IUST
Iran University of
Science and Technology

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

Designing a New Digital Modulator for Chaotic Secure Communication Systems Using Total Least Square Technique

M. Evazi*, M. Shahsavan*, M. Heidari* and A. Razminia*(C.A.)

Abstract: This paper addresses a new method for decreasing error in secure chaotic communication which utilizes an adaptive law in demodulator part. The basic tools in this process are the Total Least Square as the fundamental technique in demodulating section and a chaotic signal as the carrier one which impose some complexities on the overall system. This algorithm may be used in digital filter for estimating parameters with lower error. Using this approach an improvement can be achieved in estimating the desired signal in comparison with two famous methods, namely, ordinary Least Mean Square (LMS) and Constrained-Stability LMS (CS-LMS). An illustrative example has been used to verify the presented technique through numerical simulation.

Keywords: Chaos, Secure Communications, Total Least Square, Adaptive Digital Filter, Logistic Map.

1 Introduction

SECURE communication is defined as passing along information in such a way that a third party would not be able to overhear it. With respect to daily increased use of wireless electronic devices in home and office situations, it is necessary to ensure communication security as much as possible [1, 2]. Moreover, by chaotic communication we mean the application chaos theory to ensure information transmission security through telecommunication technologies. In parallel to this universal communication system, there are some methods in using this high-tech configuration including: switched chaotic systems with an improvement of security [3], passive synchronization of hyper- chaotic complex nonlinear system [4], switch-modulated method for chaos digital secure communication based on user-defined protocol [5], chaotic secure communication based on a gravitational search algorithm filter [6], secure communication based on a four-wing chaotic system subject to disturbance inputs [7], network coding [8], synchronization and secure communication scheme using optical star network [9]. Nowadays, secure mechanisms are widely used in communication networks such as: GSM networks [10], SWLAN networks [11], and Mobile computing [17].

Recently, index modulation (IM) as a new technique has been developed for multicarrier systems, which uses the indices of the subcarriers as a kind of resource to carry information [12]. In this paper, a high performance least square solver is presented which use recursive Cholesky decomposition. Wireless communication systems require solving least square equations in order to obtain taps weights of the FIR filter [13]. In this study, the authors propose a novel decision feedback equalizer (DFE)-based receiver, which combines channel shortening methods and dichotomous co-ordinate descent (DCD), recursive least squares (RLS), and adaptive algorithm with variable forgetting factor (VFF) [14]. The paper considers adaptive filtering algorithms for communication antenna arrays. The algorithms are based on the using of the quadratized Linearly Constrained Blind Least Mean Square criterion [15]. We propose the least squares disclosure attack (LSDA), in which user profiles are estimated by solving a least squares problem. We show that LSDA is not only suitable for the analysis of threshold mixes, but can be easily extended to attack

Iranian Journal of Electrical and Electronic Engineering, 2018.
Paper first received 23 January 2017 and accepted 09 March 2018.

* The authors are with the Dynamical Systems & Control (DSC) Research Lab., Department of Electrical Engineering, School of Engineering, Persian Gulf University, P.O. Box 75169, Bushehr, Iran.
E-mails: evazi@mehr.pgu.ac.ir, shahsavan@mehr.pgu.ac.ir, m.heidari@mehr.pgu.ac.ir and razminia@pgu.ac.ir.
Corresponding Author: A. Razminia.

pool mixes [16].

Old fashioned digital technologies totally have applied linear systems but later on, in line with technology advancement, companies began to enhance nonlinear communication systems performance. In this way, they applied chaotic communication systems for nonlinear systems [18, 19]. It is worth to mention that there are two precision necessities for the digital communication system, practically. These seemingly separated but technically related necessities are connected with robust generation of chaos and act of detecting quantization features in the channel. The former requirement verifies a very large dynamic range for the chaotic generator polynomial; and the latter one pertains to the necessary level of quantization, confirming that there are no features detectable after digital chaos converting to analog form using digital to analog converter (DAC) and its processing and transmitting.

It is well-known that there is no any exact definition for chaos except a few sorts of valid statements surrounding chaotic behavior. This statement is used for continuous time system; though there are equivalent discrete-time systems, to some extent. As for the main characteristics of the chaotic systems, one can refer to its being non-periodic, wideband, non-predictable and easy to implement practically. Any chaotic system is determined by initial conditions of equation which has a super-sensitive characteristic, when the initial condition is changed a bit, the behavior of the system will be completely different [19].

The discrete-time chaotic systems are preferred to continuous ones because they have more advantages like direct utilization of them using a microcontroller or PC. In addition, it is possible to observe chaos in simple discrete-time systems [9]. Recently, many researchers from various disciplines have paid attentions to the chaos applications. One of such important and useful fields is chaotic communication with some typical applications including: channelized chaotic communications, self-encryption, and chaotic waveform pseudo-ranging [20]. Among this hot research field, digital chaotic systems have great advantages such as simple reproduction of devices, simple parameter setting and parameter stability [21]. Due to the nature of broadband chaotic signals, they can be used as carriers in spread-spectrum communications. Low probability of being intercepted, their resistance for jamming multiple access capability and multipath protection are among the advantages of spread spectrum communications such as chaos-based ones which have more advantages compared to the spread spectrum of conventional communications. An adaptive estimator is an estimator in a parametric or semiparametric model with nuisance parameters such that the presence of these nuisance parameters does not affect efficiency of estimation.

In this paper, we propose a new method for chaotic secure communications. In fact, a Total Least Square (TLS) algorithm is used to perform the demodulation in the digital filter part. Compared to ordinary Least-Mean-Square (LMS) and Constrained-Stability LMS (CSLMS), we obtain a better performance for the presented configuration with a logistic map as the carrier in its chaotic regime.

It is worth mentioning that TLS has many applications in such different fields as computer version [29], image reconstruction [30, 32], speech and audio processing [33, 34], modal and spectral analysis [35, 36], linear system theory [37, 38], system identification [39, 42], and astronomy [43]. The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree two, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. The map was popularized in a seminal 1976 paper by the biologist Robert May, in part as a discrete-time demographic model analogous to the logistic equation first created by Verhulst.

In applied statistics, total least square is a type of errors in variables regression, a least squares data modeling technique in which observational errors on both dependent and independent variables are taken into account. It is a generalization of deeming regression and also of orthogonal regression, and can be applied to both linear and non-linear models. The total least squares approximation of the data is generically equivalent to the best, in the Frobenius norm, low rank approximation of the data matrix.

The structure of this paper is as follows. Section 2 devoted to some basic background from filtering and LMS theories. Application to chaotic communication with adaptive digital filter is discussed in Section 3. Numerical simulations are performed in Section 4. Finally, some concluding remarks in Section 5 close the paper.

2 Basic Backgrounds

In this section some preliminaries from filters fundamental, their analysis, typical classifications, and LMS theories are reviewed.

2.1 Basic Concepts of LMS

Because of its simplicity, low computational complexity and easy implementation, many filtering applications usually use LMS algorithm. Some of these applications are system identification, channel equalization, communication, control, beam forming, etc. The weight update in standard LMS is calculated using the following equation [44]:

$$\omega(n+1)=\omega(n)+\mu u(n)e^{*}(n) \quad (1)$$

where μ is a step size parameter and $e^{*}(n)$ shows the complex conjugate of the error signal between the designed signal and the output signal and $u(n)$ is the input vector. However, many improved LMS algorithms have been suggested to promote filter efficiency and convergence speed [24]. A constrained stability LMS (CS-LMS) algorithm is an algorithm suggested specifically to filter speech sounds. This algorithm is achieved through minimizing the squared Euclidean norm of the difference weight vector under a stability constraint set for the posterior estimation error. Step size is based on the error signal and is very important in this kind of algorithm. The weight update relations of CS-LMS algorithm are as follows [44]:

$$\omega(n+1) = \omega(n) + \mu \frac{\delta u(n) \delta e(n)}{\delta u(n)^2} \tag{2}$$

where $\delta = u(n) - u(n{-}1)$ and $\delta e(n) = e(n) - e(n{-}1)$ are the difference of input vector and error signal, respectively. The step size largely affects convergence speed and steady state maladjustment. The larger step size, the better convergence speed but anyway increases maladjustment [24, 25].

2.2 Total Least Square

Golub and Van Loan proposed the total least square method for the over-determined system of equations $AX \approx B$, where $A \in R^{m\times n}$ and $B \in R^{m\times d}$ are the defined data and $X \in R^{m\times d}$ is undefined [26, 27]. In case $m > n$, there is no precise solution for X, thus it is going to look for an approximate one. The total least squares method is a natural generalization of the least squares approximation method when the data in both A and B are perturbed. Notice the classic problem of total least square which searches the minimal corrections ΔA and ΔB for our defined data A and B and makes a correct system of equations $\hat{A}X = \hat{B}$, $\hat{A} := A + \Delta A$, $\hat{B} := B + \Delta B$ possible to be solved, i.e., [28]:

$$\left\{\hat{X}_{TLS}, \Delta A_{TLS}, \Delta B_{TLS}\right\}: \ \arg \min_{X, \Delta A, \Delta B} \left[\Delta A, \Delta B\right]_F \tag{3}$$

where $(A + \Delta A)X = B + \Delta B$. The total least square approximate method X_{TLS} for X is in fact a solution for a system of equations which is corrected optimally $\hat{A}_{TLS} = \hat{B}_{TLS}$, $\hat{A}_{TLS} := A + \Delta A_{TLS}$, $\hat{B}_{TLS} := B + \Delta B_{TLS}$. Formulation of the total least squares problem as a matrix low rank approximation problem [28]:

$$\begin{aligned} &\hat{C}_{TLS} := \arg \min_{\hat{C}} \left\| C - \hat{C} \right\|_F \\ &\text{Subject to } \operatorname{rank}\left(\hat{C}\right) \le n \end{aligned} \tag{4}$$

The recent method of total least squares in form of a matrix low rank estimation method is certainly advantageous over the traditional one. In case of $C = [A\ B]$, equation (3) (classical method) is basically identical to (4) (the matrix low rank approximation method). Of course, there are some exceptional times that (3) is unable to find a solution but (4) can always give a solution. However, both of these methods can evaluate fitting accuracy in different ways: the least squares method minimizes the sum of squared vertical distances but TLS method minimizes the sum of squared orthogonal distances from the data points to the fitting line, in both cases. In the former case, data approximation is carried out through correcting only the second coordinate but in the latter one (TLS), it is achieved through correcting both coordinates [28]. There is a comparison of the total least square and least square the total least squares problem has an analytic expression that is similar to the one of the least-squares solution [28]:

$$\begin{aligned} &\textbf{Least Squares}: \ \hat{x}_{LS} = (A^\top A)^{-1} A^\top b \\ &\textbf{Total Least Square}: \ \hat{x}_{TLS} = (A^\top A - \sigma_{n+1}^2 I)^{-1} A^\top b \end{aligned} \tag{5}$$

where σ_{n+1} is the smallest singular value of [A B]. While least squares minimize a sum of squared-residuals, total least squares minimize a sum of weighted squared residuals [28]:

$$\begin{aligned} &\textbf{Least Squares}: \ \min_x Ax - b^2 \\ &\textbf{Total Least Square}: \ \min_x \frac{Ax - b^2}{x^2 + 1} \end{aligned} \tag{6}$$

The solution of the classical total least squares problem [28]

$$\begin{aligned} &C := \left[A \ \ B\right] = U \sum V^\top \\ &\sum := \operatorname{diag}\left(\sigma_1, \sigma_2 \ldots, \sigma_{n+d}\right) \end{aligned} \tag{7}$$

is a singular value decomposition of C, $\sigma_1 \ge \cdots \ge \sigma_{n+d}$ be the singular values of C, and define the partitioning [28]

$$V := \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix}, \quad \sum := \begin{bmatrix} \sum_1 & 0 \\ 0 & \sum_2 \end{bmatrix} \tag{8}$$

A total least squares solution exists if and only if V_{22} is non-singular. In addition, it is unique if and only if $\sigma_n \ne \sigma_{n+1}$. In the case when the total least squares solution exists and is unique, it is given by [28]

$$\hat{X}_{TLS} = -V_{12} V_{22}^{-1} \tag{9}$$

and the corresponding total least squares correction matrix is [28]:

$$\Delta C_{TLS} := \left[\Delta A_{TLS} \ \ \Delta B_{TLS}\right] = -U \operatorname{diag}\left(0, \Sigma_2\right) V^\top \tag{10}$$

In the generic case when a unique total least squares solution exists, it is computed from the d right singular vectors corresponding to the smallest singular values by normalization. This gives Algorithm 1 as a basic algorithm for solving the classical total least squares problem (3). Note that the total least-squares correction matrix ΔC_{TLS} is such that the total least squares data approximation [28]:

$$\hat{C}_{TlS} := C + \Delta C_{TLS} = U \ \text{diag}\left(\Sigma_1, 0\right) V^T \tag{11}$$

is the best rank *n* approximation of *C*.

```
Algorithm 1 Basic total least squares algorithm
Input:   $A \in \mathbb{R}^{m\times n}$, $B \in \mathbb{R}^{m\times d}$
Output:  $X_{TLS}$ a total least squares solution of $AX \approx B$
  1: Compute the singular value decomposition $[A\ B] = U \sum V^T$
  2: If $V_{22}$ is non-singular
       Then set $\hat{X}_{TLS} = -V_{12}V_{22}^{(-1)}$
  3: Else Output a message that the problem (TLS1) has no solution and stop
  4: End If
```

3 Application to Chaos Communication with Adaptive Digital Filter

3.1 Algorithm of Total Least Square

More information on derivation and an asymptotic analysis of the proposed algorithm are presented in this section. The anti-Hebbian learning rule that is obtained from the Hebbian rule given by (1) yielded this algorithm with the sign of its incremental term being reserved. In this algorithm, first we update the vector of the linear neuron unit considering an anti-Hebbian rule, that is, first we modify the weight vector as $\bar{\omega}(n)$ by subtracting a small quantity that is proportional to the product of the input and the output signals from $\omega(n)$, as given by [44]:

$$\bar{\omega}(n+1) = \omega(n) - \mu\xi(n)e(n) \tag{12}$$

Next, a scaling operation is performed on the weight vector as given by [44]:

$$\omega(n+1) = -\frac{\bar{\omega}(n+1)}{\bar{\omega}_{k+1}(n+1)} \tag{13}$$

which essentially makes the last component $\omega(n+1)$ of the weight vector to be −1. Combining (12) and (13) yields [44]:

$$\omega(n+1) = \frac{\omega(n) - \mu\xi(n)e(n)}{1+\mu\xi_{k+1}(n)e(n)} \tag{14}$$

The anti-Hebbian learning operation is represented by the numerator of (14) and the last component of the weight vector at the value of -1 is kept by the denominator. Equation (14) is called the explicitly scaled anti-Hebbian algorithm. If the gain coefficient μ is small enough such that $|\{\mu\xi_{k+1}(n)e(n)\}| < 1$ then (14) can be expanded as a power series in μ, yielding [44]:

$$\omega(n+1) = \omega(n) - \mu e(n)\left[\xi(n) + \omega(n)\xi_{k+1}(n)\right] + O(\mu)^2 \tag{15}$$

where $O(\mu^2)$ denotes the summation of the second and higher order terms in μ. By neglecting these terms, a simple learning algorithm is obtained as given by [44]:

$$\omega(n+1) = \omega(n) - \mu e(n)\left[\xi(n) + \omega(n)\xi_{k+1}(n)\right] \tag{16}$$

which is more suitable in the numerical simulations.

3.2 Adaptive FIR Filtering

Some areas such as echo cancellation, modeling, control, equalization, and beam-forming make use of adaptive FIR filters. Here, the proposed constrained anti-Hebbian learning algorithm was formulated in the framework of parameter estimation of an adaptive FIR filter, and it was compared with the widely-used least mean square (LMS) algorithm. Based on [44] a temporal adaptive FIR filter is shown in Fig. 1, where approximation [28]:

$$u(n) = [u(n), u(n-1), \cdot\cdot\cdot, u(n-k+1)]^T \tag{17}$$

is the input vector, and

$$\omega(n) = [\omega_0(n), \omega_1(n), \cdot\cdot\cdot, \omega_{k-1}(n)]^T \tag{18}$$

is the weight vector, and *d*(*n*) is the desired output of the filter. Moreover, the actual output signal of the adaptive filter is given by the following relation:

$$y(n) = \omega^T(n)u(n) \tag{19}$$

The difference between *y*(*n*) and *d*(*n*) as given by

$$e(n) = y(n) - d(n) \tag{20}$$

is the error signal for the adaptive filter. One of the conventional training approaches used in adaptive FIR filter is the LMS algorithm, in which $\omega(n)$ is updated through adding a fraction of the approximation of the instantaneous gradient of the mean square error, as given by

$$\omega(n+1) = \omega(n) - \mu u(n)e(n) \tag{21}$$

Then the constrained anti-Hebbian algorithm is applied to this adaptive filter. Now, letting $\xi(n) = \left[u(n), d(n)\right]^T$, $\omega(n) = \left[\omega_1(n), \cdots, \omega_k(n)\right]^T$ and then (19) and (20) result in [44]:

$$e(n) = \omega^T(n)u(n) - d(n) \tag{22}$$

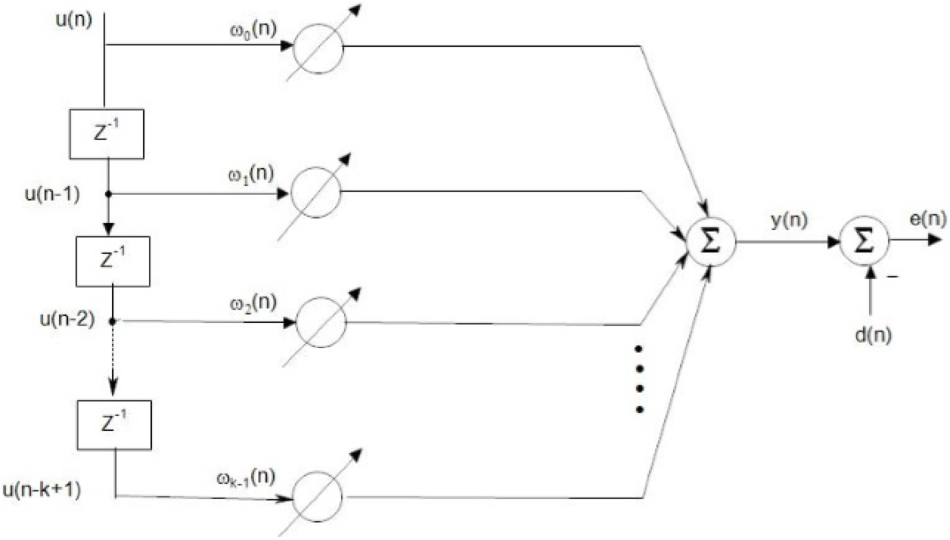

Fig. 1 Adaptive filter mechanism.

Therefore, the error signal *e(n)* of the adaptive filter, is directly obtained from the constrained anti-Hebbian learning algorithm. As in many adaptive filter applications, the error signal has the same importance as filter parameters and other signal quantities that is regarded as a very useful property. By establishing the correspondence between the anti-Hebbian neuron and the adaptive FIR filter, we can express the explicitly scaled anti-Hebbian algorithm (14) for the FIR adaptive filter as [44]:

$$\omega(n+1)=\omega(n)-\mu e(n)\left[u(n)+\omega(n)d(n)\right] \qquad (23)$$

As for the structure, (24) is more similar to the LMS algorithm (21) than (23) is. In (24), one of the incremental terms $-\mu e(n)u(n)$ is the same as the LMS incremental term. However, the feedback term $-\mu e(n)d(n)\omega(n)$, which is proportional to the product of the desired output signal and the error signal, controls the change in the weight vector in (24). The incremental term makes the algorithm optimal under the criterion of the TLS, which provides a better performance over the LMS algorithm in many applications. The learning algorithm (24) is referred to as the constrained anti-Hebbian algorithm for adaptive FIR filtering.

3.3 Application to Chaos Communication

A new communication technique in developing wide-band communication is chaotic modulation. Parameter modulation is regarded as a chaotic modulation method which hides the information signal in the bifurcation parameter of a chaotic dynamical system. Therefore, a wide bandwidth is occupied by the modulated signal in the chaotic region. No code synchronization is required for the chaotic parameter modulation and a higher capacity than the conventional spread spectrum system for multiuser communication must be provided.

Fig. 2 shows the block diagram of chaotic communication with additive white Gaussian noise (AWGN) channel. The chaotic parameter modulates the information signal $s(n)$, and the transmitted signal $u(n)$ is corrupted by AWGN shown as:

$$y(n)=u(n)+\nu(n) \qquad (24)$$

where $v(n)$ is a zero mean white Gaussian channel noise with variance $R(n)$. What we intend to use here, is applying the TLS to recover the information signal from the received signal $y(n)$. Consider the following chaotic dynamical system for modulation

$$u(n)=f\left(u(n-1),\lambda\right) \qquad (25)$$

where λ is the bifurcation parameter, and is used to modulate the information signal $s(n)$ by setting $\lambda(n) = s(n)u(n)$ which can preserve chaos by imposing $s(n)$ on the chaotic range. One of the most popular and famous discrete-time chaotic system, is the logistic map, in which against its apparent simplicity it evolve a rich chaotic behavior. A fundamental relation to the Logistic map is:

$$u(n)=\lambda u(n-1)\left(1-u(n-1)\right) \qquad (26)$$

where $\lambda = [3.7, 4]$ is the chaotic region of the logistic map. Based on the chaotic parameter modulation, the transmitted signal is given as

$$u(n)=s(n)u(n-1)\left(1-u(n-1)\right) \qquad (27)$$

when $s(n)$ is controlled to kept in the chaotic region [3.7, 4], and so the transmitted signal is wide-band chaotic signal. Based on the TLS algorithm, the desired signal is $d(n)y(n+1)$, and the information $s(n)$ is considered as the weight. The demodulator dependent on the adaptive TLS for chaos communication is designed by

$$\begin{aligned} e(n) &= y(n+1) - s(n)y(n)(1-y(n)) \\ s(n+1) &= s(n) + \mu e(n)(u(n) + d(n)s(n)) \end{aligned} \tag{28}$$

where the input signal is:

$$u(n) = y(n)(1-y(n)) \tag{29}$$

As will be illustrated in the next section, this simple algorithm has a better performance rather than the other usual LMS-based demodulation methods.

4 Numerical Simulations

Three different signals are utilized as the information to evaluate the performance of the TLS receiver.

1. a constant signal: $s_n = 3.85$;
2. multi value constant signal:

$$s_n = \begin{cases} 3.75 & 0 < n \le 400 \\ 3.8 & 400 < n \le 800 \\ 3.85 & 800 < n \le 1200 \\ 3.9 & 1200 < n \le 1600 \\ 4 & 1600 < n \le 1200 \end{cases};$$

3. . a sinusoidal signal: $s_n = 3.9 + 0.05\sin(n/5)$.

These three signals embody different time-varying characteristics. It should also be pointed that these information signals further can be applied in evaluating the filtering performance of the demodulator proposed. Gaussian white noise process is used as the measurement noise in the current attempt. We control the variance of the measurement in order to achieve the desired signal-to-noise (SNR) value. The Mean Squares Error (MSE) used as the filtering performance measure, is defined as

$$MSE = \frac{1}{n}\sum_{n=1}^{N}(s(n) - \hat{s}(n))^2 \tag{30}$$

where $\hat{s}(n)$ is the estimated signal produced by the demodulator, and N is the total length of discrete time. 100 trials were conducted to have the average of all the MSE values in the following simulations.

Figs. 3-5 show the MSE performance versus different SNR values for the three signals, respectively. By keeping the information signal, the parameters about step size are configured as $\mu = 0.7$ in the LMS, $\mu = 0.009$ in the CSLMS, and in the TLS $\mu = 0.02$. Fig. 3 shows the comparison results about the MSE versus SNR of the proposed algorithms. According to Fig. 3, for the constant signal the MSE of the TLS is always smaller than that of the CS-LMS and LMS. Consequently, the TLS-based demodulating scheme has a better performance than the LMS and CS-LMS-based demodulators for all SNR.

Let see the performance of these three demodulating techniques for the second and third signal; i.e., s_n is multivalued constant and sinusoidal. The parameters of step size are configured as $\mu = 1$ in the LMS,

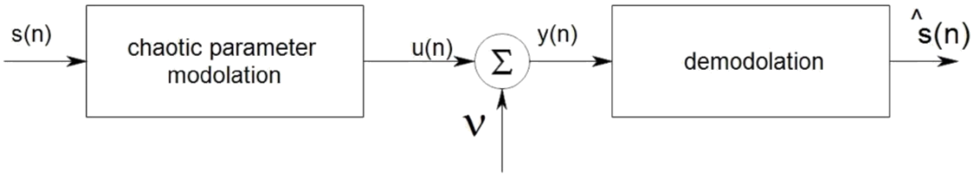

Fig. 2 Block diagram of chaotic communication.

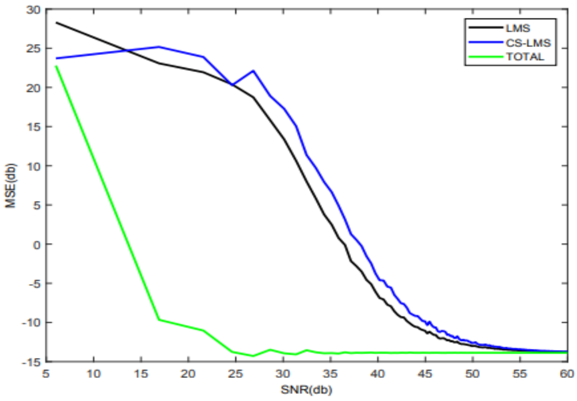

Fig. 3 MSE for constant input signal.

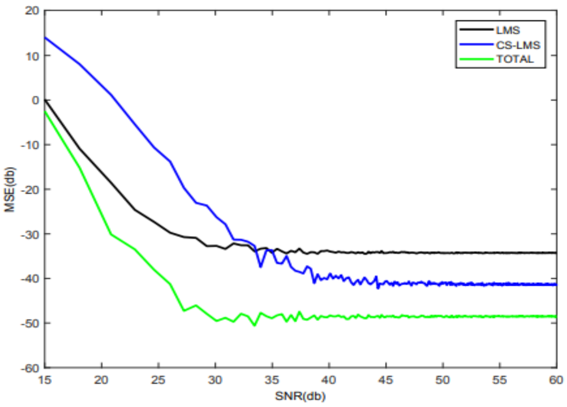

Fig. 4 MSE for multi-valued constant input signal.

$\mu = 0.08$ in the CS-LMS, and $\mu = 0.3$ in the TLS for the multivalued constant signal, and $\mu = 2$ in the LMS, $\mu = 0.35$ in the CS-LMS, and $\mu = 0.6$ in the TLS for the sinusoid signal, respectively. The comparison results of these three algorithms for the multivalued constant signal and the sinusoid signal, respectively, are shown in Figs. 4 and 5. Based on Fig. 4, the MSE of the TLS is always 8 dB smaller than the CS-LMS for all SNR values. In other words, TLS always has better demodulation performance than the CS-LMS. Nevertheless, with the increase in SNR, the TLS demodulator would perform significantly better than the two CS-LMS and LMS demodulators. When the SNR values are greater than 35 dB, we choose the TLS instead of the LMS and the CS-LMS. For the sinusoid signal, the LMS and the CS-LMS outperform the TLS in the case of smaller SNR, which is obtained from Fig. 5. When the SNR is greater than 35 dB, the TLS has the best demodulation performance in the three demodulators. The reason for degrading performance in the case of low SNR is that, the larger error signal coming from the channel measurement noise may lead to finally obtain irrelevant step size for relatively larger misadjustment. Hence, the proposed TLS can obtain a smaller misadjusment only when SNR increases.

The convergence speed of these algorithms is achieved by considering the communication environment of $SNR = 60$ dB The parameter setting is shown as follows. For the constant signal, $\mu = 6$ in the LMS, $\mu = 0.35$ in the CS-LMS, and $\mu = 0.2$ in the TLS. For the multi-valued constant signal, $\mu = 6$ in the LMS, $\mu = 0.25$ in the CS-LMS, and $\mu = 0.25$ in the adaptive CS-LMS. For the sinusoid signal, $\mu = 6$ in the LMS, $\mu = 0.35$ in the CS-LMS, and $\mu = 0.6$ in the TLS. The demodulation results for these three information signals based on the three demodulators are shown in Figs. 6-8. According to these three figures, the proposed TLS algorithm has a faster convergence speed and a better demodulation performance than the two other LMS and CS-LMS algorithms in the case of high SNR.

5 Conclusion

In this work, a new digital filter has been designed for a chaotic communication system in which the demodulating part is processed via TLS algorithm. A Logistic map has been considered as the chaos-producer at the transmitter part. The modulator section regards the information signal as the controlled bifurcation parameter to keep the output of the modulator in the

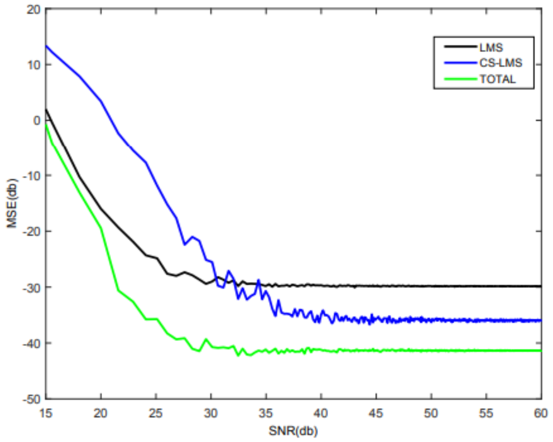

Fig. 5 MSE for sinusoidal input signal.

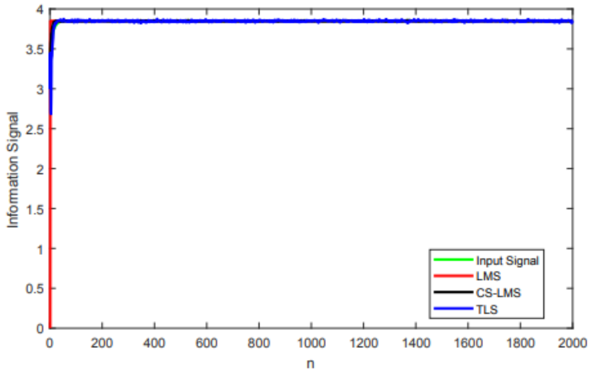

Fig. 6 Estimating the information signal when it is constant.

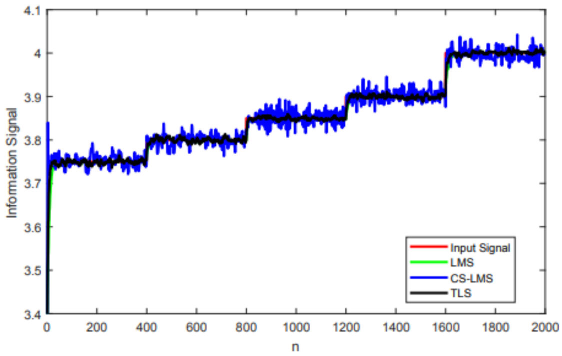

Fig. 7 Estimating the information signal when it is multi-valued constant.

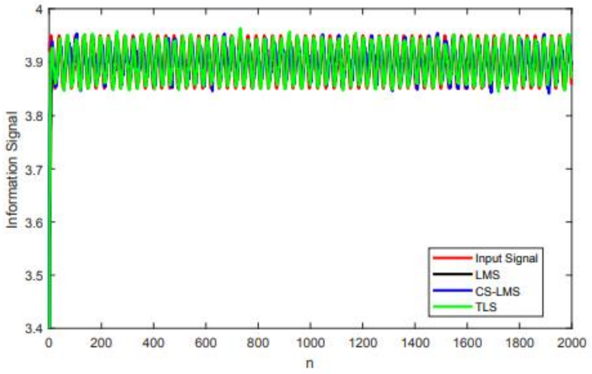

Fig. 8 Estimating the information signal when it is sinusoidal.

Chaos region. In the presence of an additive white noise of channel, what received by the demodulator is a noisy signal. Numerical simulations show that the presented technique for various information signals (e.g., constant, multivalued constant, and sinusoidal) has a better performance than the usual LMS-based methods, such as ordinary LMS and the CS-LMS one. This advantage is more highlighted for large SNRs.

References

[1] D. P. Agrawal and Q. A. Zeng, *Introduction to wireless and mobile systems*. 2nd Edition, Thomson, ISBN 978-0-534-49303-5, Apr. 2005

[2] J. F. Kurose and K. W. Ross, *Computer networking: a top-down approach*. 2nd Edition, Addison Wesley, ISBN 978-0-321-17644-8, 2003.

[3] T. H. Lee, J. H. Park, H. Y. Jung and S. M. Lee, "Improving security in communication using switched chaotic systems," *IEEE International Conference on Consumer Electronics (ICCE)*, 2015.

[4] X. Wua, C. Zhua and H. Kanb, "An improved secure communication scheme based passive synchronization of hyperchaotic complex nonlinear system," *Applied Mathematics and Computation*, Vol. 252, pp. 201–214, 2015.

[5] W. Xing-yuan and G. Yong-feng, "A switch-modulated method for chaos digital secure communication based on user-defined protocol," *Communications in Nonlinear Science and Numerical Simulation*, Vol. 15, No. 1, pp. 99–104, 2010.

[6] X. H. Han and X. M. Changn, "Chaotic secure communication based on a gravitational search algorithm filter," *Engineering Applications of Artificial Intelligence*, Vol. 25, No. 4, pp. 766–774, 2012.

[7] F. Yua and C. Wangb, "Secure communication based on a four-wing chaotic system subject to disturbance inputs," *Optik - International Journal for Light and Electron Optics*, Vol. 125, No. 20, pp. 5920–5925, 2014.

[8] Z. Cao, Y. Tang and J. Luo, "Secure communication with network coding," *Physics Procedia*, Vol. 24, pp. 1943–1950, 2012.

[9] S. Jeeva Sathya Theesar, M. R. K. Ariffin and S. Banerjee, "Synchronization and a secure communication scheme using optical star network," *Optics & Laser Technology*, Vol. 54, pp. 15–21, 2013.

[10] H. A. El Zouka, "Providing end-to-end secure communication GSM networks," *International Journal of Network Security & Its Applications*, Vol. 7, No. 4, pp. 31–41, Jul. 2015.

[11] S. Shanken, D. Hughes and T. Trellisware, "Secure wireless local area network (SWLAN)," *Military Communications Conference*, Vol. 2, pp.886–891, 2004.

[12] G. Cheng, L. Wang, W. Xu and G. Chen, "Carrier index differential chaos shift keying modulation," *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 64, No. 8, pp. 907–911, 2017.

[13] V. Pawar and K. N. Karamtot, "Least square solver for wireless communication system," in *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2016.

[14] Y. Zhang, L. Liu, D. Sun and H. Cui, "Single-carrier underwater acoustic communication combined with channel shortening and dichotomous coordinate descent recursive least squares with variable forgetting factor," *IET Communications*, Vol. 9, No. 15, pp. 1867–1876, 2015.

[15] V. I. Djigan, "Blind Least Mean Square criterion algorithms for communication adaptive arrays," *East-West Design & Test Symposium (EWDTS)*, 2013.

[16] F. P. Gonzalez, C. Troncoso and S. Oya, "A least squares approach to the static traffic analysis of high-latency anonymous communication systems," *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 9, pp. 1341–1355, 2014.

[17] M. Rautila and J. Suomalainen, "Secure inspection of web transactions," *International Journal of Internet Technology and Secured Transactions*, Vol. 4, No. 4, pp. 253–271, 2012.

[18] M. Sushchik, L. S. Tsimring and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 47, No. 12, pp. 1684–1691, 2000.

[19] S. I. Hong and E. Y. Jang, "FPGA implementation of digital transceiver using chaotic signal," *Korea Institute of Information Technology Review*, Vol. 15, No. 2, pp. 215–223, Aug. 2010.

[20] J. M. Alan and B. C. David, "Efficient and flexible chaotic communication waveform family," in *Military Communications Conference*, pp. 1250–1255, 2010.

[21] M. Stork, "Discrete-Time Chaotic Systems, Impulsive synchronization and application in communication," in *IEEE 9th International New Circuits and Systems Conference (NEWCAS)*, pp. 189–192, 2011.

[22] C. Zijian, L. Bingbing and D. Jinlei, “Application of digital filter in fiber optic gyroscope inertial navigation system,” in *IEEE Chinese Guidance, Navigation and Control Conference (CGNCC)*, pp. 88–90, 2014.

[23] F. Ashok, S. Candak, D. R. Anil and J. Patil, “Application of digital filter in fiber optic gyroscope inertial navigation system,” *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 3, No. 11, pp. 12969–12976, 2014.

[24] G. Song, G. Liu, W. Liu, Z. Long and S. Wang, “A modified constrained stability-least mean square algorithm and its application in chaos communication,” in *5th International Congress on Image and Signal Processing (CISP 2012)*, pp. 1523–1527, 2012.

[25] J. M. Grriz, J. Ramrez, S. Cruces-Alvarez, C. G. Puntonet, E. W. Lang, D. Erdogmus and S. Member, “A novel LMS algorithm applied to adaptive noise cancellation,” *IEEE Signal Processing Letters*, Vol. 16, No.1, pp.34–37, 2009.

[26] G. Golub, “Some modified matrix eigenvalue problems,” *SIAM Review*, Vol. 15, No. 2, pp. 318–344, 1973.

[27] G. Golub, C. Van Loan, “An analysis of the total least squares problem,” *Siam Journal on Numerical Analysis*, Vol. 17, No. 6, pp. 883–893, 1980.

[28] Ivan Markovsky and S. Van Huffel, “Overview of total least-squares methods,” *Signal Processing*, pp. 2283–2302, 2007.

[29] M. Muhlich and R. Mester, “The role of total least squares in motion analysis,” in *Proceedings of the Fifth European Conference on Computer Vision*, Springer, Berlin, pp. 305–321, 1998.

[30] X. Duan, X. Zhang and Q. Wang, “Computing approximation GCD of several polynomials by structured total least norm,” *Advances in Linear Algebra & Matrix Theory*, Vol. 03, No. 04, pp. 39–46, 2013.

[31] X. L. Zhao, W. Wang, T. Y. Zeng, T. Z. Huang and M. K. Ng, “Total variation structured total least squares method for image restoration,” *Industrial and Applied Mathematics, Scientific Research*, Vol. 35, No. 6, pp. B1304–B1320, 2013.

[32] H. Fu and J. Barlow, “A regularized structured total least squares algorithm for high-resolution image reconstruction,” *Linear Algebra and its Applications*, Vol. 391 No. 1, pp. 75–98, 2004.

[33] P. Lemmerling, N. Mastronardi and S. Van Huffel, “Efficient implementation of a structured total least squares based speech compression method,” *Linear Algebra and its Applications*, Vol. 366, pp. 295–315, 2003.

[34] K. Hermus, W. Verhelst, P. Lemmerling, P. Wambacq and S. Van Huffel, “Perceptual audio modeling with exponentially damped sinusoids,” *Signal Processing*, Vol. 85, pp. 163–176, 2005.

[35] P. Verboven, P. Guillaume, B. Cauberghe, E. Parloo and S. Vanlanduit, “Frequency-domain generalized total least squares identification for modal analysis,” *Journal of Sound and Vibration*, Vol. 278, No. 1-2, pp. 21–38, 2004.

[36] A. Yeredor, “Multiple delays estimation for chirp signals using structured total least squares,” *Linear Algebra and its Applications*, Vol. 391, pp. 261–286, 2004.

[37] K. Yang, X. Bu and G. Sun, “Constrained total least squares location algorithm using time-difference-of-arrival measurements,” *IEEE Transactions on Vehicular Technology*, Vol. 59, No. 3, pp. 1558–1562, 2010.

[38] S. Javed, N. A. Ahmad, “A stochastic total least squares solution of adaptive filtering problem,” *Scientific World Journal*, Vol. 2014, pp. 1–6, 2014.

[39] C. Hu, Y. Chen and Y. Peng, “On weighted total least squares adjustment for solving the nonlinear problems,” *Journal of Geodetic Science*, Vol. 4, No.1, pp.49–56, 2014.

[40] P. Lemmerling, B. De Moor, “Misfit versus latency,” *Automatica*, Vol. 37, pp. 2057–2067, 2001.

[41] X. Fang, J. Wang , B. Li, W. Zeng and Y. Yao, “On total least squares for quadratic form estimation,” *Studia Geophysica et Geodaetica*, Vol. 59, No. 3, pp. 366–379, Jul. 2015.

[42] I. Markovsky, J. C. Willems, S. Van Huffel, B. De Moor and R. Pintelon, “Application of structured total least squares for system identification and model reduction,” *IEEE Trans. Automat. Control*, Vol. 50, No. 10, pp. 1490–1500, 2005.

[43] R. Branham, “Multivariate orthogonal regression in astronomy,” *Celestial Mechanics and Dynamical Astronomy*, Vol. 61, No. 3, pp. 239–251, 1995.

[44] K. Gao, M. Omair Ahmad and M. N. S. Swamy, “A constrained anti-Hebbian learning algorithm for total least squares estimation with applications to adaptive FIR and IIR filtering,” *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, Vol. 41, pp. 718–729, 1994.

M. Evazi was born in Bushehr, Iran, in 1989. He received his B.Sc. degree in Telecommunication Systems and his M.Sc. degree in Control Systems both from Persian Gulf University, Bushehr, Iran. His research interests are nonlinear control, chaotic systems, and digital communication systems.

M. Shahsavan was born in Estahban, Fars, Iran, in 1986. He received his B.Sc. degree in Electrical Engineering and his M.Sc. degree in Control Systems from Imam Hossein University, Tehran, Iran, and Persian Gulf University, Bushehr, Iran, respectively. His research interests are model order reduction, periodic systems, and linear control design.

M. Heidari was born in Bushehr, Iran, in 1991. She received his B.Sc. degree in Telecommunication Systems and his M.Sc. degree in Control Systems both from Persian Gulf University, Bushehr, Iran. Her research interests are nonlinear control, stability analysis, and control theory.

A. Razminia was born in Bushehr, Iran in 1982. He received his B.Sc. degree in Control Systems from Shiraz University, Shiraz, Iran, in 2004, the M.Sc. degree in Control Systems from Shahrood University of Technology, Shahrood, Iran, in 2007, and the Ph.D. degree in Control Systems from Tarbiat Modares University, Tehran, Iran, in 2012. He is currently an Associate Professor with the Department of Electrical Engineering, School of Engineering, Persian Gulf University, Bushehr, Iran. His research interests include optimal control systems, nonlinear dynamical systems, system identification, fractional order systems, and chaos theory.