Chaotic Secure Communication Using Iterated Filtering Method

P. Karthik[1], *D. Gokul Prashanth*[2], *T. Gokul*[3]

Assistant Professor, Department of Electronics and Communication Engineering,
SNS College of Engineering, Coimbatore, India[1]

Under Graduate Scholar, Department of Electronics and Communication Engineering,
SNS College of Engineering, Coimbatore, India[2]

Under Graduate Scholar, Department of Electronics and Communication Engineering,
SNS College of Engineering, Coimbatore, India[3]

Abstract—**The communication process is one of the fast developing field which demands security as well as performance. For achieving high security, many chaos synchronization schemes have been proposed which are compromising the performance of the system. Also the chaos synchronization controller is not robust and adaptable to different working conditions. Thus, achieving a high security for the information at lowest possible performance degradation is a major challenge.**

This proposal aims to overcome this challenge by introducing a new approach that employs the use of Iterated Filtering Algorithm (IFA). The real time speech signal (i.e. a recorded audio) is mixed with the chaotic signal (generated by Gingerbreadman Map) at the transmitter side and then the audio signal is separated by the Iterated Filtering Algorithm (IFA) at the receiver side.

It offers an efficient method to estimate the median without time consuming data sorting techniques. Thus, it is used here to recover the speech signal from the mixed signal.

***Index Terms*—Iterated Filtering Algorithm (IFA), Gingerbreadman Map, Chaotic Signal.**

I. Introduction

The word “chaos” means “a state of disorder”. Where the present determines the future, but the approximate present does not approximately determine the future.

Chaos theory is concerned with the deterministic systems whose behavior can be predicted. Chaotic systems are predictable for a while and then appear to become random. The amount of time for which the behavior of a chaotic system can be effectively predicted depends on three things: How much uncertainty we are willing to tolerate in the forecast; how accurately we are able to measure its current state; and a time scale depending on the dynamics of the system , called the Lyapunov time. In chaotic systems the uncertainty in a forecast increases exponentially with elapsed time. Hence doubling the forecast time more than squares the proportional uncertainty in the forecast. This means that in practice a meaningful prediction cannot be made over an interval of more than two or three times the Lyapunov time. When meaningful predictions cannot be made, the system appears to be random. Thus, it is widely used in the communication process for hiding the information.

Iterated Filtering Algorithms (IFA) are a tool for maximum likelihood inference for partially observed dynamical systems. Stochastic perturbations of the unknown parameters are used to explore the parameter space. Applying sequential Monte Carlo (the particle filter) to this extended model result in the selection of the parameter values that are more consistent with the data. Iterated filtering methods have so far been used most extensively to study the infectious disease transmission dynamics.

This IFA process is employed here to separate the mixed audio and chaotic signal.

II. IMPLEMENTATION TOOL

MATLAB (Matrix Laboratory) is a numerical computing environment and fourth-generation programming language developed by Math Works. MATLAB allows matrix manipulations, plotting of functions and knowledge, implementation of algorithms, creation of user edges, and interfacing with programs written in alternative languages, together with C, C++, Java, and FORTRAN. MATLAB is a simulation tool that is helpful in finding out the dynamic nature of the communication networks.

III. EXISTING SYSTEM

A. Emperical Mode Decomposition (EMD)

The starting point of the Empirical Mode Decomposition (EMD) is to consider oscillations in signals at a very local level. In fact, if we look at the evolution of a signal *x(t)* between two consecutive extrema (say, two minima occurring at times t_- and t_+), we can heuristically define a (local) high-frequency part $\{d(t), t_- \leq t \leq t_+\}$, or local *detail*, which corresponds to the oscillation terminating at the two minima and passing through the maximum which necessarily exists in between them. For the picture to be complete, one still has to identify the corresponding (local) low-frequency part *m(t)*, or local trend, so that we have $x(t) = m(t) + d(t)$ for $t_- \leq t \leq t_+$. Assuming that this is done in some proper way for all the oscillations composing the entire signal, the procedure can then be applied on the residual consisting of all local trends, and constitutive components of a signal can therefore be iteratively extracted.

Given a signal *x(t)*, the effective algorithm of EMD can be summarized as follows:

1. Identify all extrema of *x(t)*.
2. interpolate between minima (resp. maxima), ending up with some envelope $e_{min}(t)$ (resp. $e_{max}(t)$)
3. Compute the mean,
   $m(t) = (e_{min}(t)+e_{max}(t))/2$
4. Extract the detail, $d(t) = x(t) - m(t)$
5. Iterate on the residual *m(t)*.

In practice, the above procedure has to be refined by a *sifting* process which amounts to first iterating steps 1 to 4 upon the detail signal *d(t)*, until this latter can be considered as zero-mean according to some stopping criterion. Once this is achieved, the detail is referred to as an *Intrinsic Mode Function* (IMF), the corresponding residual is computed and step 5 applies. By construction, the number of extrema is decreased when going from one residual to the next, and the whole decomposition is guaranteed to be completed with a finite number of modes.

IV. PROPOSED SYSTEM

The real time speech signal (i.e. a recorded audio) is mixed with the chaotic signal (generated by Gingerbreadman Map) with added noise at the transmitter side. The noise level can be set according to the requirement. Then, the audio signal is separated by the Iterated Filtering Algorithm at the receiver side. The Fig.1 depicts the above.

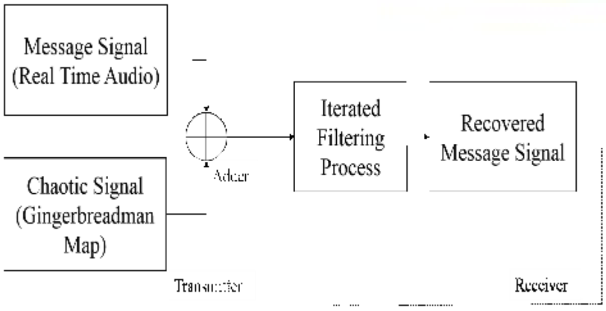
Message Signal (Real Time Audio)
Chaotic Signal (Gingerbreadman Map)
Adder
Iterated Filtering Process
Recovered Message Signal
Transmitter
Receiver

Fig.1 – Block Diagram

Here, the real time audio signal can be a recorded voice (speech) from a recording device viz. Mobile phones, etc. This audio file is given as input to the MATLAB. When it is displayed in the graphical form, it looks like the following figure.

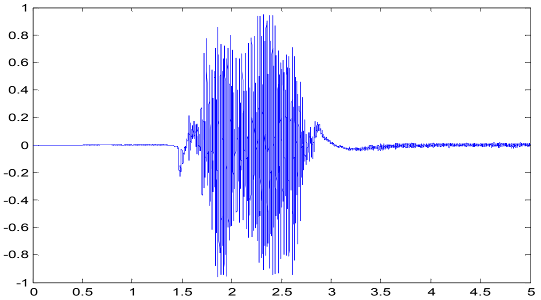

Fig.2 – Input Signal (Audio)

Now, The chaotic signal is required to add it with the audio. It is generated using Gingerbreadman Map.

V. GINGERBREADMAN MAP CHAOTIC SYSTEM

In dynamical systems theory, the Gingerbreadman map is a chaotic 2D map. It is given by the transformation (1) and (2):

$$x_{n+1} = 1 - y_n + |x_n| \tag{1}$$

$$y_{n+1} = x_n \tag{2}$$

This describes the sensitivity of the initial conditions in a chaotic system. A consequence of sensitivity to initial conditions is that if we start with only a finite amount of information about the system, then beyond a certain time, the system will no longer be predictable.

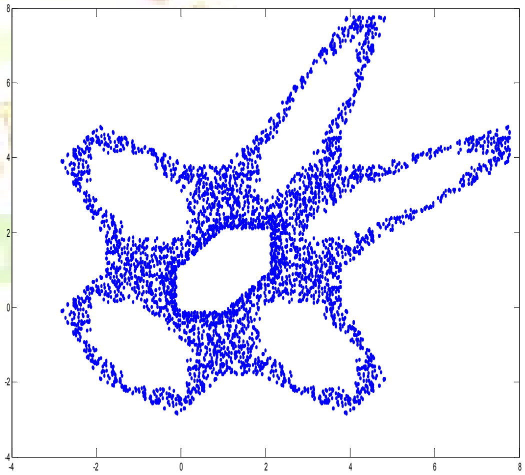

Fig.3 – Gingerbreadman Map

As the Gingerbreadman Map has been already available, it is easily predictable. Thus, in order to make it more complicate, the initial values are changed and an additional noise of known level is added to it. Now, the Gingerbreadman Map looks like the following Fig.4.

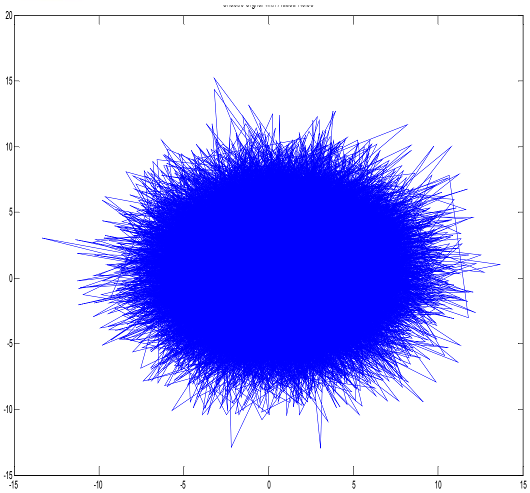

Fig.4 – Gingerbreadman Map with Added Noise

VI. Mixing of Audio Signal with the Chaotic Signal

The input audio signal is mixed with the above generated chaotic signal. This will hide the original signal. The plot of the mixed signal is shown by Fig.5.

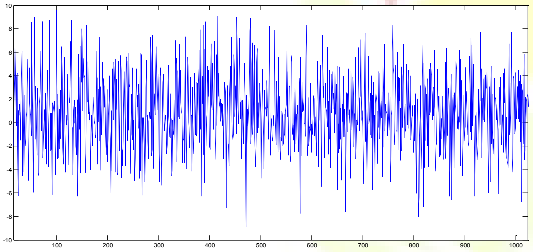

Fig.5 – Mixed Signal

Here, the information is hidden to the outside world. Thus, this signal is transmitted from the sender side which can be wired or wireless transmission.

VII. Iterated Filtering Algorithm – Receiver

The transmitted signal is received at the receiver side. In order to recover the original message signal from the received signal, the Iterated Filtering Algorithm is employed. Here, Weighted Iterative Truncated Mean Filter requires the mean and weighted mean filter values. Thus, these are first calculated.

In general, a filter output is the result of an operation on a group of inputs within a filter window. Suppose, the filter window contains n inputs residing in a data set $x_o = \{x_i\}$, $1 \leq i \leq n$. The mean and median filters, respectively, produce outputs μ_o=mean(x_o) and

$$\phi = \arg\min_{\varphi} \sum_{i=1}^{n} |x_i - \varphi|$$

In general, the outputs of mean filter μ_o and median filter □ are different. Changing the stopping criteria of the iteration, the filter can produce an output closer to the arithmetic mean.

B. Outline of the Iterative Truncated Mean Filter (ITM)

Starting from $x = x_o$, the ITM algorithm consists of three steps:

1. Compute the arithmetic mean, i.e.,
   μ = mean(x)
2. Compute dynamic threshold τ and truncate input data set $x = \{x_i\}$ by:
   $$x_i = \begin{cases} \mu + \tau, & \text{if } x_i > \mu + \tau \\ \mu - \tau, & \text{if } x_i > \mu - \tau \end{cases}, \ 1 \leq i \leq n$$
3. Return to step 1. if stopping criterion S is violated. Otherwise, terminate the iteration.

The weighted mean is the maximum likelihood (ML) estimate of location for data sets with Gaussian distribution. Assume a filter window contains n independent Gaussian distributed samples as $x_o = \{x_1, x_2,.....x_n\}$ with unknown constant mean μ_o. The variance of the ith sample is σ_i^2. The ML estimate of location μ_o is to find the value of μ, which maximizes the likelihood function. Now, the truncation procedure of the ITM filter is caried out.

C. Truncation procedure of the ITM Filter

Input: $x_o = x$; Output: Truncated x;

1. Compute the sample mean:
   μ = mean(x);
2. Compute the dynamic threshold:
   τ = mean(x - μ);
3. $b_l = \mu - \tau$, $b_u = \mu + \tau$, and truncate x by:
   $$x_i = \begin{cases} b_u, & \text{if } \ x_i > b_u \\ b_l, & \text{if } \ x_i < b_l \\ x_i, & \textit{otherwise} \end{cases}$$
4. Return to step 1, if stopping criterion S is violated. Otherwise, terminate the iteration.

The weighted Iterative Truncated Mean filter (WITM) is proposed based on the following theorems 1 and 2.

Theorem 1: For any finite data set $x = \{x_1, x_2,......x_n\}$ and weight set $w = \{w_1, w_2, ...w_n\}$ with all weights being non-negative rational numbers, the difference between the weighted mean μ_w and weighted median □$_w$ is never great than the weighted mean absolute deviation τ_w. The corresponding formula is:

$$|\phi_w - \mu_w| \leq \tau_w \triangleq \sum_{i=1}^{n} w_i |x_i - \mu_w| \Big/ \sum_{i=1}^{n} w_i$$

Theorem 2: For any finite data set x and weight set w, there exists at least one sample whose distance from the weighted mean μ_w is greater than the weighted mean absolute deviation τ_w if the weighted mean μ_w deviates from the weighted median □$_w$, i.e.,

$$x_i, x_i \in x, \text{ that } |x_i - \mu_w| < \tau_w, \text{ if } \mu_w = □_w$$

D. Truncation procedure of the WITM Filter

Input: w,x$_o$ ⇒ x ; Output: Truncated x;

```
1. Compute the weighted mean:
     $\mu_w = \sum_{i=1}^{n} w_i x_i / \sum_{i=1}^{n} w_i$;
2. Compute the weighted dynamic threshold:
     $\tau_w - \sum_{i=1}^{n} w_i |x_i - \mu_w| / \sum_{i=1}^{n} w_i$;
3. $b_l = \mu_w - \tau_w$, $b_u = \mu_w + \tau_w$, and truncate x by:
     $x_i = \begin{cases} b_w, & \text{if } x_i > b_u \\ b_l, & \text{if } x_i < b_l \\ x_i, & otherwise \end{cases}$
4. Return to step 1. if stopping criterion $S$ is violated.
   Otherwise, terminate the iteration.
```

VIII. Simulation Results

The mixed signal is passed through the mean and weighted mean filters in order to obtain the mean and weighted mean. After that, these are given as input to the Weighted Iterative Truncated Mean Filter, which recovers the audio. The mean and weighted mean filter outputs are shown below.

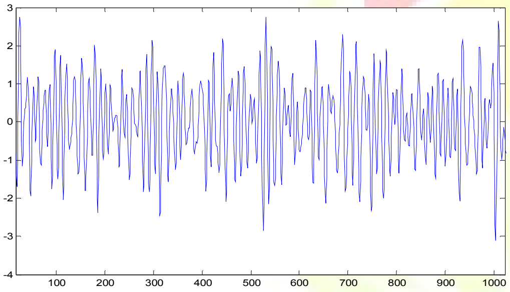

Fig.6 - Mean Filter Output

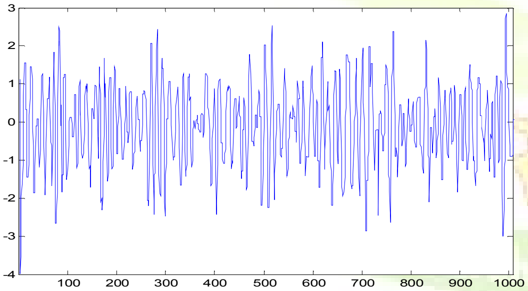

Fig.7 – Weighted Mean Filter Output

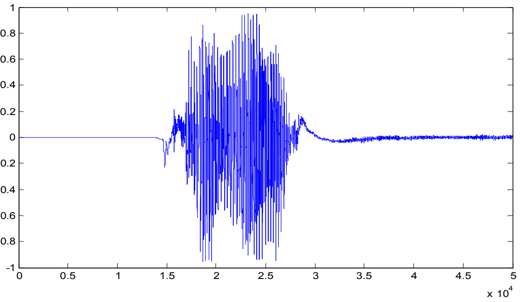

Fig.8 – Weighted Iterative Truncated Mean Filter Output

Thus, the Weighted Iterative Truncated Mean Filter (WITM) recovers the original message i.e. speech signal from the mixed signal. The Fig.8 shows the recovered signal which is similar to the initial input signal.

IX. Conclusion

In this project we have provided an alternative algorithm for the empirical mode decomposition (EMD) using iterative filters (IFs). This alternative approach replaces the mean of the spline-based envelopes in the original sifting algorithm by an adaptively chosen moving average. The use of a moving average allows in many cases for a more rigorous mathematical analysis of this proposed alternative EMD.

Thus, the security of the speech information can be achieved by using this iterated filtering technique. It can be used in the simple communication process between two ends where we need to hide the information. The future work of this project includes the increasing the speed of the process in order to bring it in a real time conversation. Also, the use of other different chaotic systems may improve the efficiency of this process.

References

[1]. Zhenwei Miao and Xudong Jiang, "Weighted Iterative Truncated Mean Filter", IEEE Transactions on Signal Processing, Vol. 61, No. 16, August 15, 2013.

[2]. Z. W. Miao and X. D. Jiang, "Further properties and a fast realization of the iterative truncated arithmetic mean filter," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 59, no. 11, pp. 810–814, Nov. 2012.

[3]. S. W. Lee, Frank K. Soong and P. C. Ching, "An Iterative Trajectory Regeneration Algorithm for Seperating Mixed Speech Sources", 1-4244-0469-X/06/$20.00 ©2006 IEEE.

[4]. Cristobald de Kerchove and Paul Van Dooren, "Iterative Filtering for a Dynamical Reputation System", Université catholique de Louvain, Dept. of Applied Mathematics, Av. Georges Lemaître 4, B-1348, Louvain-la-Neuve, Belgium.

[5]. Steffen Bittner, Peter Zillmann and Gerhard Fettweis, "Iterative Correction of Clipped and Filtered Spatially Multiplexed OFDM Signals", Vodafone Chair Mobile Communications Systems, Technische Universit¨at Dresden, D-01062 Dresden, Germany.

[6]. Luan Lin, Yang Wang, And Haomin Zhou, "Iterative Filtering as an Alternative Algorithm for Empirical Mode Decomposition".

[7]. Qu Shao-cheng, Wang Xiao-yan and Gong Mei-jing, "Secure Communication Based on Synchronization of Unified Chaotic Systems", Department of Information and Technology, Huazhong Normal University, Wuhan Hubei 430079, China.

[8]. SHEN Li-Qun, MA Jian-Wei, LIU Lu, DU Hong-Yue and ZHANG Peng, "Adaptive Sliding Mode Synchronisation of a Class of Chaotic Systems and its Application in Secure Communication", Proceedings of the 32nd Chinese Control Conference, July 26-28, 2013, Xi'an, China.

[9]. S. Akkoul, R. Ledee, R. Leconge, and R. Harba, "A new adaptive switching median filter," IEEE Signal Process. Lett., vol. 17, no. 6, pp. 587–590, Jun. 2010.

[10]. W. Wang and P. Lu, "An efficient switching median filter based on local outlier factor," IEEE Signal Process. Lett., vol. 18, no. 10, pp.551–554, Oct. 2011.

[11]. J. Chen and M. Jegen-Kulcsar, "The empirical mode decomposition (EMD) method in MT data processing", SFB 574 IFM-GEOMAR Wischhofstr.1-3, 24148, Kiel, Germany.

[12]. Gabriel Rilling, Patrick Flandrin and Paulo Goncalves, “On Empirical Mode Decomposition and its Algorithms”, Laboratoire de Physique (UMR CNRS 5672), ´Ecole Normale Sup´erieure de Lyon 46, all´ee d’Italie 69364 Lyon Cedex 07, France.

[13]. S. W. Lee, Frank K. Soong, and P.C. Ching, “An Iterative Trajectory Regeneration Algorithm for separating Mixed Speech Sources”, The Chinese University of Hong Kong, China.

[14]. P. Flandrin, G. Rilling, and P. Gonalv´es, “Empirical mode decomposition as a filter bank”, IEEE Signal Processing Lett. 11 (2004), pp 112-114.

[15]. P. Flandrin, P. Gonalv´es and G. Rilling, “EMD equivalent filter banks, from interpretation to applications, in Hilbert-Huang Transform : Introduction and Applications”, N. E. Huang and S. Shen Ed, World Scientific, Singapore (2005), pp 67–87.

[16]. Z. Wu and N. E. Huang, A study of the characteristics of white noise using the empirical mode decomposition method, Proc. Roy. Soc. London 460A (2004), pp 1597–1611.

[17]. D. Pines and L. Salvino, “Health monitoring of one dimensional structures using empirical mode decomposition and the Hilbert-Huang Transform”, Proceedings of SPIE 4701(2002), pp 127-143.

[18]. R. Meeson, “HHT Sifting and Adaptive Filtering, in Hilbert-Huang Transform : Introduction and Applications”, N. E. Huang and S. Shen Ed, World Scientific, Singapore (2005), pp 75–105.

[19]. N. Huang et al, “The empirical mode decomposition and the Hilbert spectrum for nonlinear nonstationary time series analysis”, Proceedings of Royal Society of London A 454 (1998), pp 903-995.

[20]. Yu Na, Ding Qun, “Synchronization of chaotic system with different structure and its application in secure communication”, Communication journals, 2007,Vol. 28, No.10, pp. 73-78.

Mr. P. Karthik was born on 31st July 1982. He did his B.E – ECE in Franxis Xavier Engineering College, M.S. University in 2004 and M.E (Computer and Communication Engineering) in Hindustan College of Engineering and Technology in the year 2010. He is currently working as Assistant Professor in Department of Electronics and Communication Engineering in SNS College of Engineering. His area of specialization is Communication and published papers in several National and International Conferences and Journals

Mr. D. Gokul Prashanth was born on 12th December 1992. He is currently pursuing his B.E – ECE in SNS College of Engineering, Coimbatore. His area of interest is Communication. He published paper in National Conference ‘TAPSA’15’ at Sri Krishna College of Engineering and Technology, Coimbatore.

Mr. T. Gokul was born on 21th June 1993. He is currently pursuing his B.E – ECE in SNS College of Engineering, Coimbatore. His area of interest is Communication and also includes programming. He published paper in National Conference ‘TAPSA’15’ at Sri Krishna College of Engineering and Technology, Coimbatore.