Implementation of a secure digital chaotic communication scheme on a DSP board

Rupak Kharel*, Krishna Busawon*, Woihida Aggoune**, Z. Ghassemlooy*
* School of Computing, Engineering & Information Sciences, Northumbria University, UK
** Equipe Commande des Systèmes (ECS), ENSEA, France
rupak.kharel@unn.ac.uk

Abstract— **In this paper, a new a secure communication scheme using chaotic signal for transmitting binary digital signals is proposed and which is then implemented on a Digital Signal Processor (DSP) board. The method uses the idea of indirect coupled synchronization for generating the same keystream in the transmitter and receiver side. This chaotic keystream is applied to encrypt the message signal before being modulated with a chaotic carrier generated from the transmitter. Discrete chaotic maps, 3D Henon map and Lorenz system are used as transmitter/receiver and key generators respectively. The overall system is experimentally implemented in the TMS320C6713 DSK board using code composer and Simulink showing the successful message extraction thus proving the feasibility of the system in the DSP board.**

I. INTRODUCTION

In the last decade or so, using chaotic signals for achieving secure communication have attracted lots of attention amongst researchers because of the inherent properties of chaotic signals such as being aperiodic, broad spectrum, low autocorrelation, etc. Even though chaotic systems are very sensitive to initial conditions, researchers have provided methods of synchronizing two chaotic systems thus giving an opportunity to use them in communication [1-5]. Since, a signal always has to be transmitted from one oscillator to another to achieve synchronization, the driving signal can be used as message modulating transmitting signal.

In fact, a number of different methods of transmitting message signal using chaotic systems have been proposed, such as chaotic masking, chaotic modulation, chaotic shift keying, etc [5]. Various other modified methods have also been proposed [6-9]. However, almost all of the proposed methods are unsuccessful of providing the security that it claims to provide [5, 10-15]. Methods such as nonlinear dynamics forecasting, return maps, spectral method, artificial neural network (ANN) methods, etc. have been used to attack the available methods. To come up with a method, that is not vulnerable to one or other attack methods is still a challenge for the communication system designer.

In this paper, we try to address those issues and propose a potentially secure chaotic communication method for transmitting digital signals. Chaotic systems are also very sensitive to parameter mismatches and when implemented on analog electronic components, temperatures fluctuations and parameter fluctuations in the analog circuits can be major issues in the performance of the system. Also, practical implementation of the system on analog electronic components can be hard to realize offering limited flexibility and ultimately being costly. Therefore, digital signal processing seems to be a nice option that will provide flexibility in the design logic and the temperature and parameter discrepancies will no longer be an issue. Field programmable gate array (FPGA) or DSP board can be utilized for this purpose. The architecture of either FPGA or DSP board will allow us to implement the system rather efficiently and easily. In this paper, we are using TMS320C6713 DSK DSP board for experimentally verifying the proposed secure method.

In a recent paper [16], a novel idea for secure communication was proposed using continuous-time chaotic systems. It used the idea of implementing encryption algorithm as in [9] but had the novelty of using keystream generated from a different chaotic oscillator rather than the transmitter. As a result, a new type of chaotic synchronization (indirect coupled synchronization) was proven for continuous time system and which was, in turn, applied for the secure communication. This paper follows the same spirit of reasoning as in [16] but in a discrete context such that it can easily be implemented practically on the DSP board. The objective of this paper is to demonstrate experimentally the indirect coupled synchronization for discrete-time chaotic systems and applying it for realising a secure digital communication system.

An outline of this paper is as follows: In Section II, the main methodology of the proposed method is explained and the indirect coupled synchronization is proven. In Section III, implementation of the method will be done using 3D-Henon map and discrete-time Lorenz system. In Section IV, experimental results are shown. Finally on Section V, some conclusions are drawn.

II. MAIN METHODOLOGY

In this section, first the indirect coupled synchronization is proven for a class of discrete-time chaotic systems and then its application for secure communication is proposed.

A. Indirect Coupled Synchronization

Consider the discrete-time dynamical systems described by:

$$(\mathrm{T}):\begin{cases} x(k+1) = Fx(k) + f(y_t(k)) \\ y_1(k) = h_1(x(k)) \\ y_2(k) = h_2(x(k)) \\ y_t(k) = y_1(k) + \phi(m(k), u(k)), \end{cases} \tag{1}$$

where the state $x \in R^n$ with initial condition $x(0) = x_0$. The outputs of the oscillator $y_1 \in R$ and $y_2 \in R$. The functions f, h_1 and h_2 are smooth and $m(k)$ is

the input signal. The signal $y_t \in R$ is the transmitted signal where $\phi(.)$ is a special purpose function of $m(k)$ and $u(k)$ and the function f is a smooth bounded function. The signal $u(k)$ is generated using another chaotic oscillator which is driven by the signal $y_2(k)$, i.e.

$$(\mathrm{A}):\ \begin{cases} z(k+1) = g(z(k), y_2(k)) \\ u(k) = h(z(k)), \end{cases} \tag{2}$$

where $z \in R^q$ (q is not necessarily equal to n), $u \in R$, and h is an analytical function vector of appropriate dimension.

The chaotic oscillator (R) to synchronize with (T) is given by

$$(\mathrm{R}):\ \begin{cases} \hat{x}(k+1) = F\hat{x}(k) + f(y_t(k)) \\ \hat{y}_1(k) = h_1(\hat{x}(k)) \\ \hat{y}_2(k) = h_2(\hat{x}(k)). \end{cases} \tag{3}$$

Finally, the chaotic oscillator (B) to synchronize with (A) is given as

$$(\mathrm{B}):\ \begin{cases} \hat{z}(k+1) = g(\hat{z}(k), \hat{y}_2(k)) \\ \hat{u}(k) = h(\hat{z}). \end{cases} \tag{4}$$

Note that the oscillator (A) and (B) are being driven by signal $y_2(k)$ and $\hat{y}_2(k)$ respectively in order to form some sort of indirect coupling.

We will make the following assumptions:

A1) The matrix F of (T) and (R) is stable.

A2) The function $g(z, w)$ is globally Lipschitzian with respect to z and w. Additionally, there exists a positive constant $0 \le \beta \le 1$ such that $\|g(z(k), w(k)) - g(\hat{z}(k), w(k))\| \le \beta \|z(k) - \hat{z}(k)\|$, for all $k \ge 0$ and all $w \in R$.

Our objective is to show that the oscillator (A) and (B) synchronize with each other even though there is no direct link between them.

In effect, based on the above assumptions, we state the following:

Theorem 1. *Under the Assumptions A1) and A2), we have* $\lim_{k\to\infty} \|x(k) - \hat{x}(k)\| = 0$. *In other words, the receiver (R) synchronizes exponentially with the transmitter (T).*

Proof: Let $\varepsilon(k) = x(k) - \hat{x}(k)$, then the error dynamics between transmitter (T) and receiver (R) is given by:

$$\xi(k+1) = F\xi(k). \tag{5}$$

Since F is stable, it is clear that $\|\xi(k)\| \to 0$ as $k \to \infty$. In other words, the receiver (R) synchronizes with the transmitter (T). This completes the proof of Theorem 1.

***Remark*:** If F is not stable, then we can always design an observer such that the overall error dynamics is stable. The aim here is not to show this synchronization but to show the indirect coupled synchronization, therefore the simplest form of coupled synchronization is employed for (T) and (R).

Theorem 2. *Assume that system (A) and (B) satisfies assumptions A1) and A2), then* $\lim_{k\to\infty} \|z(k) - \hat{z}(k)\| = 0$. *That is, the oscillator (A) synchronizes asymptotically with (B).*

Sketch of proof: Set $\varepsilon(k) = z(k) - \hat{z}(k)$, then the error dynamics between the (A) and (B) is given by:

$$\varepsilon(k+1) = g(z(k), y_2(k)) - g(\hat{z}(k), \hat{y}_2(k). \tag{6}$$

Now, consider the following candidate Lyapunov function:

$$W(k) = \|\varepsilon(k)\|. \tag{7}$$

Then,

$$\begin{aligned} W(k+1) &= \|\varepsilon(k+1)\| \\ &= \|g(z(k), y_2(k)) - g(\hat{z}(k), \hat{y}_2(k))\| \\ &\le \|g(z(k), y_2(k)) - g(\hat{z}(k), y_2(k))\| \\ &\quad + \|g(\hat{z}(k), y_2(k)) - g(\hat{z}(k), \hat{y}_2(k))\| \\ &\le \beta\|z(k) - \hat{z}(k)\| + \gamma\|y_2(k) - \hat{y}_2(k)\| \\ &\le \beta\|\varepsilon(k)\| + \gamma\|\xi(k)\|. \end{aligned} \tag{8}$$

Finally,

$$W(k+1) - W(k) \le (\beta - 1)W(k) + \gamma\|\xi(k)\|. \tag{9}$$

Since from theorem 1, $\|\xi(k)\| \to 0$ as $k \to \infty$, we will eventually have $W(k+1) - W(k) \le 0$.

This completes the proof of Theorem 2.

B. Application to secure communication

Now, the indirect coupled synchronization is used for implementing secure communication. The oscillator (A) and (B) will be used as key generating oscillators such that their outputs will be utilized as keystream for encrypting the message signal. Once, the synchronization is obtained between (A) and (B) using indirect coupling synchronization, the message can easily be decrypted back in the receiver side. This means that the keystream is not required to be transmitted. The digital bits can be modulated into $m(k)$ by using any digital modulation techniques such as pulse amplitude modulation, etc.

III. APPLICATION USING 3D-HENON MAP AND DISCRETE LORENZ SYSTEM

In this section, the performance of the proposed synchronization and method is demonstrated using the

3D-Henon as the transmitter/receiver system and discrete Lorenz system as the key generating oscillator. The 3D-Henon map is defined for transmitter and receiver as [17]:

$$(T):\begin{cases} x_1(k+1) = -by_t(k) \\ x_2(k+1) = 1 + x_3(k) - ay_t^2(k) \\ x_3(k+1) = x_1(k) + by_t(k) \\ y_1(k) = x_2(k) \\ y_2(k) = x_3(k) \\ y_t(k) = y_1(k) + e(m, key), \end{cases} \quad (10)$$

$$(R):\begin{cases} \hat{x}_1(k+1) = -by_t(k) \\ \hat{x}_2(k+1) = 1 + \hat{x}_3(k) - ay_t^2(k) \\ \hat{x}_3(k+1) = \hat{x}_1(k) + by_t(k) \\ \hat{y}_1(k) = \hat{x}_2(k) \\ \hat{y}_2(k) = \hat{x}_3(k), \end{cases}$$

where $a = 1.07$ and $b = 1.03$. The key generating oscillators are represented in discrete Lorenz system as [18]:

$$(A):\begin{cases} z_1(k+1) = z_1(k)z_2(k) - y_2(k) \\ z_2(k+1) = z_1(k) \\ z_3(k+1) = z_2(k) \\ key = d_0 z_3(k), \end{cases} \quad (11)$$

$$(B):\begin{cases} \hat{z}_1(k+1) = \hat{z}_1(k)\hat{z}_2(k) - \hat{y}_2(k) \\ \hat{z}_2(k+1) = \hat{z}_1(k) \\ \hat{z}_3(k+1) = \hat{z}_2(k) \\ \hat{key} = d_0 \hat{z}_3(k). \end{cases}$$

Notice that the oscillator (A) and (B) are being driven by $y_2(k)$ and $\hat{y}_2(k)$ respectively. The encryption function $e(.)$ used is a n-shift cipher algorithm given as: (as used in [9]):

$$e(m, key) = \underbrace{f_1(...f_1(f_1}_{n}(m, \underbrace{key), key),..., key}_{n}), \quad (12)$$

where $f_1(m,key)$ is a non-linear function given by:

$$f_1(m, key) = \begin{cases} m + key + 2h, \text{ for } -2h \le m + key \le -h \\ m + key, \text{ for } -h < m + key < h \\ m + key - 2h, \text{ for } h \le m + key \le 2h, \end{cases}$$

with h being an encryption parameter which is chosen such that m and key lie within the interval $[-h,h]$.

Once the keystream generator (A) synchronizes asymptotically with generator (B), the message $m(k)$ can be recovered using a decryption rule corresponding to the encryption rule and which is given by:

$$m_r(k) = e^{-1}\left(\hat{e}(m, key)\right) = \underbrace{f_1(...f_1(f_1}_{n}(\hat{e}(m, key), \underbrace{-\hat{key}), -\hat{key}),..., -\hat{key}}_{n}),$$

where $\hat{key}$ is the estimated keystream and $\hat{e}(m(k)) = y_t(k) - \hat{y}_1(k)$.

It can easily be seen that Assumption A1) for (T) and (R) holds. After some lengthy calculations it can be shown that assumption A2) is valid for (A) and (B).

In the next section, the proposed technique will be implemented practically using a TMS320C6713 DSK board. The simulation and practical results will be compared.

IV. PRACTICAL IMPLEMENTATION

For implementing the method practically, DSP board is preferred rather than analogue components because of their ease of use and simplicity. In analogue circuit, small changes might account for complete rewiring of hard-wired system but in DSP board, same changes can be accomplished by few lines of code changes in ROM or EPROM of DSP.

Matlab/Simulink Embedded IDE link in combination with Texas instrument (TI) code composer (CCS) is used for rapid prototyping of the system. The DSP board used is DSK TMS320C6713 which is capable of floating point operations with clock speed of 225 MHz and if the proposed system works in this board, it can easily be implemented on any other modern boards for high speed operations.

The proposed model is first realized in Simulink and then converted into assembly code for TMS320C6713 using Simulink and CCS. The data to be transmitted is loaded into the DSP board using real time data exchange (RTDX) and the transmitted signal and extracted data are again loaded from DSP to computer using RTDX.

The encryption parameter h is taken to be 0.02 and the signal $m(k)$ is modulated by the digital signal simply by making $m(k) = 1$ when bit 1 is present and $m(k) = 0$ when bit 0 is present.

Fig.1 shows the transmitting chaotic signal generated from the DSP board while Fig. 2 depicts the keystream being generated at the transmitter side. It can be seen that the DSP board is able to generate the chaotic signals very well. The performance of the implementation on DSP board can be seen on Fig. 3 where it shows the keystream synchronization error at the transmitter and receiver. The keystream error is converging to zero pretty rapidly proving that even though the system is implemented on a DSP board; it is able to perform the indirect coupled synchronization proving the viability of the digital implementation.

Finally, Fig. 4 shows the performance of the TMS320C6713 on successfully recovering the digital bits at the receiver. After few initial samples, which is taken for synchronization, the bits are being extracted perfectly. The effect of these first few samples which are not extracted due to the time taken for synchronization can easily be eliminated by transferring few insignificant bits at the start.

In this method, the keystream is generated from a different oscillator than the transmitting one. This means that the dynamics of the key generating oscillator is not present in the transmitted signal. In effect, without the knowledge of the keystream, the intruders will not be able to decrypt the message signal back even if they get hold of the encrypted message signal. Therefore, the method

proposed here can be a solution for secure communication. Also, since due to the encryption of the digital bits 0 and 1, there is no particular pattern on the transmitted signal therefore making any pattern classification algorithms like ANN or return maps also not feasible.

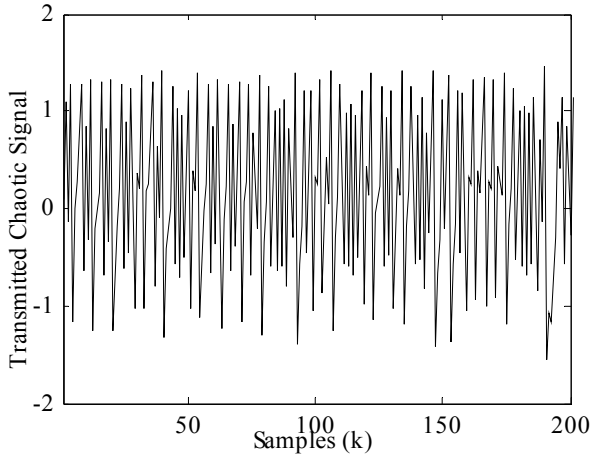

Figure 1. Transmitted Chaotic Signal generated from the DSP board.

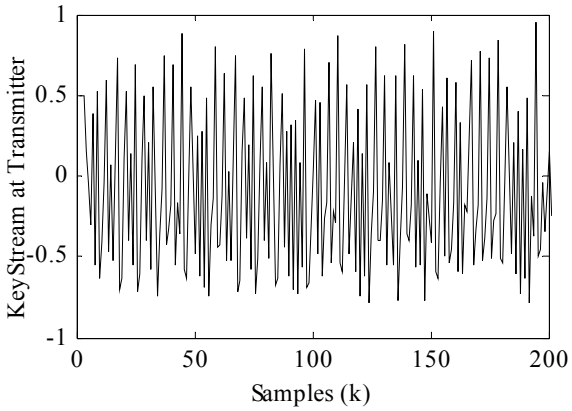

Figure 2. Keystream being generated at the transmitter.

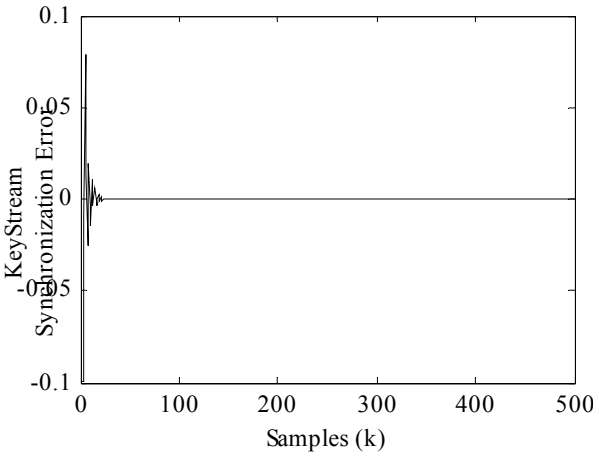

Figure 3. Performance of indirect coupled synchronization in DSP board.

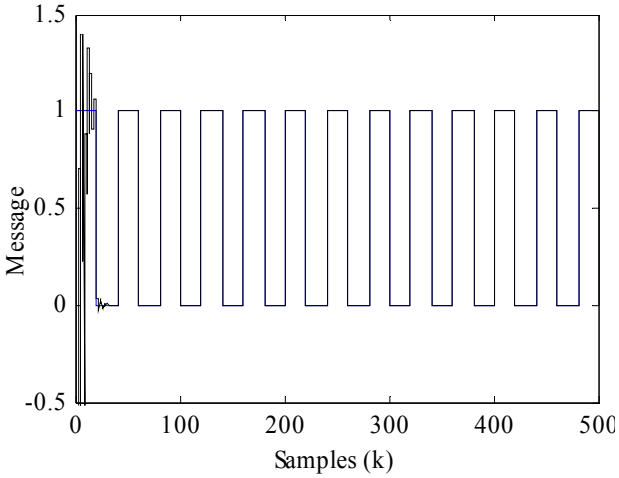

Figure 4. Performance of the DSP board on successfully extracting the digital bits.

V. CONCLUSION

In this paper, a secure digital communication system based on discrete chaotic systems is proposed. The method is based on indirect coupled synchronization for generating chaotic keystream both at the transmitter and receiver. The proposed method is implemented digitally on DSK TMS320C6713 DSP board. Matlab/Simulink Embedded IDE link in combination with TI CCS is used for rapid prototyping of the system. The proposed model is first realized in Simulink and then converted into assembly code for TMS320C6713 using Simulink and CCS. RTDX is used to transmit data from computer to DSP board and vice versa. It was shown that the proposed method on DSP board is able to extract the message successfully thus making the practical realization less complex and easy.

REFERENCES

1. W. D. Chang, "Digital secure communication via chaotic systems," *Digital Signal Processing,* vol. 19, pp. 693-699, 2009.
2. K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.,* vol. 71, pp. 65-68, 1993.
3. L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.,* vol. 64, pp. 821-824, 1990.
4. X. Y. Wang and M. J. Wang, "A chaotic secure communication scheme based on observer," *Communications in Nonlinear Science and Numerical Simulation,* vol. 14, pp. 1502-1508, 2009.
5. T. Yang, "A survey of chaotic secure communication systems," *International Journal of Computational Cognition,* vol. 2, pp. 81-130, 2004.
6. D. Materassi and M. Basso, "Time Scaling of Chaotic Systems: Application to Secure Communications," *International Journal of Bifurcation and Chaos,* vol. 18, pp. 567-575, 2008.
7. M. L'Hernault, J.-P. Barbot, and A. Ouslimani, "Feasibility of Analog Realization of a Sliding-Mode Observer: Application to Data Transmission," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 55, pp. 614-624, 2008.
8. S. Bu and B.-H. Wang, "Improving the security of chaotic encryption by using a simple modulating method," *Chaos Solitons & Fractals,* vol. 19, pp. 919-924, 2004.

9. T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications,* vol. 44, pp. 469-472, 1997.
10. T. Yang, L. B. Yang, and C. M. Yang, "Cryptanalyzing chaotic secure communication using return maps," *Physics Letters A,* vol. 245, pp. 495-510, 1998.
11. A. T. Parker and K. M. Short, "Reconstructing the keystream from a chaotic encryption," *IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications,* vol. 48, pp. 624-630, 2001.
12. G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking parameter modulated chaotic secure communication systems," *Chaos Solitons & Fractals,* vol. 21, pp. 783-787, 2004.
13. G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking Two Secure Communication Systems Based on Chaotic Masking," *IEEE Transaction on Circuit and Systems-II: Express Briefs,* vol. 51, pp. 505-506, 2004.
14. K. M. Short, "Steps toward unmasking secure communications," *International Journal of Bifurcation and Chaos,* vol. 4, pp. 959-977, 1994.
15. K. M. Short, "Unmasking a modulated chaotic communications scheme," *International Journal of Bifurcation and Chaos,* vol. 6, pp. 367-375, 1996.
16. R. Kharel, K. Busawon, and Z. Ghassemlooy, "Indirect coupled oscillators for keystream generation in secure chaotic communication," in *Proceedings of the 48th IEEE conference on Decision and Control and 28th Chinese Control Conference 2009*, 2009.
17. H.-L. An and Y. Chen, "The function cascade synchronization scheme for discrete-time hyperchaotic systems," *Communication Nonlinear Science Numerical Simulation,* vol. 14, pp. 1494-1501, 2009.
18. J. C. Sprott, *Chaos and Time-Series Analysis*: Oxford University Press, 2003