Experimental Realization of 2D Chaos Synchronization using Microcontroller TMEGA 16 and applied in a secure PIN transaction

Anup Kumar Das, Mrinal Kanti Mandal

Abstract— In this paper the synchronization scheme of the 2D chaotic Henon map and personal identification number (PIN) encryption and decryption method has been implemented by microcontroller ATMEGA16. Two different systems are taken in two different position one is driver microcontroller and another is driven microcontroller for these synchronization purposes. Two chaotic maps at parameter mismatch condition have been synchronized by open-plus-closed-loop (OPCL) coupling scheme and used in a secure PIN transaction. The proposed technique is simulated and hardware circuit is also implemented successfully.

Keywords— chaos, OPCL coupling, microcontroller, PIN

1. INTRODUCTION

In current years, the synchronization of chaos and its application in different areas is an important research topic [1, 2]. In continuous chaotic systems, lots of synchronization techniques have been described in different literature [3-5], but in discrete system the synchronization of chaos and its hardware application is very rare. For this intention, we are interested to establish the synchronization of chaos in discrete system and its application in secure PIN transaction. Different kind of synchronization technique is available in the literature like diffusive, mean field, time delay, conjugate coupling etc. And also a variety of synchronization type, namely complete synchronization (CS), anti-synchronization (AS), generalized synchronization (GS), phase synchronization (PS), anti-phase synchronization (APS), lag synchronization (LS) are described by scientists in various fields of applications [6]. The OPCL coupling scheme of chaos synchronization for secure communication is the important research interest in this time [6-7]. Generation of chaos in two different positions cannot be equal due to any mismatch parameter or for different initial condition, due to this cause OPCL coupling is used for chaos synchronization in two different positions [8-9] and applied in a secure PIN transaction. In this paper our goal is to realize CS, AS, and GS for 2D Henon chaotic map at parameter mismatch condition by two different microcontrollers ATMEGA16 are situated in different position. Next, at synchronized condition PIN number will be scan from driver microcontroller and execute encryption before sending it to the driven or server microcontroller, on the other hand, the server microcontroller decrypts the encrypted PIN to identify the originality. This paper is organized as follows: In section II we describe the coupling theory, section III describes Implementation of the synchronized 2D Henon map by microcontrollers, Section IV describes the proposed technique of PIN encryption and decryption, Section V describes some simulation and experimental results and finally section VI gives the conclusion.

Revised Version Manuscript Received on 30 May, 2018.

Anup Kumar Das, Department of Electronics and Instrumentation, Dr. B. C. Roy Engineering College, Durgapur, India. (E-Mail: anupkumardas29@yahoo.com)

Mrinal Kanti Mandal, Department of Physics, National Institute of Technology Durgapur, Durgapur, India. (E-Mail: mrinalkanti.mandal@phy.nitdgp.ac.in)

2. OPCL COUPLING THEORY

This section summarizes the synchronization method describes in Reference [6, 7], where concentration is focused on the OPCL coupling scheme. The OPCL coupling was used earlier for CS in identical Oscillators and synchronization of identical complex networks. To describe the coupling to mismatch systems, we define a driver system of n dimensional maps as,

$$x_{i+1} = f(x_{i,}\mu) + \Delta f(x_i, \mu), \quad x_i \in R^n \tag{1}$$

Where, $\Delta f(x_i)$contains mismatch parameters. The system of (1) drives a response system defined as

$$X_{i+1} = f(x_{i,}\mu), \quad X_i \in R^n \tag{2}$$

To achieve a goal of amplification the state variable$X_i = Ax_i$, where $A = (a_{ij})_{n\times n}$ is a real matrix, μ is the parameter and i is the number of iterations. The driven system is given by,

$$X_{i+1} = f(X_{i,}\mu) + D(X_i, Ax_i), \tag{3}$$

Where the coupling term $D(X_i, Ax_i)$ is defined by

$$D(X_i, Ax_i) = Ax_{i+1} - f(Ax_i, \mu) + [HJF(Ax_i)](X_i - Ax_i \quad), \tag{4}$$

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

$$f(X_{i,}\mu) = f(Ax_i, \mu) + JF(Ax_i)(X_i - Ax_i) + \cdots \tag{5}$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Recalling up to the first order terms of (5) and replacing in (3), we get error dynamics $e_{N+1} = H^N e_0$, where N is the number of iterations. Now, as H is a real matrix its eigenvalues 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 synchronization between driver and driven systems. For proper selections of the matrices A and H, complete synchronization (CS), anti-synchronization(AS) and amplification (GS) can be achieved as described below using a 2D Henon map.

A. Synchronization of 2D Henon map

The driver system of 2D Henon map is given by,

$$x_{i+1} = \mu_1 - x_i^2 + \mu_2 y_i + \Delta\mu_1 + \Delta\mu_2 y_i \quad (6a)$$

$$y_{i+1} = x_i \quad (6b)$$

The driven system according to OPCL coupling [7] is given by,

$$X_{i+1} = -X_i^2 + \mu_2 Y_i + a_{11}(\mu_1 - x_i^2 + \mu_2 y_i + \Delta\mu_1 + \Delta\mu_2 y_i) + a_{12}x_i + (a_{11}x_i + a_{12}y_i)^2 - \mu_2(a_{21}x_i + a_{22}y_i) + \{h_{11} + 2(a_{11}x_i + a_{12}y_i)\}(X_i - a_{11}x_i - a_{12}y_i) + (h_{12} - \mu_2)(Y_i - a_{21}x_i - a_{22}y_i)$$

(7a)

$$Y_{i+1} = X_i + a_{21}(\mu_1 - x_i^2 + \mu_2 y_i + \Delta\mu_1 + \Delta\mu_2 y_i) + a_{22}x_i - a_{11}x_i - a_{12}y_i + (h_{21} - 1)(X_i - a_{11}x_i - a_{12}y_i) + h_{22}(Y_i - a_{21}x_i - a_{22}y_i)$$

(7b)

The above equations (6a)–(7b) are implemented in microcontrollers and digital to analog conversion circuit using the Proteus simulation software and hardware and it is shown in Fig. (1) And the block diagram is represented in Fig. 2. The simulation results are shown in Figs. 3-5 with the parameter values of $\mu_1 = 1.8$, $\mu_2 = -0.005$, $\Delta\mu_1 = 0.1$, $\Delta\mu_2 = 0.0005$ and $H = [0.95{,}0; 0{,}0.95]$. Figure 3(a) shows the CS between driver and driven systems and Fig. 3(b) represents the variation of $x_i$with X_i.Figure 4(a) shows the AS between driver and driven systems and Fig. 4(b) represents the variation of x_i with X_i .5(a) shows the GS between driver and driven systems and Fig. 5(b) represents the variation of $x_i$with X_i.

B. Figures

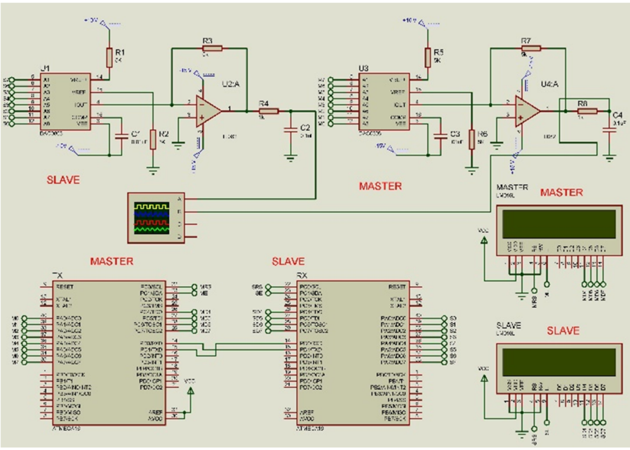

Fig.1 Simulation circuit using the Proteus software.

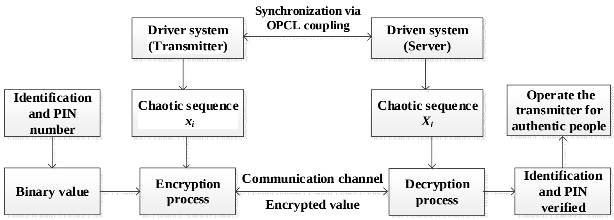

Fig. 2 Proposed block diagram of PIN transaction.

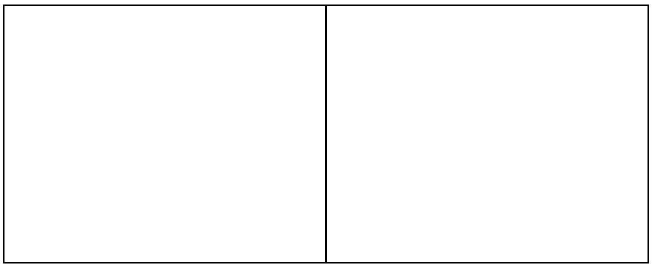

Fig. 3(a) The successive iterates of x_i(red) and X_i(black) for $A = [1, 0; 0, 1]$. 3(b) $X_i$vs. x_i plot

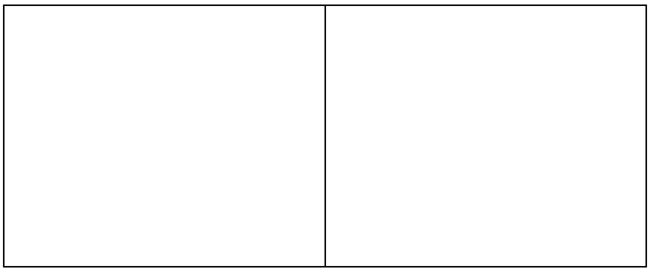

Fig. 4(a) The successive iterates of x_i(red) and X_i (black) for $A = [-1, 0; 0, -1]$. 4(b)$X_i$vs. $-x_i$ plot

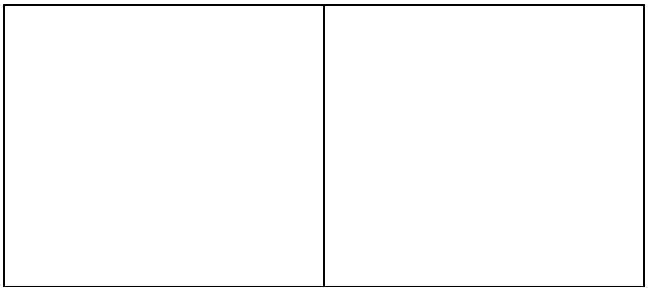

Fig. 5(a) The successive iterates of x_i(red) and X_i(black) for $A = [2, -1; 2, 1]$. 5(b) $X_i$vs. $(2x_i - y_i)$ plot

3. THE CIRCUIT IMPLEMENTATION

The proposed, implemented circuit for synchronization of the chaotic sequences according to the equations (6a)-(7b) is shown in Fig. (1).This prototype circuit consists of two microcontrollerATMEGA16 for driver and driven system, digital to analog converter DAC0808 and operational amplifier TL082. Except microcontroller, the remaining circuit components are used to latch the 8-bit chaotic sequence from the microcontroller and it converts into measurable voltage. MicrocontrollerATMEGA16 has suitable features including 16 KB of in-system programmable flash with Read-While-Write capabilities, 512

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Bytes EEPROM, 1 KByte SRAM, 32 general-purpose I/0 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 synchronized 2D Henon map illustrated in equations (6a)-(7b) to generate the chaotic sequences. The program is written in BASCOM AVR language. The microcontroller evaluate the fractional output value of the inbuilt program of the 2D Henon map. These fractional value is multiplied by 100 to get the suitable integer and if the number is negative, then its 2's complement form will be generated and send it at the output port of the Microcontroller. The output of the microcontroller generates the chaotic sequence between 0 and 255 because it provides 8-bits digital output. Here the output port of the microcontroller is connected to DAC to get the suitable output voltage. Two ports of ATMEGA16 Microcontrollers, port-B (Driver) and port-B(Driven) are used here to take the output data. The output data are separately converted into suitable analog voltage with the help of ICs, the DAC 0808 and TL082.The chaotic voltage pattern and synchronization are shown in the result section. Now based on this OPCL synchronization, secure PIN transaction technique is described below.

4. PROPOSED TECHNIQUE

Here the driver microcontroller act as a transmitter of identification number and PIN number and driven microcontroller act as a server microcontroller which has been already stored with the identification number and PIN number of known sets or authentic sets of people. At first, 255 different Identification and PIN number of known people already stored in two different lookup tables on the server or driven microcontroller. Here driver and driven microcontroller is programmed to 2D Henon chaotic map with an OPCL coupling scheme in BASCOM AVR language platform. To access the server microcontroller, Tx and Rx pin are connected with Rx and Tx pin with driver/transmitter microcontroller with connecting wire of both the driver and driven microcontroller of PIN transaction. The program is written in this way, at first the parameter mismatch condition both the transmitter and server microcontroller running simultaneously, when after few iterations it has been synchronized by the opcl coupling method, then portB.1 pin of transmitter microcontroller has been high or glow a LED(red), it means now it is allowable to entering the Identification number(0-255 different nos.) from port A of transmitter microcontroller within 15 second, after entering the authentic identity number, driver microcontroller scan the port A to get the number and after receiving this value(say I) it has been exclusive or(XOR) logical operation with the last chaotic number(xi)generated in driver multiplied by 100 to get the integer value(say C) and the new encrypted value (E)[(E)=(C) XOR (I)] is now ready to send in server, after receiving the encrypted value by serial port(Rx pin) the server has been done decryption process by same logical operation to get the identification number[(C) XOR (E)=(I)] because both the system are synchronized so the last chaotic number(Xi) in server must be same as (xi) transmitter. Now this identification number (I) has been found from look-up table no.1 (which already stored previously from authentic people) by the comparison statement in server microcontroller. If the identification number (I) matches with look-up table no.1 number (I) then the only server sends the signal to transmitter to get the PIN from port A within 15 second by port B.2 pin high or glow LED(green) signal otherwise port B.1 has been high for waiting new identification number. Now suppose port B.2 pin high (after matching the identity number) then within 15 second PIN (say P) has been entered in the port A of transmitter microcontroller and then the same way encryption has been done by logical operation with the multiplied by 100 (Y) value of 2D Henon chaotic iterative value (yi) [(En)=(P) XOR (Y)]. After receiving the encrypted value (En) from a transmitter to server microcontroller same decryption process has been done to get the PIN (P), and then it has been found the Pth position from look-up table no.2 (which already stored previously from authentic people) by comparison method in the server. If the PIN matches, then the server sends a signal to the transmitter as port B.3 pin high to operate ATM/ gate open/Motor on etc.

A. Step wise algorithm

Step 1. Driver and driven or user and server microcontrollers run simultaneously.

Step 2. These two will be synchronized after a few iterations by OPCL coupling.

Step 3. At synchronized condition port B.1 pin high or glow LED of user/driver microcontroller, now it scans port A (for 15 second) for a user id number.

Step 4. After completion of scanning data value Di (0-255) has been encrypted with the chaotic integer value xi (chaotic value generated in driver/user microcontroller multiplied by 100, i.e. xi XOR Di = Ei and sends through the Tx pin of sever microcontroller.

Step 5. After receiving the encrypted value Ei through the Rx pin of the server then it has been applied the reverse process of decryption (Xi XOR Ei = Di) to get the user id value, because xi and Xi is same.

Step 6. This Di value compares with the lookup table-1, [where the user id data values previously stored in server from authentic people].

Step 7. After successful authentication of server/driven microcontroller send to allow the request for a PIN to the user/driver microcontroller as port B.2 pin high or glow LED indication and again port A scan (for 15 second).

Step 8. Again, authentic people put the PIN (0-255) value Pi in driver system and encryption process has been done with the chaotic integer value yi [yi XOR Pi = Ci] and send it to the server.

Step 9. After receiving, the encrypted PIN value on the server the reverse technique applied (Yi XOR Ci = Pi) to get the Pi data value and now find Pi th value stored in lookup table-2 and compare with user id number for authentic the right person.

Step 10. If a PIN has been matched then port B.3 pin high or glow LED to operate the system.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

5. RESULTS

This section presented the Proteus simulation results in tabular form along with the hardware experimental results for the driver and driven system based on microcontroller ATMEGA 16 with additional circuitry described in Section III. Tables-I provided the values for the first five iterations of the driver and driven systems for CS on the 2D Henon map. The hardware experimental results recorded using TEKTRONICS Oscilloscope are shown in Fig. 6 for complete synchronization (CS) between driver (lower tracing- green colour waveform) and driven system (upper tracing – pink colour waveform) of 2D Henon map for CS.

Table-I. Simulated and Experimental values of x_i and X_i for CS (initial value of x_i=0.4, y_i=0.6and X_i=0.4, Y_i=0.6):$\mu_1 = 1.8$,$\mu_2 = -0.005$, ,$\Delta\mu_1 = 0.1$, $\Delta\mu_2 = 0.0005$,$H = [0.95, 0; 0, 0.95]$ and $A = [1, 0; 0, 1]$

Simulation results				Experimental results
i	x_i×100 port B (Driver)	X_i×100 port B(Driven)	Equivalent Hex value Port B (driver/driven)	Equivalent Hex value port B (driver/driven)
1	173.72	173.72	AD	AD
2	-112.00	-112.00	90	90
3	63.77	63.77	3F	3F
4	149.83	149.83	95	95
5	-34.77	-34.77	DE	DE

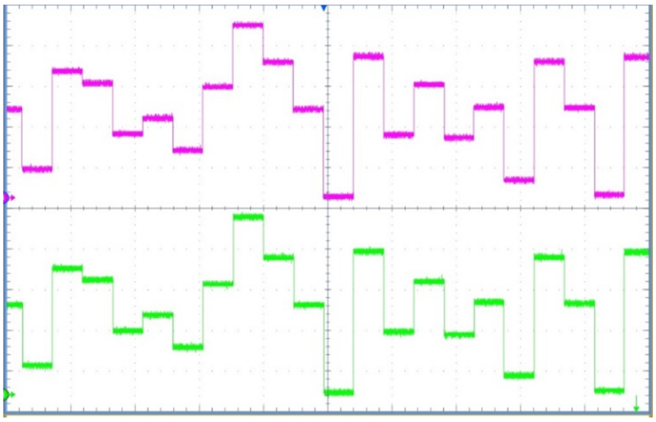

Fig.6. The Oscilloscope output of x_i(Green) and X_i (Pink) for $A = [1, 0; 0, 1]$ under complete synchronization. Amplitude: 500mv/div, Time: 500ms/div.

6. CONCLUSION

In this paper an experimental realization of the OPCL coupling technique using microcontroller has been proposed. Complete synchronization, anti-phase Synchronization and generalized synchronization can be achieved in a precise and organized way under parameter mismatch condition from this technique. The OPCL coupling scheme for discrete maps are very fast therefore the scheme is suitable to study the synchronization behavior of a large number of chaotic maps and therefore microcontroller is suitable for this purpose. The hardware circuit is verified for secure PIN transaction purposes.

REFERENCES

1. 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, August 2015.
2. A. Argyris, et al., "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature (London), vol. 438, pp. 343-346, November 2005.
3. T. L. Carroll, L. M. Pecora, "Synchronizing chaotic circuits," IEEE Trans. Circuits and Syst., vol. 38, pp. 453-456, April 1991.
4. G. Grassi, D. A. Miller, "Theory and experimental realization of observer-based discrete-time hyperchaos synchronization," IEEE Trans. Circuits Syst. I., vol. 49, pp. 373-378, August 2002.
5. D. A. Miller, G. Grassi, "Experimental realization of observer-based hyperchaos synchronization," IEEE Trans. Circuits Syst. I., vol.48, pp. 366-374, March 2001.
6. I Grosu, E. Padmanaban, P. K. Roy, S. K. Dana, "Designing Coupling for Synchronization and Amplification of Chaos," Phys. Rev. Lett., vol. 100, pp. 234102, June 2008.
7. 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, March 2015.
8. C. K. Volos, "Chaotic random bit generator realized with a microcontroller," Journal of Computations & Modelling, vol. 3, pp. 115-136, November 2013.
9. A. K. Das, S. Hazra, M. K. Mandal, "RGB image encryption using microcontroller ATMEGA 32," Microsystem Technologies, published online: 1st June, 2018. https://doi.org/10.1007/s00542-018-3980-5

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication