Awakening to Reality

Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical Engineering

Elixir Elec. Engg. 122 (2018) 51685-51689

Elixir

ISSN: 2229-712X

Secure Communication using Microcontroller ATMEGA 16

Anup Kumar Das[1] and M. K. Mandal[2]

[1]Department of Electronics and Instrumentation, Dr. B. C. Roy Engineering College, Durgapur 713206, India.

[2]Department of Physics, National Institute of Technology, Durgapur 713209, India.

ARTICLE INFO

Article history:

Received: 20 July 2018;

Received in revised form:

24 August 2018;

Accepted: 4 September 2018;

Keywords

Chaos,

OPCL coupling,

Microcontroller ATMEGA16,

Secure communication.

ABSTRACT

The synchronization of the chaotic sequence using open plus closed loop (OPCL) coupling is presented in this paper by realizing 1D logistic map in microcontroller based hardware electronic experiment. The masking of the information signal in driver and demasking in the driven system is done in the chaotic region by using two microcontrollers ATMEGA 16 for secure communication. These two microcontrollers are used for driver and driven systems. In the synchronized condition driver system received the modulating signal from the signal generator and mask it with the chaotic sequence for transmitting to the driven system. In the receiver, section demasking is done to retrieve the information signal. The proposed scheme is simulated in Proteus simulator and the complete hardware circuit has been implemented and the obtained hardware experimental results confirm the validity of the proposed circuit.

Introduction

The data security and secrecy in communication are the important aspects in today’s world. Secure communication may be achieved by employing chaos based communication (such as chaos masking, chaotic modulation etc.) or by adopting cryptographic techniques. Chaotic communication is popular due to its inherent properties like highly unpredictable, random-look nature and ease of implementation of chaotic trans-receiver in a prototype electronic circuit. The chaos based secure communication systems may be designed in both analog and digital domain. In analog domain, it is possible due synchronization [1] of chaos in analog electronic circuits. Under synchronization, the driver system control the response system in such a way that both the systems produce synchronous output. But in digital domain, the system parameters and initial condition play the role of controlling signal for synchronization. A number of articles are reported in the literature by addressing the synchronization of chaos and its application in secure communication systems. In ref. [2] chaotic Chua oscillator is modified by incorporating smooth and bounded function to use it as a chaos generator in the transmitter part and the similar circuit is also used in receiver part for chaos synchronizer to design secure communication system. In ref. [3], a discrete chaotic map is used for the generation of chaotic sequences for secure communication using microcontroller Arduino.

The use of logistic map in chaotic cryptography is also reported in the literature [4, 5]. These two references presented the symmetric key cryptographic algorithm for encrypting text and image respectively by confusion and diffusion process using chaotic sequence of logistic map. Another chaotic encryption algorithm for real time communication is presented in [6] by using XilinxVirtex6FPGA based embedded systems. A fractional logistic map is analyzed in ref. [7] to generate chaotic signals and a modified logistic map is used in ref. [8] to generate true random numbers. Logistic map has many applications in the literature, in electronics, it is used in secure communication [9, 10] and in biological systems it is used to study the dynamic of birth and death processes [11] of many species. The logistic map is also used to model some chemical reaction, economic growth prediction, etc.

In this paper, we presented microcontroller based secure communication system by synchronizing two logistic maps through OPCL coupling. In the driver system, the generated chaotic sequence is used to encrypt the information signal before sending it to the receiver. The synchronized driven system is then follows the reverse technique to return back to the information to complete the communication process. The rest of the article is as follows. A brief description of chaotic logistic map is given in section 2 with its bifurcation diagram and initial conditions sensibility test. Section 3 described the OPCL coupling theory using *n* dimensional map and the driver and driven system equations using 1D logistic map are mentioned according to this theory. Section 4 presents a secure communication scheme based on microcontroller with proper block diagram and flowchart. The results of the experimental realization are given in section 5. Section 6 states the summary of the whole study and conclusion.

The logistic map

The logistic map is a one dimensional non-linear relation with a single parameter r given by [12, 13],

$$\mathbf{x_{n+1} = r x_n(1 - x_n)} \qquad (1)$$

The state variable x_n represents the chaotic sequence which lies between zero and one as shown in Fig.1. The sensitivity of the logistic map to the initial conditions $x_0 = \mathbf{0.495}$ and $\mathbf{x_0} = \mathbf{0.470}$ is shown in Fig. 2. The blue colour represents the discrete time trajectory corresponding to $\mathbf{x_0 = 0.495}$ and the brown colour corresponding to $x_0 = \mathbf{0.470}$.. The parameter r is a positive number in the range 0 to 4. At r approximately 3.57 is the onset of chaos, at the end of the period-doubling behaviour.

Tele: +91 343 2754784

E-mail address: mrinalkanti.mandal@phy.nitdgp.ac.in

The values beyond 3.57 exhibit chaotic behaviour, but there are still certain isolated values of *r* that appear to show non-chaotic behaviour; these are sometimes called islands of stability. For instance, beginning at $\mathbf{1+\sqrt{8}}$ there is a range of parameters $\mathbf{r}$ which show oscillation between three values, and for slightly higher values of *r* oscillation between 6 values, then 12 etc. But beyond $\mathbf{r = 4}$, the value of $\mathrm{x_n}$ eventually leave the interval [0, 1] and $\mathbf{x_n}$diverge for almost all initial values of $\mathbf{x_{n=0}}$. These phenomenon are illustrated in bifurcation diagram in Fig. 3. The different region of chaos for r between 3.57 and 4 are shown in Fig. 4 by plotting the Lyapunov exponents λ with *r*. The expression of Lyapunov exponent for the orbit starting at $x_{n=0}$ is given by

$$\boldsymbol{\lambda = \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1} ln\left|\acute{f}(x_i)\right|}$$
(2)

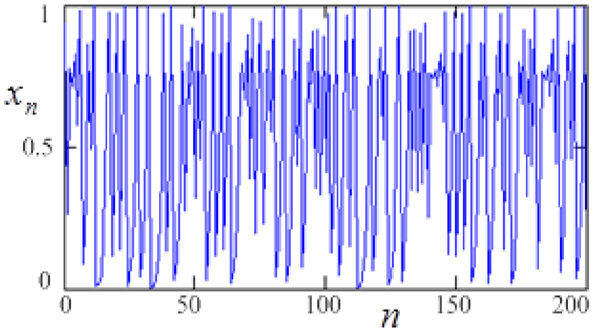

Fig. 1. Chaotic behaviour of state variable x_n with number of iteration (*r* =3.9).

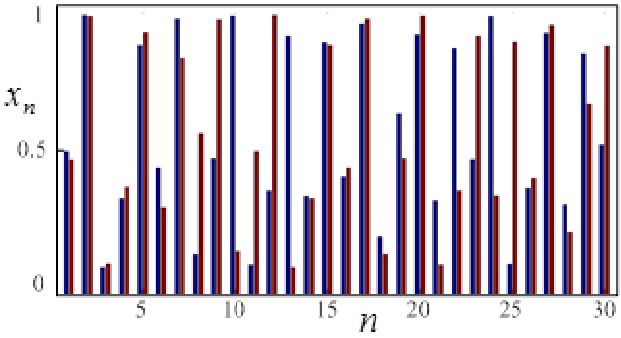

Fig. 2.Initial conditions sensibility test (*r* =3.9).

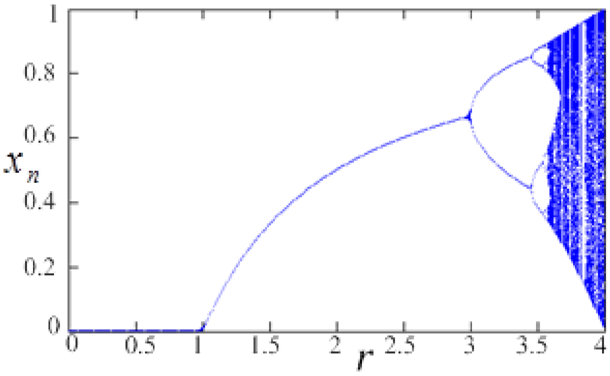

Fig. 3. Bifurcation diagram of logistic map.

OPCL coupling scheme

The OPCL coupling mechanism is described briefly in this section for the sake of completeness. The OPCL coupling [14, 15] was used earlier for complete synchronization of identical Oscillators and identical complex networks. To describe the coupling mechanism, we define a driver system of *n* dimensional map as,

$$\mathbf{x_{i+1} = f\big(x_{i,}\mu\big) + \Delta f(x_i,\mu), x_i \in R^n} \qquad (3)$$

where, $\mathbf{\Delta f(x_i)}$contains mismatch parameters. The system (3) drives an identical driven system along with coupling term $\mathbf{D(X_i, Ax_i)}$ is defined as

$$\mathrm{X_{i+1} = f\big(X_{i,}\mu\big) + D(X_i, Ax_i), X_i \in R^n} \qquad (4)$$

To achieve a goal of amplification the state variable $\mathbf{X_i = Ax_i}$, where $\mathbf{A}\,(= \mathbf{a_{jk}})$ is a real $(\mathbf{n}\times\mathbf{n})$matrix,μ is the parameter and *i* is the number of iteration. The coupling term $\mathbf{D(X_i, Ax_i)}$ is defined by

$$\mathbf{D(X_i, Ax_i) = \ Ax_{i+1} - f(Ax_i, \mu) + [H - JF(Ax_i)](X_i - Ax_i)}. \qquad (5)$$

Where $\mathbf{JF}$ is the Jacobian of $\mathbf{f\big(x_{i,}\mu\big)}$ and $\mathbf{H}\,(= \mathbf{h_{jk}})$ is an arbitrary constant$(\mathbf{n}\times\mathbf{n})$Hurwitz matrix whose eigenvalues must lie inside the unit circle on the complex plane for a stable synchronization.The error signal of the coupled system can be written as $\mathbf{e_i = (X_i - Ax_i)}$, and $\mathbf{f\big(X_{i,}\mu\big)}$ can be expanded in Taylor series as

$$\mathrm{f\big(X_{i,}\mu\big) = f(Ax_i, \mu) + JF(Ax_i)\big(X_i\text{-}Ax_i\big) + \cdots} \qquad (6)$$

Recalling up to the first order terms of (6) and replacing in (4), we get the error dynamics $\mathrm{e_{N+1} = H^N e_0}$, where *N* is the number of iteration. Now as *H* is real matrix its eigen values are either real or complex conjugate pairs. The error $e_N \to 0\ as\ N \to \infty$ if the parameter of the *H* matrix is so preferred that its eigenvalues all lie inside a unit circle. This indicates complete synchronization between driver and driven systems for proper selections of the matrices *A* and *H*.

In this paper we have taken one dimensional logistic map with mismatch as a driver system is given by,

$$\mathbf{x_{i+1} = \ \mu x_i(1 - x_i) + \ \Delta\mu x_i(1 - x_i)} \qquad (7)$$

The corresponding driven system according to OPCL coupling is written as,

$$\mathbf{X_{i+1} = \mu\, X_i\,(1 - X_i) + a_{11}\,(\mu + \ \Delta\mu)x_i\,(1 - \ x_i) + (h_{11} - \ \mu + 2\mu a_{11}x_i)(X_i\ - \ a_{11}X_i) - \mu a_{11}x_i\,(1 - a_{11}x_i\,)} \qquad (8)$$

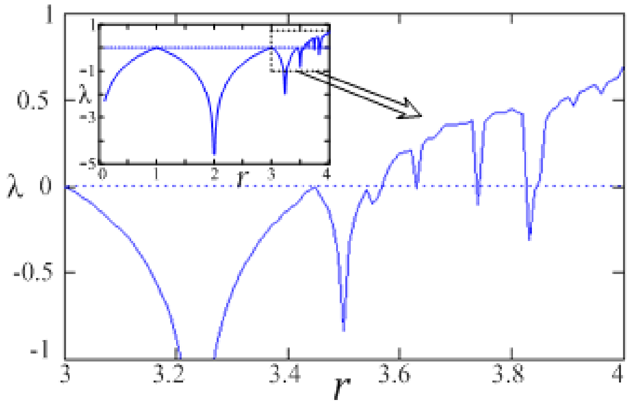

Fig. 4. Lyapunov exponent of logistic map.

The proposed communication scheme

The basic requirements for secure communication are to generate and synchronization of chaos between two trans-receivers separated in space. In the proposed scheme we have used two microcontrollers ATMEGA 16 and discrete electronic components for driver and driven systems. In driver system, a simple logistic map is simulated in microcontroller to generate the chaotic signal. On the other hand in driven system, a synchronizing scheme based on OPCL coupling is implemented in another microcontroller. A brief description of OPCL coupling is given in previous section. The microcontroller ATMEGA16 has suitable features including 16 KB of in-system programmable flash with Read-While-Write capabilities, 512 Bytes EEPROM, 1 KB SRAM, 32 general-purpose I/O lines, 32 general-purpose working registers, a JTAG interface for boundary-scan on-chip debugging support and programming architecture.

The microcontroller is programmed with the logistic map for driver system and driven system is programmed with OPCL coupling mechanism to generate the chaotic sequences and its synchronization respectively for different initial conditions and parameter values. The program is written in Bascom-AVR language. When both the system runs simultaneously then after a few iterations both the systems become synchronized by OPCL coupling rule. The driver and driven systems are programmed in such a way, so that, when the difference between these two chaotic sequences will be zero, at that moment (*i*-th iteration) the information signal from outside of the microcontroller of driver system will scan through analog pin of ATMEGA16. This analog information signal (modulating signal) should be in the range of 0-5Volt and each scan value will be converted into an8-bits digital data which is equivalent to a decimal number in the range 0-255. In general, the driver and driven systems generates chaotic sequences of fractional numbers. At synchronized condition the chaotic sequence (at (*i*+1)-th iteration) of the driver system is multiplied by 100 to get the integer decimal value and thereafter it execute logical XOR operation with the externally scan data. This 8-bits XORed data is modulated signal which has been communicated to the driven system in serial port. The microcontroller in the driven system received the data and perform XOR operation with its generated chaotic sequence at (*i*+1)-th iteration multiplied by 100. Next, this XORed data is converted into pulse width modulation (PWM) and taken output from the specified PWM port (D.5) from the microcontroller and converted into analog value using low pass filter to get back the information signal. But the synchronized condition between driver and driven are shown by taking digital data from microcontroller and converting into analog signal using DAC 0808.The sequence of all the logical steps of driver and driven systems are represented in flowchart in Fig. 5. The proposed algorithm is verified through simulation experiment and hardware electronic experiment.

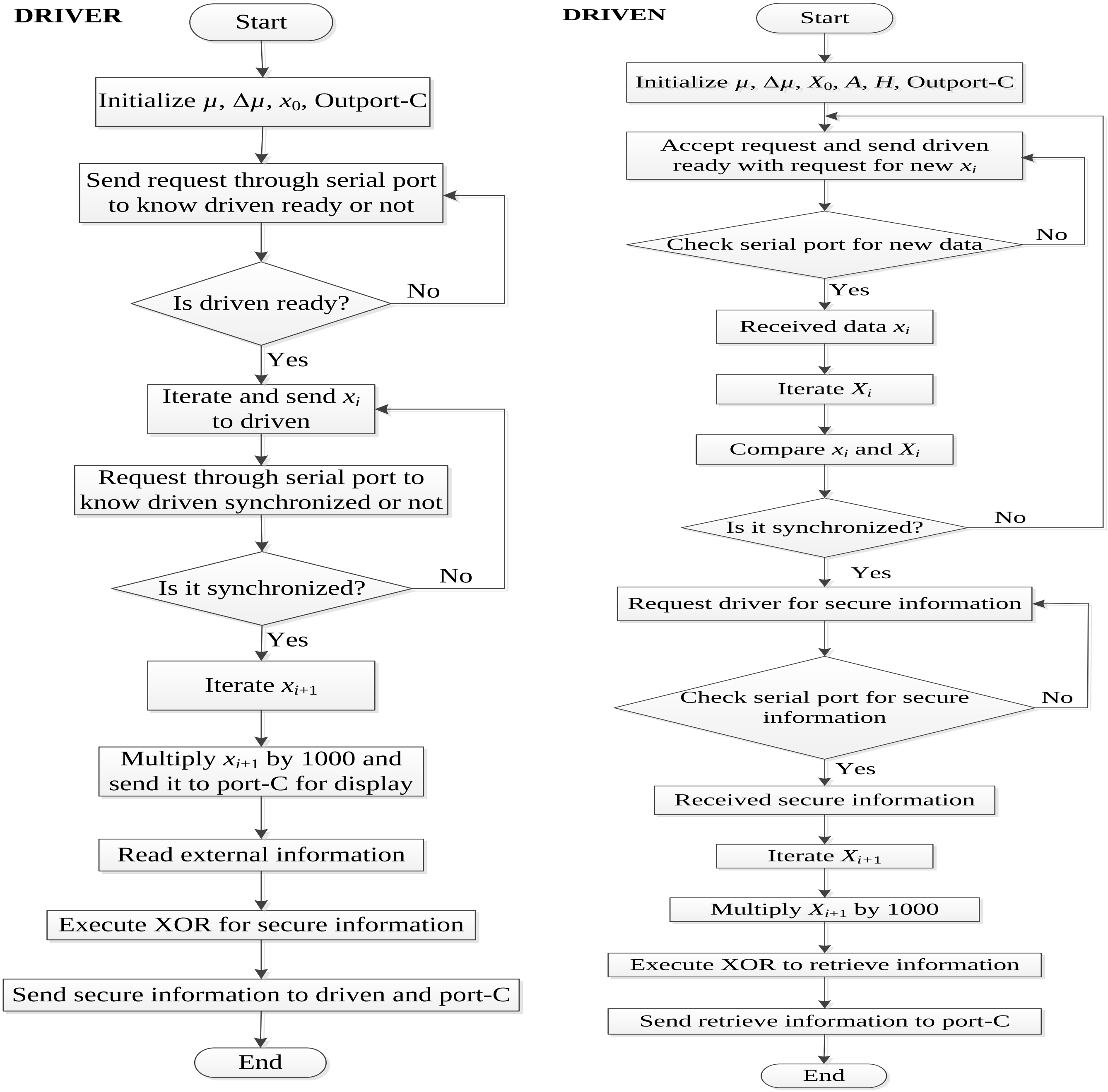
DRIVER
Start
Initialize μ, $\Delta\mu$, x_0, Outport-C
Send request through serial port to know driven ready or not
Is driven ready?
No
Yes
Iterate and send x_i to driven
Request through serial port to know driven synchronized or not
Is it synchronized?
No
Yes
Iterate x_{i+1}
Multiply x_{i+1} by 1000 and send it to port-C for display
Read external information
Execute XOR for secure information
Send secure information to driven and port-C
End
DRIVEN
Start
Initialize μ, $\Delta\mu$, X_0, A, H, Outport-C
Accept request and send driven ready with request for new x_i
Check serial port for new data
No
Yes
Received data x_i
Iterate X_i
Compare x_i and X_i
Is it synchronized?
No
Yes
Request driver for secure information
Check serial port for secure information
No
Yes
Received secure information
Iterate X_{i+1}
Multiply X_{i+1} by 1000
Execute XOR to retrieve information
Send retrieve information to port-C
End

Fig. 5. Flowchart for driver and driven systems.

Experimental results

The proposed communication scheme has been verified through simulation and hardware experiment. The circuit diagram of the simulation experimental is shown in Fig. 6 and it is simulated in PROTEUS software. Both the microcontrollers used in this experiment (driver and driven system)are programmed in Bascom-AVR language for different initial conditions and parameter values based on the flowchart given in Fig. 6 and OPCL coupling scheme of logistic map. An input sinusoidal signal is taken as the information signal for communication purpose. The crystal clock frequency of both the microcontrollers is set on 8MHz for testing purpose. Initially, we have taken different initial conditions $\mathbf{x} = \mathbf{0.32}$ for driver and X = 0.30 in driven system to verify the system responses and after certain iterations both the value of the state variables are equal (up to four decimal places) which indicates complete synchronization between driver and driven systems as shown in Fig. 7. Under synchronized condition both the state variables *x* and *X* are varies in similar fashion as indicated in Fig. 7. The variation of *X* with *x* indicates a straight line in Fig. 8, which confirmed the synchronization between two systems. Here the input information signal (sine wave) and the modulated state variable of driver are shown in Fig. 9. This modulated signal is transmitted to the driven system through serial port and driven system demodulated it by executing XORed operation between received signal and its state variable *X*. Figure 10 shows the input information signal (blue) and demodulated signal (red). The same experiment is also performed in hardware circuit by taking ATMEGA16 PCB and other electronic ICs as shown in Fig. 11. The input information signal (sine wave) and the recovered signal from the driven system is shown in Fig. 12. This figure confirmed the validity of the communication scheme.

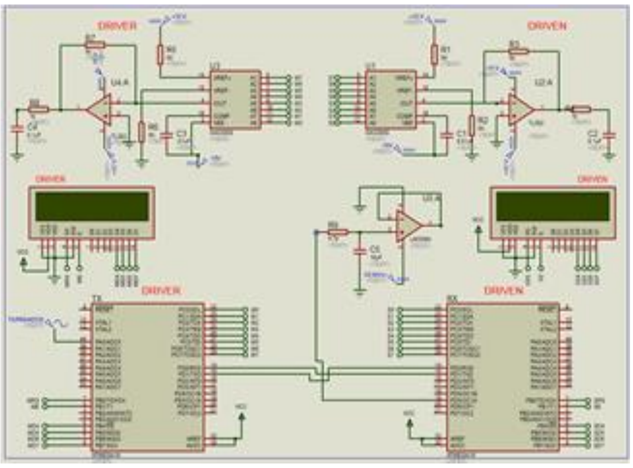

Fig. 6.The circuit diagram of the simulation experimental in PROTEUS software.

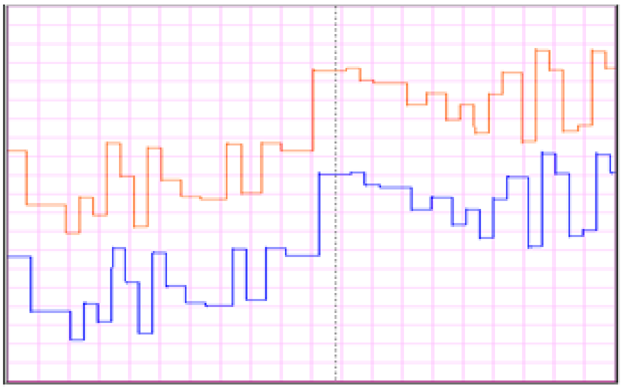

Fig. 7. State variables *x* (driver red) and *X* (driven blue) in time domain view under complete synchronization.

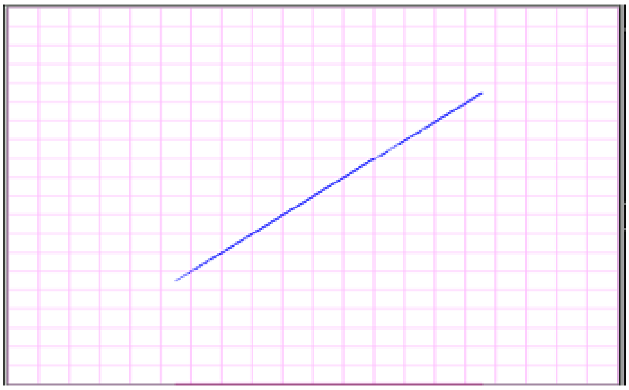

Fig. 8.Phase plane plot of State variables *x* (driver) verses *X* (driven) under complete synchronization.

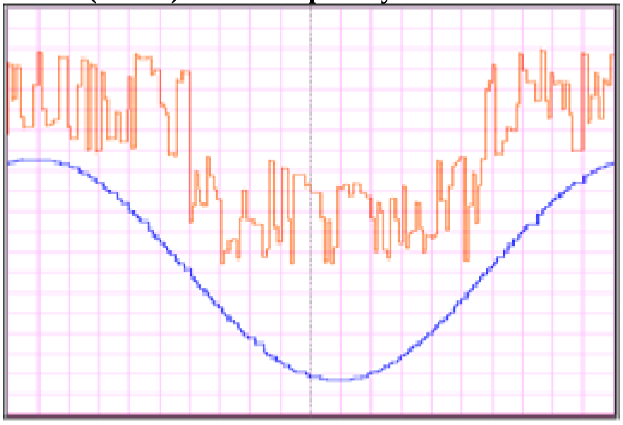

Fig. 9.The input information signal (sine wave) and the modulated state variable of driver system.

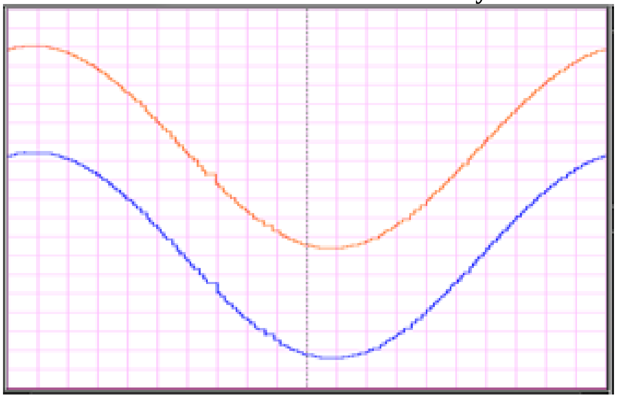

Fig. 10.The input information signal (blue) and demodulated information signal (red).

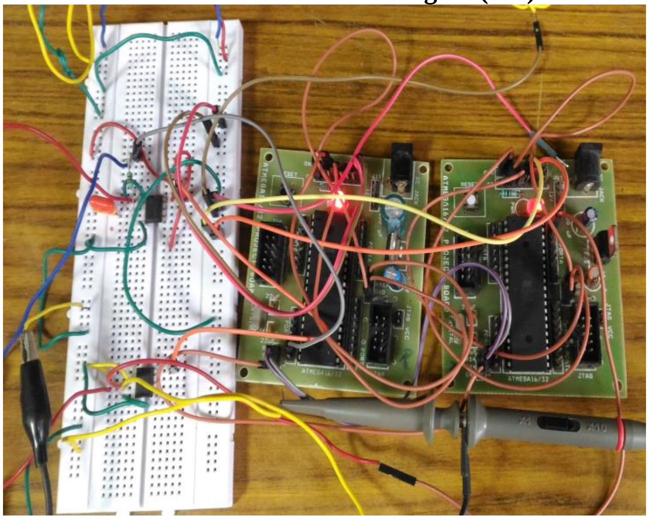

Fig. 11. The hardware electronic experimental setup using ATMEGA16 microcontroller.

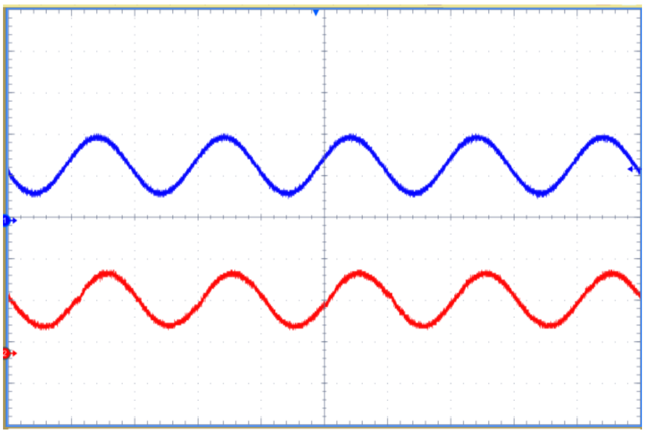

Fig. 12.The hardware experimental results: input information signal (red) and recovered signal from driven system (blue); x-axis: 500ms/div and y-axis: 0.5V/div.

Conclusions

We have presented a simple discrete chaotic system and its synchronization by implementing OPCL coupling theory using microcontroller ATMEGA 16.A secure communication scheme through chaos masking using two microcontroller is demonstrated in digital domain. The proposed discrete synchronization technique and secure communication scheme are verified through simulation and hardware experiment.

References

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

[2]. M. Zapateiro, De la Hoz, L. Acho and Y. Vidal, "A modified Chua chaotic oscillator and its application to secure communication", "Applied Mathematics and Computation" vol. 247, pp.712-722, Jul 2014.

[3]. L. Acho, "A discrete-time chaotic oscillator based on the logistic map: A secure communication scheme and a simple experiment using Arduino", Journal of the Franklin Institute vol.352, pp. 3113-3121, Aug 2015.

[4]. M. A. Murillo-Escobar, et al., "A novel symmetric text encryption algorithm based on logistic map", Int. Conf. on Communication, Signal Processing and Computers, Honolulu, Hawaii, USA, February 2014.

[5]. M. Kar, M. K. Mandal and D.Nandi,"Bit-plane Encrypted Image Cryptosystem using chaotic quadratic and cubic maps",IETE Technical Review vol.33, pp.651-661, Feb 2016.

[6]. A Pande and J. Zambreno, "A chaotic encryption scheme for real time embedded systems: design and implementation", Telecommunication Systems vol.52, pp. 551-561, Feb 2013.

[7]. G.C. Wu and D. Baleanu, "Discrete fractional logistic map and its chaos", Nonlinear Dynamics vol.75, pp.283-287, Jan 2014.

[8]. I Cicek, A. E. Pusane and G. Dundar, "A novel design method for discrete time chaos based true random number generators", VLSI Journal vol.47, pp.38-47, Jan 2014.

[9]. B. Jovic and C. P. Unsworth, "Fast synchronisation of chaotic maps for secure chaotic communications", Electronics Letters vol.46, pp. 49-50, Jan 2010.

[10]. M.K. Mandal,G.D.Banik,D.Chattopadhyay and D.Nandi, "An image encryption process based on chaotic logistic map",IETE Technical Review vol.29, pp.395-404, 2012.

[11]. W. T. Gibson and W. G. Wilson, "Individual-based chaos: extensions of the discrete logistic model", Journal of Theoretical Biology vol.339, pp.84-92, Dec 2013.

[12]. A J G. Radwan, "On some generalized discrete logistic maps", Journal of Advanced Research vol.4, pp.163-171, Mar 2013.

[13]. S.H.Strogatz,"Nonlinear dynamics and chaos with applications to Physics, Biology, Chemistry and Engineering" , New York, 1994.

[14]. I Grosu, E. Padmanaban, P. K. Roy and S. K. Dana, "Designing Coupling for Synchronization and Amplification of Chaos",Phys. Rev. Lett.vol.100,pp. 234102(1-4), Jun 2008.

[15]. P. Pal, S. Debroy, M. K. Mandal, and R. Banerjee, "Design of coupling for synchronization in chaotic maps", Nonlinear Dynamics vol.79, pp. 2279-2286, Mar 2015.