that the synchronization error for the novel scheme is smaller when $R_c \leq 10$ mΩ and complete synchronization occurs.

We have demonstrated in simulations that chaotic circuits can be synchronized and applied to secure communication. Chaos synchronization and chaos masking were realized using MultiSIM programs.

In this paper, it has been shown that Rossler circuit can be used in a communication security system at a frequency information interval of 0.2 kHz - 9 kHz. When the frequency information is more than 9 kHz or less than 0.2 kHz. The chaotic masking communication is not occur.

References

1. H. Ogras and M. Turk, Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function, *World Academy of Science, Engineering and Technology*, Vol. 67, 2012, pp. 555-558.
2. D. M. Porto, A Fuzzy Description of the Henon Chaotic Map, *Proceedings of the 5th WSEAS/IASME Int. Conf. on SYSTEMS THEORY and SCIENTIFIC COMPUTATION*, Malta, September 15-17, 2005, pp. 1-5.
3. C. K. Volos, I. M. Kyprianidis and I. N. Stouboulos, Designing a coupling scheme between two chaotic Duffing-type electrical oscillators, *WSEAS Transactions on Circuits and Systems*, Vol. 5, 2006, pp. 985-991.
4. M. S. Papadopoulou, I. M. Kyprianidis, and I. N. Stouboulos, Complex Chaotic Dynamics of the Double-Bell Attractor, *WSEAS Transactions on Circuit and Systems*, Vol 7, 2008, pp. 13-21.
5. M. Yao, Qinlong Gu, H. Zhu, Uncertainty-Driven Synchronization of a Hyper-chaotic System, *Proceedings of the 5th WSEAS International Conference on Applied Computer Science, Hangzhou, China*, 2006, pp. 629-634.

6. M. Sanjaya W. S, M. Mamat, Z. Salleh, and I. Mohd, Bidirectional Chaotic Synchronization of Hindmarsh-Rose Neuron Model, *Applied Mathematical Sciences,* Vol. 5, No. 54, 2011, pp. 2685 – 2695.
7. M. Sanjaya W. S, I. Mohd, M. Mamat, Z. Salleh, Mathematical Model of Three Species Food Chain Interaction with Mixed Functional Response. *International Journal of Modern Physics: Conference Series* Vol. 9, 2012, pp. 334–340.
8. F. Neri (2012). Agent based modeling under partial and full knowledge learning settings to simulate financial markets, AI Communications, IOS Press, printing.
9. J. C. Sprott, Dynamical models of love, *Nonlinear Dyn. Psych. Life Sci.* Vol. 8, 2004, pp. 303–314.
10. C. K. Volos, N. G. Bardis, I. M. Kyprianidis, I. N. Stouboulos, Implementation of Mobile Robot by Using Double-Scroll Chaotic Attractors. *WSEAS Recent Researches in Applications of Electrical and Computer Engineering, Vouliagmeni Beach, Athens, Greece.* March 7-9, 2012, pp. 119-124.
11. E. Steur, On Synchronization of Electromechanical Hindmarsh-Rose Oscillators, PhD thesis, *Eindhoven University of Technology Department of Mechanical Engineering Dynamics and Control Group*, Eindhoven, 2007.
12. C. Huygens, The pendulum or geometrical demonstrations concerning the motion of pendula as applied to clocks (translated by R. Blackwell), *Iowa State University Press*, 1986.
13. L. M. Pecora, and T. L. Carroll. Synchronizatin in Chaotic Systems, *Physical Review Letters,* Vol. 64, 1990, pp. 821–825.
14. Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, Experimental Demonstration of a Chaotic Cryptographic Scheme, *WSEAS Trans. Circuits Syst.*, Vol. 5, 2006, pp. 1654-1661.
15. T. L. Caroll, A Simple circuit demonstrating regular and synchronized chaos. *Am J Phys*. Vol. 63, No.4, 1995, pp. 377-379.
16. J. H. G. Lopez, R. J. Reatgui, A. N. Pisarchik, A. M. Hernandez, C. M. Gutierrez, R. V. Hernandez, R. V. Rauda, Novel Communication scheme based on chaotic Rossler circuits, *J. Phys. Conf. Ser*, Vol. 23, 2005, pp. 276-284.
17. D. L. Mancilla, V. E. Acero, R. J. Reatgui, J. H. G. Lopez, C. E. C Hernandez, Analysis of Experimental Encryption for a Chaos-Based Communication System, *International Congress on Instrument and Applied Sciences*, 2010.
18. E. J. P. Van den Hoven, Synchronization of Complex Networks, PhD thesis, *Centro de Investigation Cientıficay de Education Superior de Ensenada* (CICESE), Ensenada, Baja California, Mexico, 2007.
19. S. X. Wang, Simulation of Chaos Synchronization, PhD thesis, University of Western Ontario, London, 1998.
20. H. Zhang, Chaos Synchronization and Its Application to Secure Communication, PhD thesis, *University of Waterloo*, Canada, 2010.

Dynamics of Coupled Chaotic Bonhoeffer – van der Pol Oscillators

I M. KYPRIANIDIS, V. PAPACHRISTOU, I. N. STOUBOULOS
Physics Department
Aristotle University of Thessaloniki
Thessaloniki 54124
GREECE
imkypr@auth.gr, vpapachr@el.teithe.gr, stouboulos@physics.auth.gr

CH. K. VOLOS
Department of Mathematics and Engineering Studies
University of Military Education - Hellenic Army Academy
Athens, GR-16673
GREECE
chvolos@gmail.com

Abstract: - In the present paper, we have studied the dynamics of coupled chaotic Bonhoeffer – van der Pol (BvP) electrical oscillators. In the case of series connection and bidirectional coupling via linear resistor, as the coupling strength varies, the chaotic states are driven to periodic states. In the case of ring-type connection, synchronization is observed in the case that the voltage driven BvP oscillator have different circuit parameters than the two identical current-driven BvP oscillators. The Bonhoeffer – van der Pol (BvP) electrical nonlinear oscillators simulate neuron cells and in this case the linear coupling resistors act as electric synapses. These synapses varying their resistance control the dynamics of the neuron cells, from chaotic to periodic states.

Key-Words: - Bonhoeffer – van der Pol, nonlinear electrical oscillators, chaos control, chaotic synchronization, bidirectional coupling, neuron cells, electric synapse, electronic simulator, antimonotonicity.

1 Introduction

As the understanding of chaotic behavior has been deepend, a significant interest in the problem of controlling chaotic dynamics of nonlinear systems has been observed [1-5].

After the pioneering work of Ott, Grebogi and Yorke [6], several algorithms have been developed to achieve control of chaotic behavior in nonlinear dynamical systems. Patidar et al. [7], have shown, that in the case of two bidirectionally coupled nonlinear oscillators of the same kind, one periodic and one chaotic, chaotic behavior is converted into the desired periodic behavior, as the coupling factor is varied, while Kyprianidis et al. [8] have shown that chaotic behavior is converted into the desired periodic behavior, in both coupled schemes, unidirectional and bidirectional.

The notion of chaotic synchronization was introduced by Pecora and Carroll [9] in 1990. A wide range of research activity, in a variety of complex physical, chemical and biological systems has been stimulated, ever since [10-13]. In particular, the topic of synchronization of coupled chaotic electronic circuits has been studied intensively [14-15].

Chaos control and synchronization have important potential applications [16-18] in several scientific areas including biology [19], medicine [20], electric circuits [21-27], laser technology [28-30], secure communication [31-34], and neuroscience [35-37] to name but a few.

The system of two FitzHugh-Nagumo cells coupled with gap junctions is the simplest possible system simulating two coupled neuron cells via an electric synapse [38]. As introduced by Fitzhugh [39], the BvP model for a spiking neuron is a two dimensional reduction of the Hodgkin – Huxley equations [40]. A qualitative description of the single neuron activity is given, according to FitzHugh, by the system of coupled nonlinear differential equations:

$$\begin{cases} \dot{x} = \gamma\left(x - \frac{1}{3}x^3 + y + z\right) \\ \dot{y} = -\frac{1}{\gamma}\left(x - \alpha + \beta y\right) \end{cases} \tag{1}$$

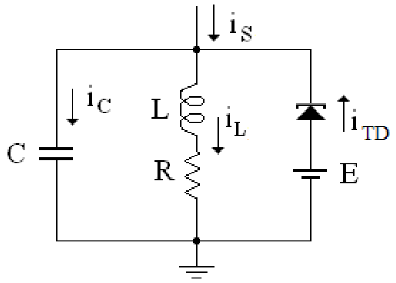


Fig.1. The electronic simulator of the BvP model proposed by Nagumo et al. [41].

The variable x describes the potential difference across the neural membrane and y can be considered as a combination of the different ion channel conductivities, present in the Hodgkin-Huxley model. The control parameter z of the BvP system describes the intensity of the stimulating current. Nagumo et al. [41] proposed an electronic simulator of the BvP model of FitzHugh using a tunnel diode as the nonlinear element (Fig.1).

The BvP model of nonlinear differential equations (1) can be simulated by a different nonlinear electric circuit (Fig.2), using a nonlinear resistor with a smooth cubic i-v characteristic.

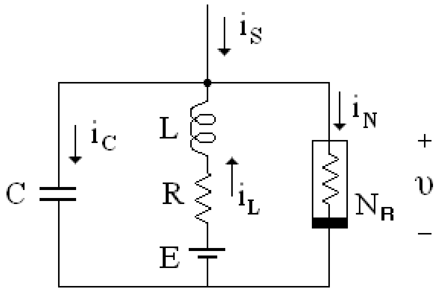


Fig.2. The electronic simulator of the BvP model of FitzHugh, proposed in the present paper.

2 Analysis of the New BvP Model

The smooth cubic i-v characteristic of the nonlinear resistor of the circuit of Fig.2 is given by the following equation:

$$i_N = g(\upsilon) = -\frac{1}{\rho}\left(\upsilon - \frac{1}{3}\frac{\upsilon^3}{V_0^2}\right) \tag{2}$$

where ρ and V_0 are normalization parameters. From Kirchhoff's laws:

$$i_C - i_L + i_N = i_S \tag{3}$$

and

$$\upsilon = E - Ri_L - L\frac{di_L}{dt} \tag{4}$$

or

$$\frac{d\upsilon}{dt} = \frac{1}{C}\left\{\frac{1}{\rho}\left(\upsilon - \frac{1}{3}\frac{\upsilon^3}{V_0^2}\right) + i_L + i_S\right\} \tag{5}$$

and

$$\frac{di_L}{dt} = \frac{1}{L}\left(-\upsilon - Ri_L + E\right) \tag{6}$$

By introducing new, normalized variables, $\tau = \frac{t}{\sqrt{LC}}$, $x = \frac{\upsilon}{V_0}$, $y = \frac{\rho i_L}{V_0}$, and $z = \frac{\rho i_S}{V_0}$, equations (5) and (6) are reduced to equations (7) and (8).

$$\frac{dx}{d\tau} = \gamma\left(x - \frac{1}{3}x^3 + y + z\right) \tag{7}$$

$$\frac{dy}{d\tau} = \frac{1}{\gamma}\left(-x - \beta y + \alpha\right) \tag{8}$$

where

$$\alpha = \frac{E}{V_0}\ ,\ \beta = \frac{R}{\rho}\ \text{ and }\ \gamma = \frac{1}{\rho}\sqrt{\frac{L}{C}} \tag{9}$$

The nonlinear differential equations (7) and (8) are the FitzHugh equations (1).

2.1 The BvP model proposed by Rajasekar and Lakshmanan

Rajasekar and Lakshmanan proposed a slightly different form of BvP oscillator [42,43] given by the following state equations:

$$\begin{cases} \dfrac{dx}{d\tau} = x - \dfrac{1}{3}x^3 - y + z \\ \dfrac{dy}{d\tau} = c\left(x + a - by\right) \end{cases} \tag{10}$$

The study of Eqs.(10) revealed the existence of chaotic behavior, following the period doubling route to chaos, and devil's staircases. The nonlinear differential equations (10) can be also simulated by a nonlinear electric circuit, using a nonlinear resistor with a smooth cubic i-v characteristic. The nonlinear electric circuit is shown in Fig.3. The smooth cubic i-v characteristic of the nonlinear resistor of the circuit of Fig.3 is given by the same equation, as before,

$$i_N = g(\upsilon) = -\frac{1}{\rho}\left(\upsilon - \frac{1}{3}\frac{\upsilon^3}{V_0^2}\right) \qquad (11)$$

where ρ and V_0 are normalization parameters. From Kirchhoff's laws:

$$i_C + i_L + i_N = i_S \qquad (12)$$

and

$$\upsilon = -E + Ri_L + L\frac{di_L}{dt} \qquad (13)$$

By introducing new, normalized variables $\tau = \dfrac{t}{\rho C}$, $x = \dfrac{\upsilon}{V_0}$, $y = \dfrac{\rho i_L}{V_0}$, and $z = \dfrac{\rho i_S}{V_0}$, equations (12) and (13) are reduced to equations (10), where,

$$a = \frac{E}{V_0}\ ,\ b = \frac{R}{\rho}\ \text{and}\ c = \frac{\rho^2 C}{L} \qquad (14)$$

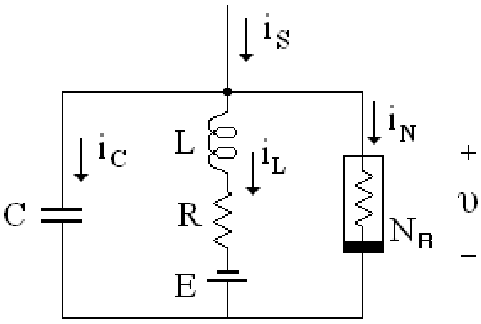


Fig.3. The nonlinear electric circuit simulating Eqs.(10).

The topology of the circuits of Fig.2 and Fig.3 is exactly the same, proving the equivalence of equations (1) and (10).

3 BvP Electrical Oscillator Driven by a Voltage Source

In the circuits of Figures 2 and 3, the driving source is a current source. But in most cases, circuits are driven by voltage sources. In this section, we will study the circuit of Fig.3 driven by a voltage source, as it is shown in Fig.4.

The smooth cubic i-v characteristic of the nonlinear resistor of the circuit of Fig.4 remains the same as before,

$$i_N = g(\upsilon) = -\frac{1}{\rho}\left(\upsilon - \frac{1}{3}\frac{\upsilon^3}{V_0^2}\right) \qquad (15)$$

and applying Kirhhoff's laws we have:

$$i_C + i_L + i_N = i_S \qquad (16)$$

where

$$i_S = \frac{\upsilon_S - \upsilon}{R_S} \qquad (17)$$

and

$$\upsilon = -E + Ri_L + L\frac{di_L}{dt} \qquad (18)$$

The normalized time, $\tau = \dfrac{t}{\rho C}$ and the normalized variables are:

$$x = \frac{\upsilon}{V_0}\ ,\ y = \frac{\rho i_L}{V_0}\ ,\ u = \frac{\rho \upsilon_S}{R_S V_0} \qquad (19)$$

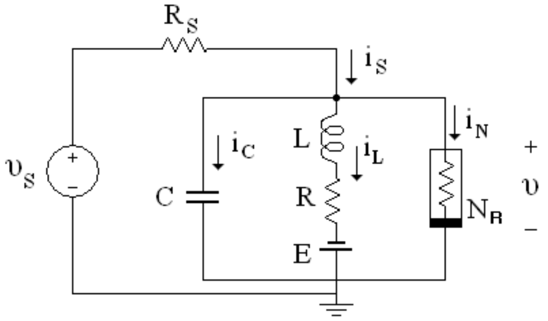


Fig.4. The equivalent circuit of BvP oscillator's state equations by Rajasekar and Lakshmanan driven by a voltage source.

Then the normalized state equations are the following.

$$\begin{cases} \dfrac{dx}{d\tau} = x(1-\varepsilon) - \dfrac{1}{3}x^3 - y + u \\ \dfrac{dy}{d\tau} = c(x + a - by) \end{cases} \tag{20}$$

where

$$a = \frac{E}{V_0},\ b = \frac{R}{\rho},\ c = \frac{\rho^2 C}{L} \text{ and } \varepsilon = \frac{\rho}{R_S} \tag{21}$$

In the general case, the driving voltage source has the following form:

$$\upsilon_S = B_S + B_0 \cos 2\pi f t \tag{22}$$

including a DC plus a sinusoidal term of frequency f, so:

$$u = U_S + U_0 \cos 2\pi f_N \tau \tag{23}$$

where the normalized frequency f_N will be $f_N = \rho C f$.

As we can observe, this circuit driven by a voltage source has one additional circuit parameter, ε, in relation to the current driven circuits of Figures 2 and 3, which enriches the complexity of its dynamics.

3.1 Dynamics of the circuit – Bifurcation diagrams

We have studied the dynamics of the circuit keeping constant the following parameters: a = 0.7, b = 0.8, c = 0.1, f_N = 0.160 and U_S = 0.0. The birurcation diagrams, y vs. U_0, for different values of factor ε, are shown in the following figures 5-8 and antimonotonicity, forward and reverse period doubling sequences, is observed [44-47].

4 The Coupled System

By coupling the circuits of Figures 3 and 4 via a linear resistor, we get the system of Fig.9. The two sub-circuits have identical circuit elements, L, R, C, E and NR .

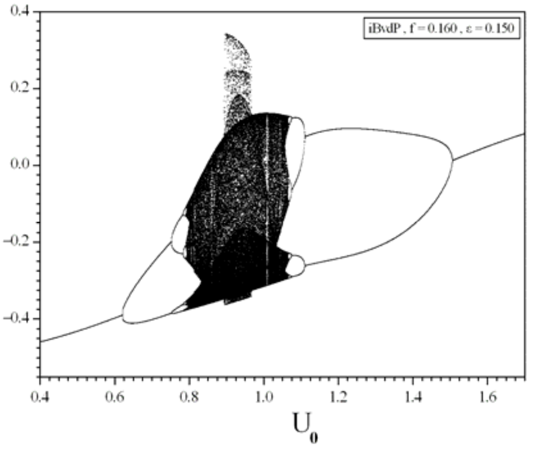


Fig.5. Bifurcation diagram, y vs. U_0, for ε = 0.150.

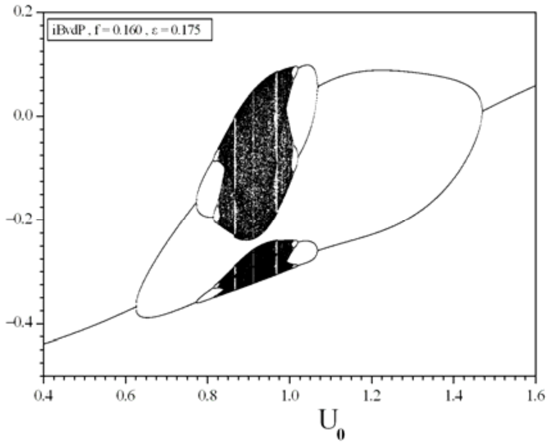


Fig.6. Bifurcation diagram, y vs. U_0, for ε = 0.175.

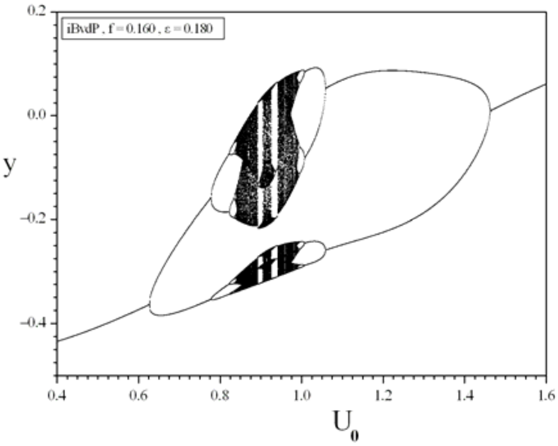


Fig.7. Bifurcation diagram, y vs. U_0, for ε = 0.180.

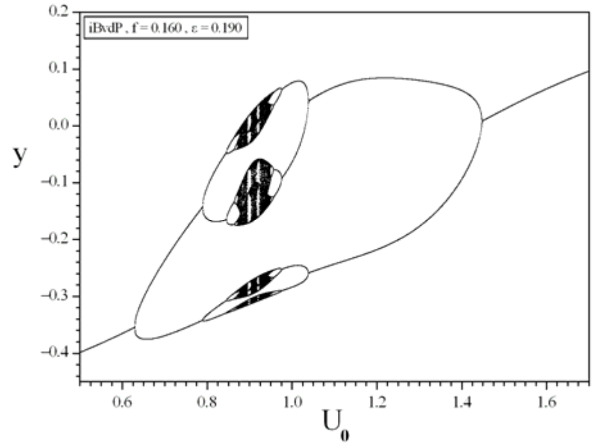


Fig.8. Bifurcation diagram, y vs. U_0, for ε = 0.190.

The normalized state equations of the system are:

$$\begin{cases} \dfrac{dx_1}{d\tau} = x_1(1-\varepsilon) - \dfrac{1}{3}x_1^3 - y_1 - \xi(x_1 - x_2) + u_S \\ \dfrac{dy_1}{d\tau} = c(x_1 + a - by_1) \\ \dfrac{dx_2}{d\tau} = x_2 - \dfrac{1}{3}x_2^3 - y_2 + \xi(x_1 - x_2) \\ \dfrac{dy_2}{d\tau} = c(x_2 + a - by_2) \end{cases} \tag{24}$$

where $\tau = \dfrac{t}{\rho C}$, and

$$x_j = \frac{\upsilon_j}{V_0}, \; y_j = \frac{\rho i_{Lj}}{V_0}, \; j = 1,2 \tag{25}$$

$$u_S = \frac{\rho \upsilon_S}{R_S V_0}, \;\; \varepsilon = \frac{\rho}{R_S}, \;\; \xi = \frac{\rho}{R_C} \tag{26}$$

while ξ is the coupling factor of the system. By choosing a = 0.7, b = 0.8, c = 0.1, f_N = 0.160, ε = 0.150, U_S = 0.0 and U_0 = 0.9, the first sub-circuit operates in a chaotic mode (see Fig.5).

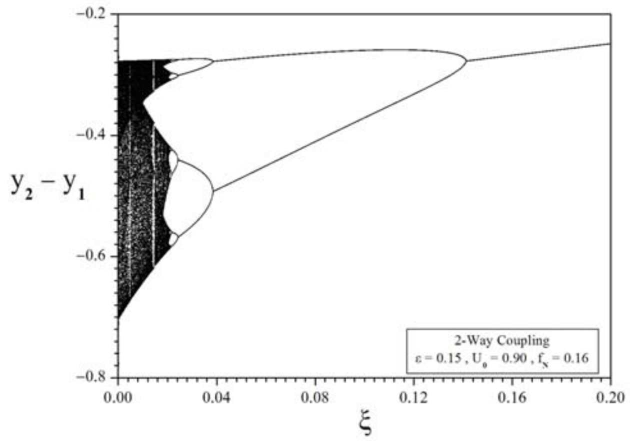


Fig.10. Bifurcation diagram (y_2 − y_1) vs. ξ presenting the dynamics of the coupled system of Fig.9.

By increasing the value of coupling factor, the system, starting from a chaotic state, undergoes a reverse period doubling and finally is locked in a period-1 state [7, 8] (see Fig.10).

Considering that the linear coupling resistor plays the role of an electric synapse, we conclude that it can control the chaotic dynamic state of the system.

By coupling one more sub-circuit, we get the system of Fig.11. The bifurcation diagrams vs. the coupling factor are shown in Figs.12-14. The electric synapses control the chaotic behavior, as in the previous case, and lock the system in a periodic state.

4 The Coupled System in a Ring Connection

The coupled system in a ring connection is shown in Fig.15. The voltage driven oscillator is 2-way coupled to current driven oscillators forming a ring connection via linear resisting coupling [15,48,49]. All three oscillators have the same circuit parameters.

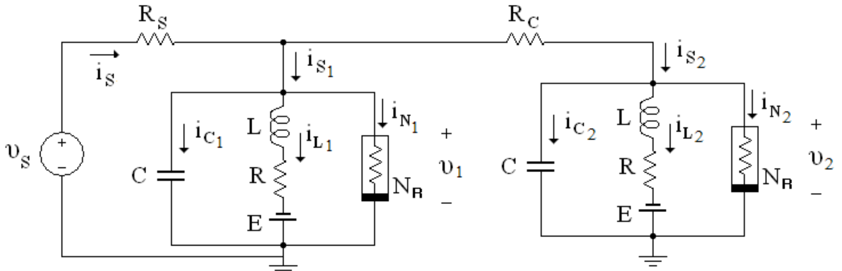


Fig.9. The bidirectional coupled system via the linear resistor.

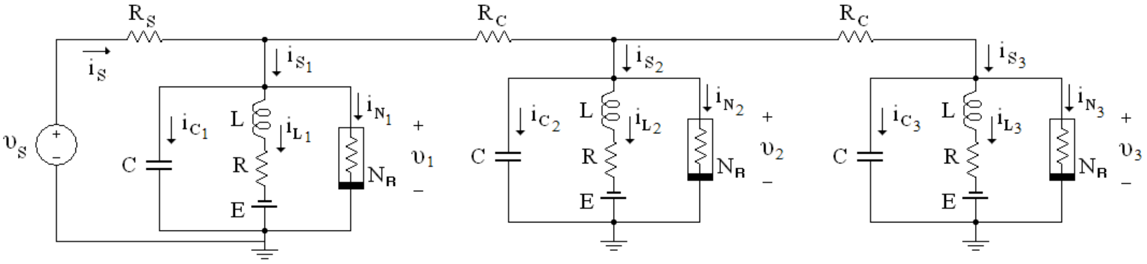


Fig.11. The coupled system consisting of three sub-circuits.

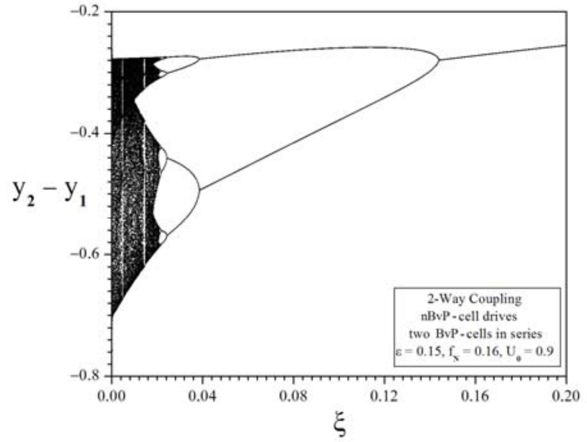


Fig.12. Bifurcation diagram $(y_2 - y_1)$ vs. ξ presenting the dynamics of the coupled system of Fig.11.

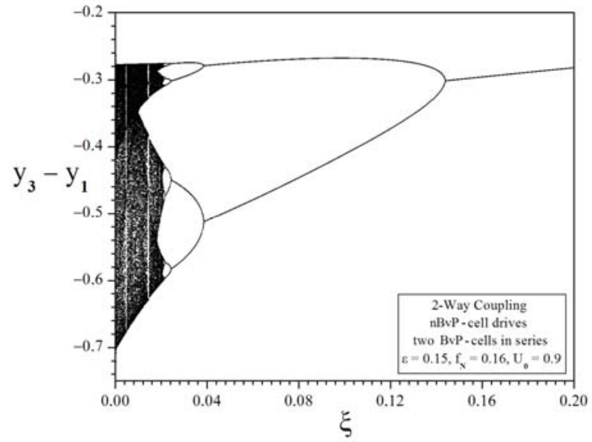


Fig.13. Bifurcation diagram $(y_3 - y_1)$ vs. ξ presenting the dynamics of the coupled system of Fig.11.

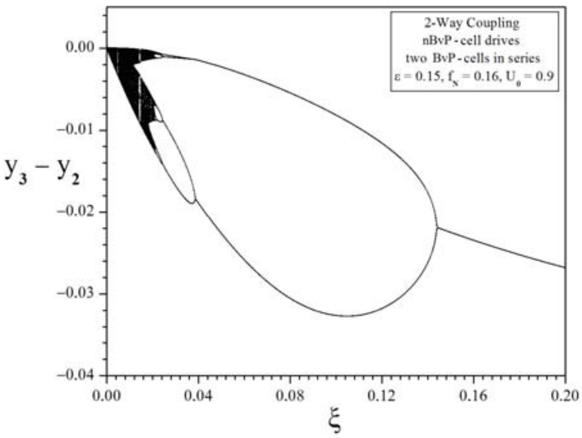


Fig.14. Bifurcation diagram $(y_3 - y_2)$ vs. ξ presenting the dynamics of the coupled system of Fig.11.

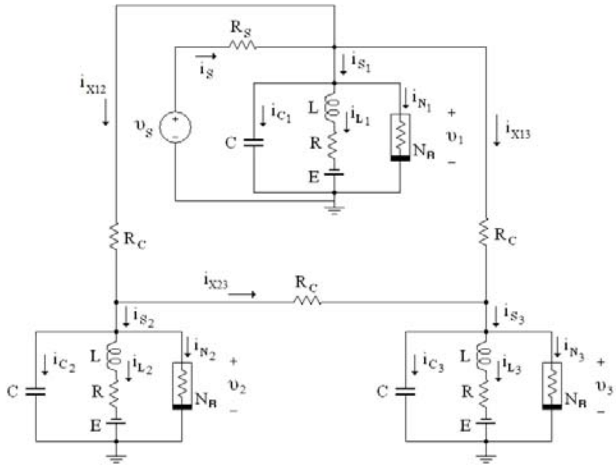


Fig.15. The coupled system in a ring connection.

The υ-i characteristics of the nonlinear resistors are given by the following relationship.

$$i_{Nj} = g(\upsilon_j) = -\frac{1}{\rho}\left(\upsilon_j - \frac{1}{3}\frac{\upsilon_j^3}{V_0^2}\right) \ , \ j = 1,2,3 \qquad (27)$$

Using Kirchhoff's laws the state equations of the system are the following:

$$\begin{cases} \dfrac{d\upsilon_1}{dt} = \dfrac{1}{C}\left\{\dfrac{1}{\rho}\left(\upsilon_1 - \dfrac{1}{3}\dfrac{\upsilon_1^3}{V_0^2}\right) - i_{L1} + \right. \\ \qquad\qquad \left. + \dfrac{\upsilon_S - \upsilon_1}{R_S} - \dfrac{2\upsilon_1 - \upsilon_2 - \upsilon_3}{R_C}\right\} \\ \dfrac{di_{L1}}{dt} = \dfrac{1}{L}\left(\upsilon_1 - Ri_{L1} + E\right) \\ \dfrac{d\upsilon_2}{dt} = \dfrac{1}{C}\left\{\dfrac{1}{\rho}\left(\upsilon_2 - \dfrac{1}{3}\dfrac{\upsilon_2^3}{V_0^2}\right) - i_{L2} + \dfrac{\upsilon_1 - 2\upsilon_2 + \upsilon_3}{R_C}\right\} \\ \dfrac{di_{L2}}{dt} = \dfrac{1}{L}\left(\upsilon_2 - Ri_{L2} + E\right) \\ \dfrac{d\upsilon_3}{dt} = \dfrac{1}{C}\left\{\dfrac{1}{\rho}\left(\upsilon_3 - \dfrac{1}{3}\dfrac{\upsilon_3^3}{V_0^2}\right) - i_{L3} + \dfrac{\upsilon_1 + \upsilon_2 - 2\upsilon_3}{R_C}\right\} \\ \dfrac{di_{L3}}{dt} = \dfrac{1}{L}\left(\upsilon_3 - Ri_{L3} + E\right) \end{cases} \qquad (28)$$

The normalized state equations of the system are:

$$\begin{cases} \dfrac{dx_1}{d\tau} = x_1\left(1-\varepsilon\right) - \dfrac{1}{3}x_1^3 - y_1 - \\ \qquad - \xi\left(2x_1 - x_2 - x_3\right) + u_S \\ \dfrac{dy_1}{d\tau} = c\left(x_1 + a - by_1\right) \\ \dfrac{dx_2}{d\tau} = x_2 - \dfrac{1}{3}x_2^3 - y_2 + \xi\left(x_1 - 2x_2 + x_3\right) \\ \dfrac{dy_2}{d\tau} = c\left(x_2 + a - by_2\right) \\ \dfrac{dx_3}{d\tau} = x_3 - \dfrac{1}{3}x_3^3 - y_3 + \xi\left(x_1 + x_2 - 2x_3\right) \\ \dfrac{dy_3}{d\tau} = c\left(x_3 + a - by_3\right) \end{cases} \qquad (29)$$

where $\tau = \dfrac{t}{\rho C}$ and

$$x_j = \frac{\upsilon_j}{V_0} \ , \ y_j = \frac{\rho i_{Lj}}{V_0} \ , \ j = 1,2,3 \qquad (30)$$

$$u_S = \frac{\rho\upsilon_S}{R_S V_0}, \ \varepsilon = \frac{\rho}{R_S}, \ \xi = \frac{\rho}{R_C} \qquad (31)$$

while ξ is the coupling factor. Keeping the same values of the system parameters, and increasing the value of the coupling factor, the bifurcation diagram of Fig.16 shows the change in dynamics of the voltage driven sub-circuit. The state variables of this sub-circuit, follow a reverse period doubling route from chaos to a period-1 state, while the state variables x_2, y_2, x_3 and y_3 have different dynamics. They, very fast, converge to an equilibrium point $Q(x_Q, y_Q)$ for every value of the coupling factor. For ξ = 0,001 we have $Q(x_Q, y_Q)$ = (-1,198, -0,624).

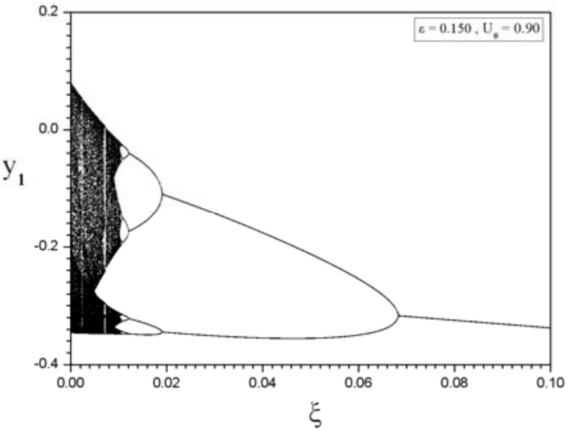


Fig.16. Bifurcation diagram y_1 vs. ξ presenting the dynamics of the voltage driven sub-circuit of Fig.15

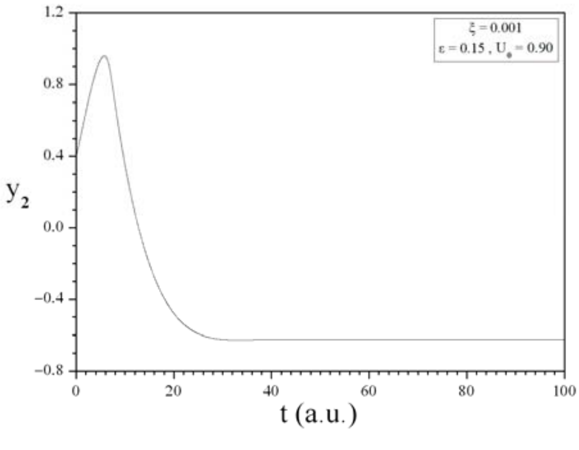


Fig. 17. The waveform of y_2 for $\xi = 0.001$.

The waveforms of y_2 and y_3 as well as their difference ($y_2 - y_3$) are shown in the figures 17-19, for $\xi = 0.001$, when the voltage driven sub-circuit is in a chaotic state.

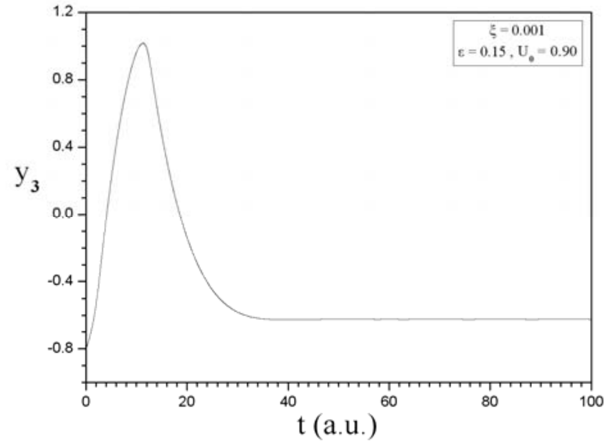


Fig. 18. The waveform of y_3 for $\xi = 0.001$.

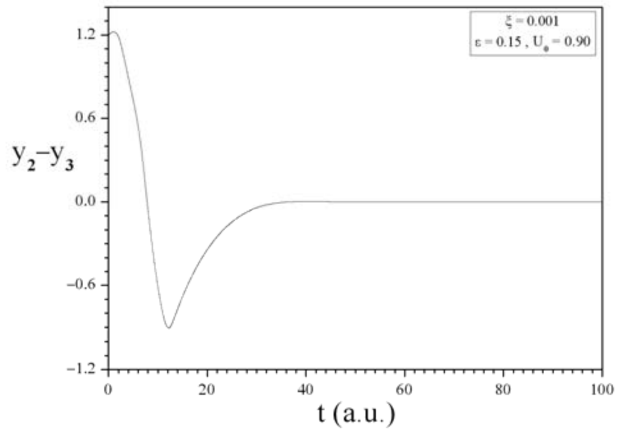


Fig. 19. The waveform of $\left(y_2 - y_3\right)$ for $\xi = 0.001$.

4.1 Chaotic Synchronization

In order to increase the complexity of the system, we have changed the circuit parameters a, b and c, which are no more identical for all the sub-circuits, while all the other parameters keep the same values. In this case, the state equations of the system (29) take the following form:

$$\begin{cases} \dfrac{dx_1}{d\tau} = x_1\left(1-\varepsilon\right) - \dfrac{1}{3}x_1^3 - y_1 - \\ \qquad -\xi\left(2x_1 - x_2 - x_3\right) + u_S \\ \dfrac{dy_1}{d\tau} = c_1\left(x_1 + a_1 - b_1 y_1\right) \\ \dfrac{dx_2}{d\tau} = x_2 - \dfrac{1}{3}x_2^3 - y_2 + \xi\left(x_1 - 2x_2 + x_3\right) \\ \dfrac{dy_2}{d\tau} = c_2\left(x_2 + a_2 - b_2 y_2\right) \\ \dfrac{dx_3}{d\tau} = x_3 - \dfrac{1}{3}x_3^3 - y_3 + \xi\left(x_1 + x_2 - 2x_3\right) \\ \dfrac{dy_3}{d\tau} = c_3\left(x_3 + a_3 - b_3 y_3\right) \end{cases} \tag{32}$$

For the following values of the circuit parameters $a_1 = 0.7$, $b_1 = 0.8$, $c_1 = 0.1$, $a_2 = a_3 = 0.0$, $b_2 = b_3 = 1.0$, $c_2 = c_3 = 0.425$, the bifurcation diagram ($x_2 - x_3$) vs. ξ is shown in Fig.20. For $\xi > 0.000012$ complete chaotic synchronization between the current driven sub-circuits is observed, while there are not synchronization phenomena between the voltage driven sub-circuit and any current driven sub-circuit (Fig.21). We have to notice, that chaotic synchronization between the current driven sub-circuits is observed because these two circuits are identical. If they are not identical, synchronization is not observed.

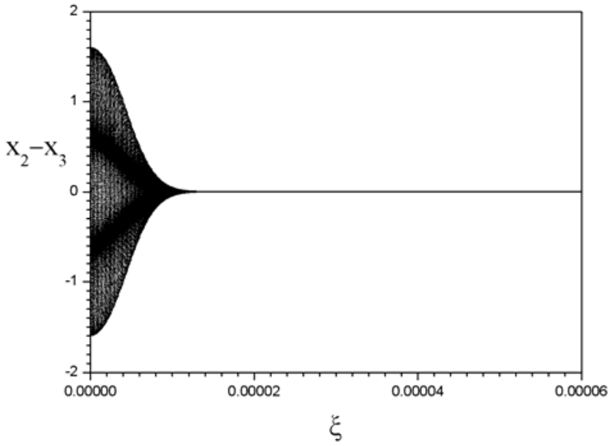


Fig.20. The bifurcation diagram ($x_2 - x_3$) vs. ξ, in the case of different a, b, c parameters of the sub-circuits.

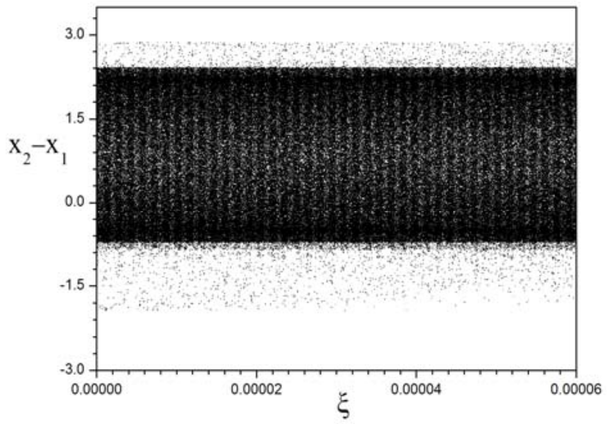


Fig.21. The bifurcation diagram ($x_2 - x_1$) vs. ξ, in the case of different a, b, c parameters of the sub-circuits.

5 Conclusions

In this paper we have introduced a Bonhoeffer – van der Pol (BvP) electrical oscillator driven by a sinusoidal voltage source and have studied coupled schemes consisting of Bonhoeffer – van der Pol electrical oscillators, which simulate the behavior of coupled neurons. The neurons are coupled via electric synapses, and the linear resistors play this role in the coupled system. In the case of bidirectional coupling, these synapses varying their resistance controlling the dynamics of the neuron cells, from chaotic to periodic states, as it is shown by the bifurcation diagrams. In the case of unidirectional coupling, the dynamics of the coupled system remains chaotic, as the coupling factor is varied. Periodic states are not observed.

In the case of ring-type connection, synchronization is observed in the case that the voltage driven BvP oscillator have different circuit parameters than the two identical current-driven BvP oscillators. The system has very interesting dynamics and its study is in progress.

References:

[1] G. Chen and X. Dong, *From Chaos to Order: Perspectives, Methodologies and Applications*, World Scientific, 1998.

[2] A. L. Fradkov and A. Yu. Pogromsky, *Introduction to Control of Oscillations and Chaos,* World Scientific, 1998.

[3] H. Zhang, D. Liu, and Z. Vang, *Controlling Chaos: Suppression, Synchronization and Chaotification*, Springer, 2009

[4] M. A. F. Sanjuan and C. Grebogi, *Recent Progress in Controlling Chaos*, World Scientific, 2010.

[5] S. Boccaletti, C. Grebogi, Y.-C. Lai, H. Mancini, D. Maza, The Control of Chaos: Theory and Applications, *Phys. Reports*, Vol. 329, 2000, pp. 103-197.

[6] E. Ott, C. Grebogi, and J. A. Yorke, Controlling Chaos, *Phys. Rev. Lett*, Vol.64, 1990, pp. 1196-1199.

[7] V. Patidar, N. K. Pareek, and K. K. Sud, Suppression of Chaos Using Mutual Coupling, *Phys. Lett*, Vol.A304, 2002, pp. 121-129.

[8] I. M. Kyprianidis, Ch. Volos, and I. N. Stouboulos, Suppression of Chaos by Linear Resistive Coupling, *WSEAS Trans. Circuits Syst.*, Vol.4, 2005, pp. 527-534.

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

[10] A. C. J. Luo, A theory for synchronization of dynamical systems, *Commun. Nonlinear Sci. Numer. Simul.*, Vol. 14, 2009, pp. 1901-1951.

[11] A. Pikovsky, M. Rosenblum and J. Kurths, *Synchronization: A universal concept in nonlinear sciences*, Cambridge University Press, 2003.

[12] E. Moselkide, Y. Maistrenko and D. Postnov, *Chaotic synchronization: applications to living systems*, World Scientific, 2002.

[13] S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares and C. S. Zhou, The synchronization of chaotic systems, *Phys. Rep.*, Vol.366, 2002, pp. 1-101.

[14] I. M. Kyprianidis and I. N. Stouboulos, Synchronization of two resistively coupled nonautonomous and hyperchaotic oscillators, *Chaos Solitons & Fractals*, Vol. 17, 2003, pp. 317-325.

[15] I. M. Kyprianidis and I. N. Stouboulos, Chaotic synchronization of three coupled oscillators with ring connection, *Chaos Solitons & Fractals*, Vol.17, 2003, pp. 327-336.

[16] G. Chen, *Controlling Chaos and Bifurcations in Engineering Systems*, CRC Press, 2000

[17] E. Schöll and H. G. Schuster, (Eds), *Handbook of Chaos Contro*l, Wiley-VCH, 2008.

[18] J. M. Gonzalez-Miranda, *Synchronization and Control of Chaos: An Introduction for Scientists and Engineers*, Imperial College Press, 2004.

[19] B. Lading, E. Moselkide, S. Yanchuk and Y. Maistrenko, Chaotic synchronization between coupled pancreatic β-cells, *Progr. Theor. Phys. Suppl.*, Vol.139, 2000, pp. 164-177.

[20] N.-H. Holstein-Rathiou, K.-P. Yip, O. V. Sosnovtseva and E. Moselkide, Synchronization phenomena in nephron-nephron interaction, *Chaos*, Vol.11, pp. 417-426, 2001.

[21] I.M. Kyprianidis, A. N. Bogiatzi, M. Papadopoulou, I. N. Stouboulos, G. N. Bogiatzis, and T. Bountis, Synchronizing chaotic attractors of Chua's canonical circuit. The case of uncertainty in chaos synchronization, *Int. J. Bifurc. Chaos*, vol. 16, 2006, pp. 1961-1976.

[22] Ch. K. Volos, I. M. Kyprianidis and I. N. Stouboulos, Various synchronization phenomena in bidirectionally coupled double scroll circuits, *Commun Nonlinear Sci Numer Simulat*, Vol.16, 2011, pp. 3356-3366.

[23] Ch. K. Volos, I. M. Kyprianidis and I. N. Stouboulos, Designing a coupling scheme between two chaotic Duffing-type electrical oscillators, *WSEAS Transactions on Circuits and Systems*, Vol.5, 2006, pp. 985-991.

[24] F. Dragan, Controlling Chaos in DC/DC Converters using Ott-Grebogi-Yorke and Pyragas Methods, *WSEAS Trans. Circuits Syst.*, Vol.5, 2006, pp. 849-854.

[25] Y. An, Z. Chen, C. Sun, Z. Liu, K. Yan, K. Warbinek, Control of Chaotic Behavior in Thruster Motor System for Deepwater Ocean Robot, *WSEAS Trans. Circuits Syst.*, Vol.5, 2006, pp. 774-777.

[26] O. Tsakiridis, E. Zervas, E. Lytra, J. Stonham, Two Inputs Electronic Controlled Chaotic Pattern Modulator, *WSEAS Trans. Circuits Syst.*, Vol.4, 2005, pp. 1464-1468.

[27] V. Grigoras, C. Grigoras, Encryption Method Based Non-Additive Discrete-Time Chaos Synchronization, *WSEAS Trans. Circuits Syst.*, Vol.5, 2006, pp. 1608-1613.

[28] I. V. Ermakov, V.Z. Tronciu, P. Colet and C. R. Mirasso, Controlling the unstable emission of a semiconductor laser subject to conventional optical feedback with a filtered feeback branch, *Optics Express*, Vol.17, 2009, pp.8749-8755.

[29] I. Wedekind and U. Parlitz, Synchronization and antisynchronization of chaotic power drop-out and jump-ups of coupled semiconductor lasers, *Phys. Rev. E*, vol.66, 2002, 026218.

[30] S. Sivaprakasam, E. M. Shahverdiev, P. S. Spencer, and K. A. Shore, Experimental demonstration of anticipating synchronization in chaotic semiconductor lasers with optical feedback, *Phys Rev Lett*, vol.87, 2001, 154101.

[31] S. Boccaletti, A. Farini, and F.T. Arecchi, Adaptive synchronization of chaos for secure communication, *Phys Rev E*, Vol.55, 1997, pp. 4979–4981.

[32] A. N. Miliou, I. P. Antoniades, S. G. Stavrinides and A. N. Anagnostopoulos, Secure communication by chaotic synchronization: Robustness under noisy conditions, *Nonlinear Analysis: Real World Applications*, Vol.8, 2007, pp. 1003-1012.

[33] B. Nana, P. Woafo, and S. Domngang, Chaotic synchronization with experimental application to secure communications, *Commun Nonlinear Sci Numer Simulat*, Vol.14, 2009, pp. 2266-2276.

[34] L. Gámez-Guzmán, C. Cruz-Hernández, R. M. López-Gutiérrez, E. E. García-Guerrero, Synchronization of Chua's Circuits with Multiscroll Attractors: Application to Communication, *Commun Nonlinear Sci Numer Simulat*, Vol.14, 2009, pp. 2765-2275.

[35] N. Axmacher, F. Mormann, G. Fernandez, C. E. Elger and J. Fell, Memory formation by neuronal synchronization, *Brain Research Reviews*, Vol.52, 2006, pp. 170-182.

[36] J. Wang, Y. Q. Che, S. S. Zhou and B. Deng, Unidirectional synchronization of Hodgkin-Huxley neurons exposed to ELF electric field, *Chaos Solitons & Fractals*, Vol.39, 2009, pp. 1335-1345.

[37] Q. Y. Wang, Q. S. Lu, G. R. Chen and D. H. Guo, Chaos synchronization of coupled neurons with gap junctions, *Phys. Lett. A*, Vol.356, 2006, pp. 17-25.

[38] M. Aqil, K-S. Hong, M-Y. Jeong, Synchronization of coupled chaotic FitzHugh-Nagumo systems, *Commun Nonlinear Sci Numer Simlat*, Vol.17, 2012, pp. 1615-1627.

[39] R. FitzHugh, Impulses and physiological states in theoretical models of nerve membrane, *Biophys. Journal*, Vol.1, 1961, pp. 445-466.

[40] A. L. Hodgkin and A. F. Huxley, A quantitative description of membrane current and its application to conduction and excitation in nerve, *J. Physiol.*, Vol.117, 1952, pp. 500-544.

[41] J. Nagumo, S. Arimoto, and S. Yoshizawa, An Active Pulse Transmission Line Simulating Nerve Axon, *Proc. IRE*, Vol.50, 1962, pp. 2061-2070.

[42] S. Rajasekar and M. Lakshmanan, Period-Doubling Bifurcations, Chaos, Phase-Locking and Devil's Staircase in a Bonhoeffer – van der Pol oscillator, *Physica D*, Vol.32, 1988, pp. 146-152.

[43] S. Rajasekar and M. Lakshmanan, Algorithms for Controlling Chaotic Motion: Application for the BVP oscillator, *Physica D*, Vol.67, 1993, pp. 282-300.

[44] M. Bier and T. C. Bountis, Remerging Feigenbaum Trees in Dynamical Systems, *Phys. Lett. A*, Vol.104, 1984, pp. 239-244.

[45] I. M. Kyprianidis, P. Haralabidis, I. N. Stouboulos, and T. Bountis, Antimonotonicity and Chaotic Dynamics in a Fourth Order Autonomous Nonlinear Electric Circuit, Int. *J. Bifurcation & Chaos*, Vol.10, 2000, pp. 1903-1915.

[46] I. M. Kyprianidis and M. E. Fotiadou, Complex Dynamics in Chua's Canonical Circuit with a Cubic Nonlinearity, *WSEAS Trans. Circuits Syst.*, Vol.5, 2006, pp. 1036-1043.

[47] I. N. Stouboulos, I. M. Kyprianidis, and M. S. Papadopoulou, Experimental Study of Antimonotonicity in a 4th Order Nonlinear Autonomous Electric Circuit, *WSEAS Trans. Circuits Syst.*, Vol.5, 2006, pp. 1662-1668.

[48] Y. Yu, S. Zhang, Global Synchronization of three coupled chaotic systems with ring connection, *Chaos Solitons & Fractals*, Vol.24, 2005, pp. 1233-1242.

[49] Y. Horikawa, Exponential Transient Propagating Oscillations in a Ring of Spiking Neurons with Unidirectional Slow Inhibitory Synaptic Coupling, *J. Theor. Biology*, Vol.289, 2011, pp. 151-159.

Low Color-Depth Image Encryption Scheme for use in COTS Smartphones

NIKOLAOS DOUKAS
Department of Mathematics and Engineering Science, Informatics and Computer Science Lab
Univ. Military Education - Hellenic Army Academy
Vari - 16673,
GREECE
nikolaos@doukas.net.gr

Abstract: - Cyber security and privacy are sources of increasing importance for the successful deployment of information and communication technology. This paper investigates aspects concerning privacy during the communication of low color depth images in encrypted form via low bit-rate, error prone channels. Existing approaches for region of interest determination in images, image encryption and image compression within this context are presented. The problem is established and conflicts between the aims of data compression and data encryption are out-lined and theoretically founded. An innovative approach is hence presented that automatically selects regions of interest in low color depth images, while achieving an acceptable level of security without increasing the data volume of the resulting image. The technique is suitable for cases where the data being transmitted has a limited lifecycle period and the compressed and encrypted image data are likely to be corrupted, such as the transmission via channels that are not guaranteed error – free. An error correction add-on to the algorithm permits an increase on the average decrypted image quality. Initial crypt-analytic resilience results for the proposed scheme are given. The proposed scheme is intended as a means of facilitating the deployment of COTS technology in tactical situations, by increasing the level of security of the underlying infrastructure.

Key-Words: - image encryption; encoding; low resolution; error resilience; COTS

1 Introduction

Information system security has grown over the years from a problem that concerned only military users of Information and Communication Technologies, to the primary concern of civilian and military authorities as well as commercial organizations at all levels of their respective hierarchies. In military and public applications, the introduction of command and control systems has given a new perspective in the efficiency of administration of the forces, but the fact that information systems and transmission networks extend to the last soldier in the field, has greatly increased the importance of managing the risk of some of the content traveling towards the command centers falling on hostile hands. Similar reasoning applies to government organizations that exploit distributed information systems in order to optimize the effectiveness of their administration. Commercial institutions are similarly organized in a distributed manner via exploitation of information systems so as to optimize their efficiency, exploit local manufacturing opportunities, reduce costs of traveling and better market their products and services in local markets by satisfying local particularities.

Communication of image data is of paramount importance both to military applications (e.g. command and control systems) as well as applications like health services (telemedicine, medical records etc). The image signal has its own particular characteristics. Images are in general large in size but may contain a significant amount of redundant information, even after a compression such that offered by standards like jpeg or tiff. Depending on the type of application, the encryption requirements will vary: military applications require that the image becomes totally unrecognizable while the requirements of a subscription television channel might be satisfied with significant degradation of the image quality [1]. The redundant information, when encrypted for security purposes, will give rise to even larger quantities of encrypted data that may not have a reason for existing [1]. It is sometimes feasible to accept the existence of such redundant data in images that are stored and processes off –

line or in systems whit excessive computational and storage capabilities. In certain applications however, where processing power is severely limited and storage and transmission bandwidth scarce, such waste is prohibiting for the use of security algorithms. Such applications include portable devices carried by personnel in the field, facsimile data, remote imaging devices etc. Security analysis of such systems is still an open issue [2], since cryptanalytic research focuses mainly on the needs of encryption of abstract data, without taking into consideration the needs of multimedia processing [2]. A fundamental problem in multimedia encryption is splitting the data stream into meaningful part, in a way such that no particular part alone is sufficient to attackers [3]. Another important open issue is concerned with removing the excessive redundancy contained in the image data, so as not to strain the system bandwidth [4]. An interesting approach is presented to this respect in [4] that additionally aims to exploit the data compression process as an additional encryption step. Further approaches for reducing the data volume by selecting the regions of interest are reported in [5]. A method for reducing the correlation present in images, due to the large areas of the background, is given in [6] and uses a pixel permutation block before the encryption. An attempt to simplify scanned document encryption, so that it may be implemented on an autonomous, FPGA based device was presented in [7]. A hierarchical encryption scheme that offers a beneficial compromise between the speed of encryption and the need for selective access to the image data is presented in [8]. An interesting image specific cryptanalysis example is presented in [9], giving significant information in the aspects of security that should be considered specifically for the case of image data. Additional information on cryptanalysis techniques based solely on permutations and XOR operations is given in [10]. The benefits and difficulties of block based image encryption schemes are analyzed in [11]. The fact that seemingly simplistic approaches, such as XOR masking of the image pixel data, may provide reliable encryption solutions depending on application requirements is pointed out in [12], [27], [28]. A particularly ambitious scheme for expert system based determination of the regions of interest of an image is presented in [13]. Permutation based encryption schemes targeted specifically to video images are presented in [14]. Selective encryption is another open topic appearing in literature. A selective encryption technique, suitable for directly encrypting compressed MPEG images is developed in [15]. The interaction between image compression and image encryption is analyzed in [16] and a method for bandwidth reduction via batch processing of correlated images, such as those found in video, is proposed. A significant drawback of standard security analyses for image encryption schemes is the lack of objective measures that have proven significance for the cryptanalytic resilience of such schemes [17]. Such objective measures are the object of current research [17]. The use of COTS smart phones by tactical edge users is seen by modern military as a means of promoting the situational awareness of this class of users that are frequently information challenged due to lack of secure communication channels [23]. This lightweight but robust encryption scheme addresses the problem of protecting the image Data-in-Transit [23]. Additional protection is of course needed for Data-At-Rest or In-Processing [23]. The overall development aims to promote the goal of exploiting COTS software, hardware and network infrastructure for the purpose of improving war and peace time tactical communication capabilities [24].

The paper is organized as follows. Section 2 gives an extensive account of the problems arising when attempting to design cryptographic protection for image transmission systems. The different requirements and compromises dictated by different applications are presented. Specific attention is given to the particular constraints imposed by the necessity for transmission of the images. Additional constraints due to computational resources are also examined. A detailed specification of the requirements from such cryptosystems is hence deduced. Section 3 describes the proposed approach for solving the problem, with particular emphasis on the scalability of the solution so as to match diverse set of cases. Additionally, issues concerning the selection of regions of interest and the application of error detection and correction techniques are also addressed. The proposed scheme aims to promote the level of security offered by portable COTS devices and hence promote the usability of such devices by field personnel in tactical operations. Section 4 presents a first approach to the cryptanalytic assessment of the proposed solution. Considerations concerning merit of cryptanalytic attacks on encrypted image transmission systems are first presented. The plaintext, approximation and a number of statistical and image specific cryptanalytic attacks are hence considered and an initial assessment of the resilience of the proposed system against such attacks is attempted. Finally conclusions are drawn and directions for future work are given.

2 Description of the problem

Image signals may vary dramatically in the resolution they carry, the rate at which data becomes available and the level of security they necessitate. Indeed, a medical image may be of high resolution, all of which is required to be encrypted and stored so as to satisfy the legal personal data protection requirements. A movie transmitted for recreational purposes via a subscription television service at high definition quality, produces large amounts of data at an extremely high rate but it is just required that unauthorized persons are incapable of viewing the images at their best quality.

On the other hand, imaging data coming from a field camera or facsimile images may be of low resolution, may contain large redundant areas (e.g. the white area of a page or the background of an area under surveillance) and the most difficult to achieve requirement is encrypting this information and transmitting it using channels that are likely to corrupt it. A small amount of corruption that would be acceptable in unencrypted transmissions, will lead to the total loss of data if security is also required. Consider for example the paradigm of a fax transmission. If in a plaintext fax a few bits were corrupted, this would lead to a few extra dots appearing in the page. Most users would hardly notice this happening. If however same the number of transmission errors happened in an encrypted transmission, depending on the encryption principle (block based and block size), the entire image might be lost. This problem may in some cases prohibit the use of secure channels for communication and hence jeopardize the efficiency of critical or sensitive operations, such as military operations.

The study of existing literature, presented in the previous section has demonstrated that, even though image encryption has been extensively studied, the case of extremely low color depth images has not been tackled. This study focuses on low depth images that carry critical information that is short – lived. Furthermore, the transmission is to be made in situations where neither the bandwidth nor computational resources are unlimited and the absence of transmission errors may not be assumed. In such cases it is common practice not to use any cryptography at all, since doing so would be impractical. This study proposes the introduction of a cryptographic algorithm that is lightweight enough for enabling utilization, while it is strong enough so as to render the decryption of the data by the adversary, within its useful lifetime, impractical. This problem is of particular importance to military applications, in the case of transmission of images concerning orders that are to be executed imminently. In this case the adversary might not know what the friendly forces are planning, but is going to be able to observe their actions within a very short period of time. Depending on the occasion, this could be of the order of hours, minutes or even seconds. As an example, consider a military unit that is about to be attacked by enemy forces. Their headquarters may wish to convey visual information concerning the approach of the attackers, or the required defense tactics. The enemy might already know or is about to find out this information respectively in each case, but it may prove of significant advantage for the friendly forces, if this happens after a significant time delay. Additionally, the algorithm is required to be such that, it can be practically implemented using normal, dispensable battlefield equipment, that is preferably COTS, while it cannot be cryptanalyzed, within time limits that are useful for the enemy, using equipment that the enemy would be willing to transport, install and maintain for this purpose.

This research is particularly focused on applications where low resolution and low color depth images are sufficient for the required performance. Typically in such cases both the bandwidth available for storage and transmission will be limited and the computational power that can be devoted for the cryptographic calculations will be severely restricted. In this context, the standard features desirable in any cryptosystem (as outlined and analyzed in [1]) may be interpreted as follows:

- Complexity: In such applications, computational power should be considered as being severely limited. Resources should ideally be uniquely directed to the Regions Of Interest (ROI’s) of the image. Real time operation is desirable, but could in cases be slightly circumvented, as for example in the case of surveillance picture frames that could be updated less often than normal television frames.

- Compression efficiency and Bandwidth expansion: Possibly the most difficult goal to satisfy. Compressing the data too much creates processing overhead while not compressing data enough will adversely affect bandwidth restrictions. The answer may only be given on a per case basis, taking into consideration the particular hardware capabilities.
- Perceptibility: In general, the applications this research focuses on are security targeted and hence no level of leftover perceptibility of the encrypted image is acceptable. In contrast to examples like pay TV, in secure storage or transmission problems any perceived part of the image leaks information to potential cryptanalysts.
- Format compliancy: If an encryption process produces data that is compatible to the format of the plaintext data one encounters in the same application, this means that the encryption block may be introduced as an add-on feature to existing systems. This could prove particularly beneficial for the penetration of the technology.
- Error resilience: Depending on the type of application, some error resilience may be mandatory. This is especially true for applications where transmission is involved, since in general the existing infrastructure might not necessarily provide error-free data communication services.
- Adaptability, scalability and multi-level encryption: Given that the previous requirements are satisfied, possible adaptability of the algorithms to the capabilities of different devices that may be simultaneously operating in the same network is desirable. Adapting image quality is not applicable in general, since typically images will be binary. Hence, in most cases, all users will require to be able to process the entire image.
- Content agnosticity: The encryption process should be able to compensate for variations in the incoming image statistical properties.

At this point it should be clarified that the problem which the focus of this work was not the improvement of the compression rate of existing algorithms. The aim was to develop reliable encryption algorithms, given the compression of existing image encoding techniques used in various applications (tiff, jpeg etc). The level of security achieved by these encryption algorithms was also the object of investigation. The following section describes an encryption process that satisfies the requirements and solves the problems that have been described for the case of low color depth images.

3 Proposed approach

The approach tested in this study combines a linear and a non linear encryption scheme in order to ensure that information remains protected, while the exposure to transmission errors does not endanger but only small areas of the useful image. The work presented here is extending the method presented in [19], so as to increase security without losing the suitability for COTS based deployment. Furthermore, a recently proposed error detection and correction scheme [20] is applied that increases the reliability of the essentially unreliable channel.

Regions of interest (ROI) are determined by a very strict approach. The ROI determination algorithm is based on the facsimile transmission paradigm. A typical image following this paradigm is shown in Figure 1.

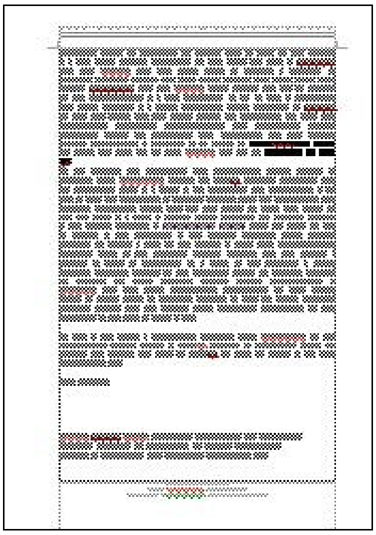


Figure 1. Typical Facsimile page form

The image may be assumed to be systematically laid out in rows. The scanning for ROI's is therefore carried out on a row by row basis. The pixels corresponding to a full block are assembled and examined. Any block with a single pixel different from its background is considered to mark the onset of a new region of interest. Given a row of pixels

$\{p_i\}$, with $i \in [0,N]$, the decision criterion is given in Equation 1.

$$\min(i) : p_i \neq \underline{0} \qquad (1)$$

The end of a row is scanned backwards in a similar manner to find the end of the region of interest. The blocks of the region of interest are then passed on for encryption, while blocks outside the ROI bypass this stage. All blocks are required to be complete and no blocks are allowed to cross the boundaries of the row within which they start. This approach leads to bandwidth savings for the facsimile transmission paradigm. This is true because, a text page will typically produce large white areas around its borders that will be left unencrypted. Similarly, large in – text gaps will also produce savings in bandwidth.

Before attempting estimates of bandwidth gains achieved, it should be noted that bandwidth reductions in encrypted images are much more significant in absolute terms that corresponding reductions in plaintext images. A typical encrypted facsimile page has been measured in experiments to be 4 to 9 times bigger in size than the corresponding plaintext image, even though both may be encoded in the same format (e.g. jpeg). This is because the encrypted image will typically present little or no redundancy [4]. For a typical A4 page with margins of 2.5 centimeters, the minimum bandwidth gain can be calculated as 40%. However this number is misleading as it takes into account the printing margins, which are easily detectable. The most important bandwidth reduction results from the detection of white areas within the useful area of the page (paragraph margins, inter – paragraph gaps, title spacing etc). Even though statistics of these gains are difficult to estimate, due to their high variability, but a conservative estimate for a mean paragraph size of 10 lines and single spacing may be conservatively estimated at 7%. Variants of this approach may be designed for perceived text layouts differentiating from the one shown in Figure 1 (e.g. double column, floating text segments etc).

Despite the ROI selection, the letters and symbols still contain a large proportion of white space inside their boundaries, while they consist themselves of uniformly, or almost uniformly, colored areas. This is due to the nature of the image being processed (text), as well as the fact that the images are of very low color depth (typically binary). Encrypting such an image, would therefore typically still produce systematic patterns on the encrypted result that would easily, or even readily, be legible as symbols. A sample of the systematic patterns that may appear in this situation is shown in Figure 2. In this picture it is relatively straightforward to distinguish the digits O, 1 and 4 and the letter sequence "www".

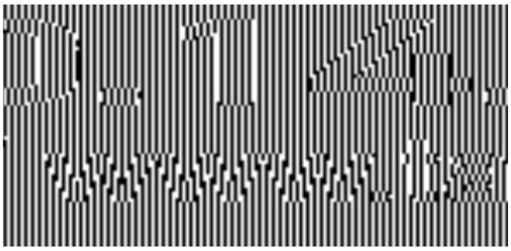


Figure 2. Sample systematic patterns appearing in encrypted segments

The encryption process therefore consists of two stages. In order to achieve reliable encryption, the data is first masked using random values originating from a pseudo random number generator and a linear masking function (XOR). Given a pixel sequence $\{p_i\}$ and a pseudo – random sequence $\{r_i\}$, the first stage cipher text $\{C_{1,i}\}$ will be obtained as shown in Equation 2.

$$C_{1,i} = p_i \oplus r_i \qquad (2)$$

The linearly encrypted data is hence encrypted with a block based non-linear algorithm, namely the AES. The block size and the key size of the AES have to be chosen in such a way as to maintain computational and bandwidth restrictions. Hence the second stage cipher text, given key k_i, is given as shown in Equation 3.

$$C_{2,i} = AES\left(C_{1,i}, k_i\right) \qquad (3)$$

A block diagram of the encryption process is shown in Figure 3.

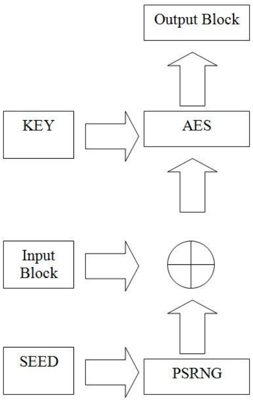


Figure 3. Block diagramof the stages of the encryption process

The polynomial of the random number generator is fixed while the seed changes in every line, according to a prearranged sequence of seeds, in a rolling manner. Additionally, the keys of the AES change between rows of the same transmission again according to a rolling key principle, thereby reducing the possibilities of cryptanalytic attacks such as the ciphertext only attack. In the results given in the following section, this was achieved via the use of tables of keys, pre – agreed between sender and receiver. It is planned for the final prototype to use a one time key. It should be noted that the key to the process is composite and consists of the AES key sequence, the PSRNG polynomial and the PSRNG seed sequence. As it was detailed above, the two ends of the communication channel need to be able to maintain and share those keys. The problem addressed by the proposed algorithm involves mainly portable devices to be used by personnel temporarily away from base for missions. It is therefore practical to implement the pre – agreement of keys based on a operational model of loading the device with enough keys before each mission.

For the results considered for this paper, block sizes of 8, 16 and 32 pixel values were used. A useful block is fed into the AES module with a key size of 256 bits, padded with non-significant data, as shown in Equation 2. Using a larger block size reduces the bandwidth necessary, while smaller sizes imply a higher level of security.

As it is apparent from the above description, the AES is implemented for operating in the Electronic Codebook (ECB) mode encryption, which is the most suitable for the limited computational resource case. However, the principle drawbacks of the ECB mode of operation for image encryption [25] are alleviated in this implementation. The masking with the random sequence and the padding imply that the resulting cipher is not suffering from the lack of randomness that is the principle drawback of ECB [25]. Furthermore, since the padding data is pseudorandom, identical data blocks do not produce identical cipher blocks, making the scheme unsusceptible to replay attacks.

In order to maintain the format compliancy requirement stated earlier on, the encrypted blocks are reassembled into a valid image file. In order to reverse the process, the receiver will need to be able to synchronize with the seeds and keys used at the transmitter side. Due to the noise-like appearance of the cryptographic algorithm output, it is not possible to perform a detection process, reciprocal to the region of interest detection described earlier. Therefore, synchronization symbols had to be inserted at the beginning of each row in the final output. Given a row of pixels $\{p_i\}$, with n the determined onset of the ROI and m the determined end of the ROI, the insertion of the synchronization symbol requires the assignments of symbols shown in Equation 4, where $\underline{1}$ denotes a unit pixel (for bitmap a value of 1) and ≡ denotes assignment.

$$\begin{aligned} p_{n-1} &\equiv \underline{1} \\ p_{m+1} &\equiv \underline{1} \end{aligned} \tag{4}$$

These symbols do not inhibit the compliancy to the format of the data, which can still be perceived by any of the remaining processing elements of the system as a valid image file. Visually, these symbols appear as isolated dots on the image that could be ignored as unperceivable for the average application, or could be removed if this is necessary.

The use of error correction techniques as an enabling technology for robust secure image transmission has been proposed in literature [18]. A method was recently proposed for correcting transmission errors corrupting the data that could deal with both isolated and burst errors [20]. This method, which operates at a reasonable computational overhead, was used as an additional block enhancing the error resilience properties of the encryption scheme. The use of error correction schemes could be relevant even for a smart phone based implementation, in the case where transmission is based on tethering the device to radio equipment, or should be disabled in the case where 3G type networks are used.

Alternative encryption schemes involving non-linear Boolean transformations, such as those that the author has recently studied for user authentication purposes [21], are currently being investigated.

A simplified block diagram of overall the proposed approach is shown in Figure 4.

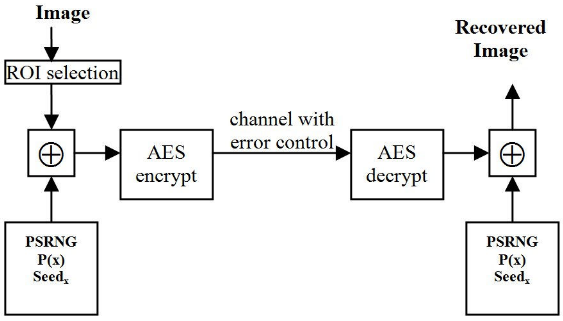


Figure 4. Block diagram of the proposed setup

The possibility of integrating advanced authentication and key management techniques (such are those presented in [22]) is being investigated. Additionally, advances in automated algorithmic design that are anticipated following the research in [21], are expected to enhance the overall security of the system, while reducing the required computational complexity, via the use of Boolean cryptographic functions.

The proposed encryption scheme was implemented in Matlab using C functions. The results of the simulation and cryptanalytic tests performed are given in the following section.

4 Cryptanalytic Assessment

Cryptanalytic attacks with particular significance for image encryption systems include the Known Plaintext Attack but also the Approximation Attack, the Error Concealment Attack and the Statistical Attack [1].

The proposed approach is meant to be useful for applications where the useful life of image data is of limited duration and where normally none or limited cryptographic protection would be used. This encryption scheme aims to maintain confidentiality and integrity of the data, without guaranteeing availability. Availability, especially in tactical situations, is an independent problem which is tackled by use of specialized communication channel infrastructure. Therefore, for the application paradigm, encompassing the conditions outlined above, a first approach to the cryptanalytic assessment of the scheme will be attempted. All analyses were made using the Matlab suite of tools.

4.1 Plaintext attack

In order to mount a known plaintext attack on an image cryptosystem, a cryptanalyst would try to exploit specific characteristics of the encrypted data in order to recover the encryption keys [1]. Such characteristics include the existence of file headers and frame markers, of smooth spaces in images and still frames in video. The proposed approach produces images that are format compliant, i.e. the file headers are there in plaintext format and correspond to the encrypted version of the data. They hence carry no information concerning the encryption keys that a cryptanalyst could exploit. Areas of the image that are smooth (white) are either left unencrypted or are masked with a random pattern before being encrypted. Given the rolling random seeds and the rolling encryption keys, such areas will convey no information about the encryption key that might be useful to a cryptanalyst. A mathematical proof for this statement is currently being developed and will be presented in a future publication.

4.2 Approximation attack

An approximation attack will try to detect any traces of perceptual information that are still visible after the encryption process, even if it is not possible to extract the exact original image. This is mainly achieved via exploitation of the spatial correlation in the image data [1]. This type of danger might be considered as extremely significant for the particular application considered in this research, given that scanned text might still be legible even if only a small amount of such correlation exists. Additional dangers will materialize if edge information remains in place after the encryption process. In order to investigate this type of attack, the correlation properties of selected areas of both encrypted and plaintext images have been studied. Figure 5 shows a sample portion of an encrypted image.

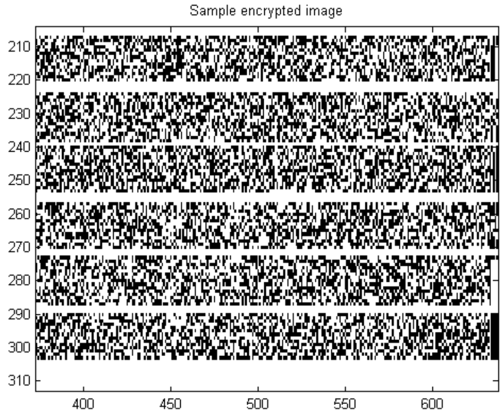


Figure 5. Example of an encrypted text image

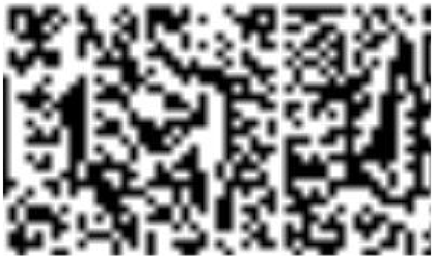


Figure 6. Detail of the encrypted image

The noise-like properties of this image are clearly visible. Figure 6 depicts a detail of a text segment, where all the systematic patterns of Figure 2 shown in the previous section have disappeared. Figure 7 depicts an attempt to apply edge detection (using the Sobel method) on the encrypted image of Figure 5. The result shows that there exists no apparent exploitable edge information in this example. The same conclusion has been drawn on several similar experiments with different images and different operators such as the Prewitt, Roberts, Laplacian and zero – crossing methods for edge detection.

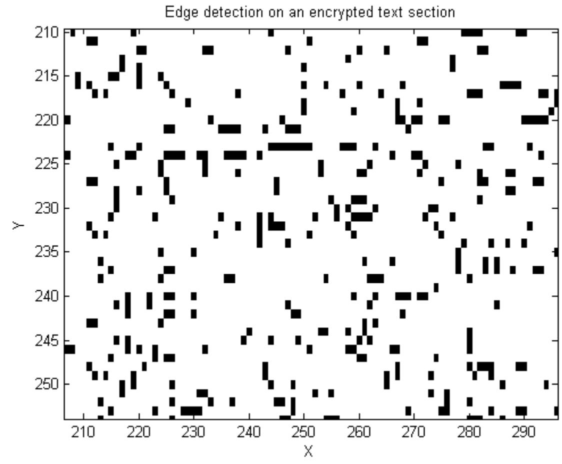


Figure 7. Sobel edge detection on the sample image

4.3 Error concealment attack

An Error Concealment attack would attempt to exploit statistical information and knowledge about the format of the data to achieve a perceptual cracking of the encryption [1]. Such an attack would be considered as successful, if the attacker managed to recover a recognizable version of the image, with inferior quality compared to the original [1]. In the case o this attack, the weak point of the ciphertext is redundancy left over after the region of interest selection and encryption processes, which may be exploited for revealing degraded but recognizable parts of the image [1].

In order to investigate the resilience of the proposed algorithm to such attacks, the correlation properties of the encrypted image have also been studied, both at large scale (image level) and at small scale (letter level). Correlation would reveal any similarity existing between the original image and the ciphertext image, as required by this type of attack in order to function. The result in Figure 8 shows the correlation of a 300x300 encrypted region with its plaintext version.

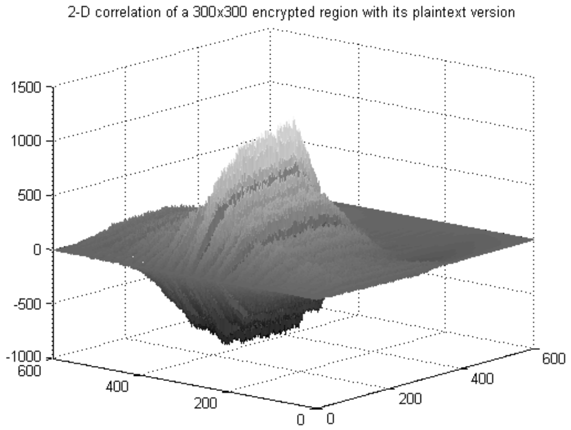


Figure 8. Correlation between encrypted and plaintext images

For the above calculation, the bitmap image has been normalized by subtracting its mean and hence contains negative values. A maximum correlation score of roughly 4000 is hence expected. The observed peak of approximately 500 should therefore be attributed to windowing effects rather than any real correlation between the data of the two images. Furthermore, the above correlation result should be compared with Figure 9 that shows the autocorrelation of the plaintext version of the same region and Figure 10 that shows the cross correlation of the encrypted region with another random encrypted region of the same dimensions.

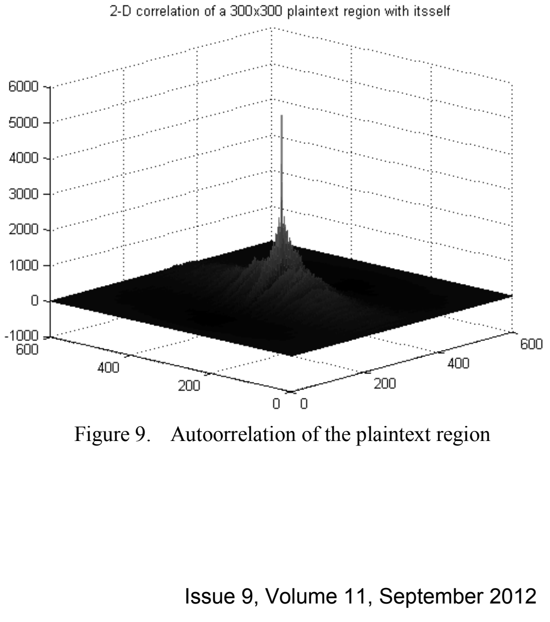


Figure 9. Autoorrelation of the plaintext region

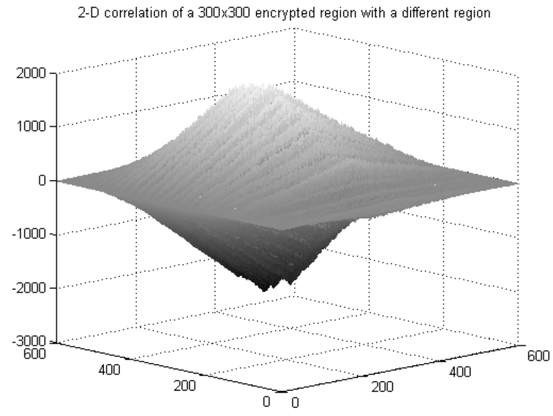


Figure 10. Cross correlation of the encrypted region with a randomly selected one

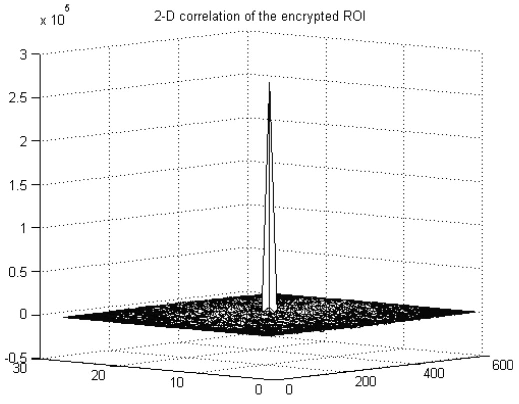


Figure 11. Autocorrelation of a ROI segment

From Figures 9 and 10, it may be concluded that indeed a high correlation score should have been achieved if there were indeed any leftover unencrypted exploitable information left in the encrypted image. The second conclusion that may be drawn is that the correlation score is independent of the area of the image that is being examined. Attackers are therefore prevented from managing to use known plaintext to mount either of the two above types of cryptanalytic attacks. Additionally, Figure 11 shows the autocorrelation of a segment of the encrypted image that corresponds solely to a region of interest segment of the image. The noise like behavior of the encrypted image is clearly observable. It should be noted that all the previous results (apart from Figure 11) have been obtained using areas of the image that correspond principally to useful data (areas in the middle of paragraphs containing small intermediate line spacing).

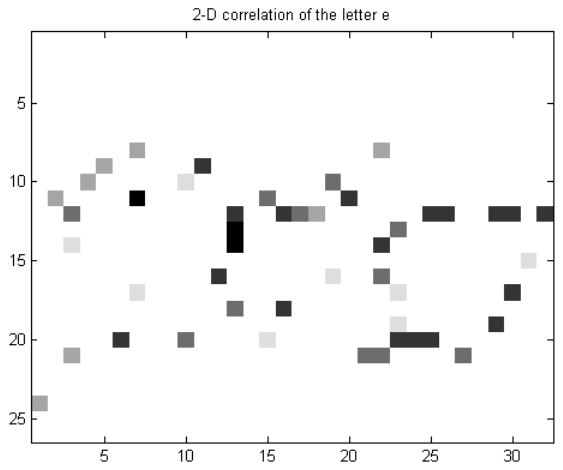


Figure 12. Cross correlation of the letter “e” with its neighbourhood

4.4 Statistical attack

A statistical attack on this particular cryptosystem would try to exploit the language redundancies that would cause the repeated appearance of common letters in the encrypted data. The cryptanalyst would exploit the predictability of a particular element of the image or relationships between the original bitstream and the cipher codestream [1]. Such relationships would lead either to recovering the plaintext without knowing the key or to substantially reducing the search space upon which a brute force attack may be mounted.

The conceptual elements in the case of the facsimile paradigm are the letters of the alphabet. In order to produce an initial assessment of the resilience of the proposed algorithm to such attacks, it was investigated whether it would be feasible to exploit linguistic and format knowledge in order to locate letters within the ciphertext.

Towards this aim, the area where the letter “e” lies in the encrypted image was separated and its correlation with various areas of the image was calculated. The results obtained at the area where this letter is actually located are shown in Figure 12. Similar results were obtained when examining other areas of the image. It should be noted that the letter “e” is a letter that appears with a high probability in the English language. The experiment was repeated with all letters of the alphabet. The conclusion drawn from the above experiment is that attempts to detect letters in the encrypted image are not successful.

4.5 Other types of attacks

Further quantitative analysis of the resilience of the proposed method to cryptanalytic attacks is under way and the applicability of quantitative measures like the Luminance Similarity Score and Edge Similarity Score [1] is being investigated, together with other objective security metrics such as those proposed in [17].

Summarizing this initial cryptanalysis assessment and considering the combination of linear and non-linear cryptography that the proposed method uses, the small block size appears as an advantage against cryptanalytic attacks. If a particular block were to be jeopardized, then the limited amount of data that would become available to the attacker would be insufficient for reducing the random sequence used. Furthermore, the masking of the data via the use of the random sequence essentially makes the operation of the AES more effective, since there exist no more white areas where there is a risk for repetitive patterns carrying information to leak out of the encryption process.

The proposed scheme exploits the fact that the images for encryption are of low color depth, in order to employ the simplistic region of interest selection technique described in Section 3 above. Extensions may be envisaged that may be applied to higher color depth images, e.g. by serializing the corresponding bits, provided that the short lifespan of the information prerequisite continues to be maintained.

This technology is consistent with the current trend of using COTS systems for military applications in order to minimize the ever increasing costs of development [23], [24]. The principles of this approach are that COTS technologies are evolving far more rapidly than military technology may ever evolve, since the funds available for military research are being constantly reduced. Furthermore, this equipment requires shorter training periods for military staff than purpose built field equipment, since especially younger personnel, are extremely familiar with its operation. In this spirit, COTS smartphones are being deployed for battlefield use. Such devices are powerful enough to apply the proposed scheme to significantly more complex images, such as content enhanced COTS territorial maps, such as Google maps. An Android phone prototype implementation of the proposed scheme is currently being developed, that will be used for more thorough testing and evaluation.

An open issue remaining to be investigated is the case where the device implementing the algorithm is captured by prospective attackers. The requirement is in this case that future communications are not jeopardized because of this fact. This problem is currently being investigated. A partial solution, concerning the protection of the AES block, was presented by the author and associated researchers in [26]. This solution’s applicability however, depends on the physical circuit layout of the device being used and its ability to be connected to additional elements such as smart cards. Other COTS technologies, such as screen locks, pins and passwords, may also contribute towards this aim, combined with more specialized countermeasures. These countermeasures may include mechanisms for merging the memory contents or honey pots that are activated when user authentication fails [23], [24].

5 Conclusion

A study of encryption of digital image data has been presented. The particular nature of the problem of encrypting image data that is intended for transmission or storage was analyzed. This problem was studied in the broader context of facilitating the exploitation of COTS technology and networks, for the benefit of tactical level military users. A review of the state of the art of image encryption in current literature was given and the fact that many issues still remain open was concluded. The problem and particular requirements from image encryption schemes that deal exclusively with encrypting low color depth images are extensively analyses and the applicability of standard image encryption requirements to this particular problem is extensively investigated.

An encryption scheme is proposed that is intended for providing secure and robust transmission of encrypted images over channels permitting errors was proposed. An initial cryptanalysis study for the proposed scheme was presented that demonstrated satisfactory robustness properties against common attacks. Further work is currently under way in the fronts of introducing more secure encryption algorithms in the scheme, of further reducing the computational effort required for the encryption process and of selecting relevant objective security metrics and applying them to better assess the resilience of the scheme to attacks.

An analysis was made for applications of the proposed scheme to COTS communication equipment intended for battlefield use. The advantages and drawbacks of such applications was considered.

References:

[1] N. S. Kulkarni, B. Raman, and I. Gupta, "Multimedia Encryption: A brief overview" *Rec. Advan. in Mult. Sig. Process. and Commun., SCI 231*, pp. 417–449, 2009

[2] S. Lian, D. Kanellopoulos and G. Rufo, "Recent Advances in Multimedia Information System Security", Informatica 33 (2009) pp 3–24.

[3] W. Fang and J. Lin, "Multi-channel Secret Image Transmission with Fast Decoding: by using Bit-level Sharing and Economic-size Shares," International Journal of Computer Science and Network Security, vol.6 No.5B, pp 228 – 234, May 2006.

[4] D. Xie and C. Jay Kuo, "Multimedia encryption with joint randomized entropy coding and rotation in partitioned bitstream," EURASIP Journal on Information Security Volume 2007, Article ID 35262, 18 pages, 2007.

[5] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, "Overview on Selective Encryption of Image and Video: Challenges and Perspectives," EURASIP Journal on Information Security Volume 2008, Article ID 179290, 18 pages 2008.

[6] M. Younes and A. Jantan, "An image encryption approach using a combination of permutation technique followed by encryption": International Journal of Computer Science and Network Security, VOL.8 No.4 pp 191 – 197, April 2008.

[7] I. Atakli, Q Wu, Y, Chen and S. Craver. "BLINK: Pixel-Domain Encryption for Secure Document Management" MM&Sec '09 Proceedings of the 11th ACM workshop on Multimedia and security, pp 171-176, 2009

[8] C. Fonteneau, J. Motsch, M. Babel and O. D´eforges. "A Hierarchical Selective Encryption Technique in a Scalable Image Codec". In International Conference in Communications, Bucharest, Romania, 2008, http://hal.archives-ouvertes.fr/hal-00336403/

[9] S. Li, Chengqing Li, K. Lo, and G. Chen. "Cryptanalysis of an Image Scrambling Scheme without Bandwidth Expansion. IEEE Transactions on Circuits and Systems for Video Technology, VOL. 18, NO. 3, PP. 338–349, 2008

[10] M. Younes and A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm": International Journal of Computer Science, VOL. 35 No. 1, February 2008.

[11] J. Hu, F. Han. "A pixel-based scrambling scheme for digital medical images protection". Journal of Network and Computer Applications 32, 788–794, 2009

[12] A. Wong and W. Bishop. "Expert Knowledge Based Automatic Regions-of-Interest (ROI) Selection in Scanned Documents for Digital Image Encryption" Proceedings of the 3rd IEEE Canadian Conference on Computer and Robot Vision, 2006

[13] D. Socek. "Permutation-based transformations for digital multimedia encryption and steganography." PhD Thesis, Florida Atlantic University, 2006

[14] M. Droogenbroeck and R. Benedett. "Techniques for a selective encryption of uncompressed and compressed images". Proceedings of ACIVS 2002 (Advanced Concepts for Intelligent Vision Systems), Ghent, Belgium, September 9-11, 2002

[15] D. Arroyo, C. Li, S. Li, G. Alvarez and W.A. Halang. "Cryptanalysis of an image encryption scheme mased on a new total shuffling algorithm" Chaos, Solitons & Fractals, Volume 41, Issue 5, 15 September 2009, Pages 2613-2616

[16] T.H. Chen, C.S. Wu. "Compression-unimpaired batch-image encryption combining vector quantization and index compression". Information Sciences 180 1690–1701, 2010

[17] J. Sun, Z. Xu, J. Liu and Y. Yao. An objective visual security assessment for cipher-images based on local entropy. Multimed Tools Appl 53:75–95 2011

[18] M.A. El-Iskandarini, S. Darwish, S.M. Reliable wireless error correction technique for secure image transmission., 2009. 43rd Annual 2009 International Carnahan Conference on Security Technology, pp 184 – 188, 2009

[19] N. Doukas and N.V. Karadimas. A blind source separation based cryptography scheme for mobile military communication applications. WSEAS Transactions On Communications , Volume 7 Issue 12, pp 1235-45, 2008

[20] Bardis, N.G, Markovskyi, O., Doukas, N. Efficient burst error correction method for application in low frequency channels and data storage units. IEEE Digital Signal Processing (DSP), 2011 17th International Conference on, 2011

[21] Bardis, N., Doukas N. and Markovskyi, O. 'Fast subscriber identification based on the zero knowledge principle for multimedia content distribution', To appear in the Int. J. of Multimedia Intelligence and Security.

[22] Nikolaos Bardis, Nikolaos Doukas, and Konstantinos Ntaikos. 2008. A new approach of secret key management lifecycle for military applications. WSEAS. Trans. on Comp. 7, 12 (December 2008), 2011-2021.

[23] A. M. Buibish, N. E. Johnson, D. Emery and M. Prudlow. Cryptographic Solutions for COTS Smart Phones. Military Communications Conference (MILCOM) 2011 , Page(s): 1434 – 1439

[24] R.S. Oregon. Smart Fires: A COTS Approach to Tactical Fire Support Using a Smartphone. PhD Thesis, Naval Postgraduate School, September 2011

[25] Wikipedia: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

[26] Bardis, N.G.; Doukas, N.; Markovskyi, O.P.; , "Organization of the polymorphic implementation of Rijndael on microcontrollers and smart cards," Military Communications Conference, 2010 - MILCOM 2010 , vol., no., pp.1783-1787, Oct. 31 2010-Nov. 3 2010

[27] Ch. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Image Encryption Process Based on a Chaotic True Random Bit Generator", In Proc. Of 16th IEEE International Conference on Digital Signal Processing (DSP 2009), Vols. 1 and 2, pp. 1091-1094, July 2009, Santorini, Greece.

[28] F. Neri, Software Agents as A Versatile Simulation Tool to Model Complex Systems. WSEAS Transactions on Information Science and Applications, WSEAS Press (Wisconsin, USA), Issue 5, Vol. 7, 2010, pp.609-618.