Encrypting Digitized Voice Signals using the Chaotic Behavior of a Nonlinear Discrete Time Dynamical System

Manju Pandey

***Abstract* — A method for the encryption and decryption of voice signals using the chaotic dynamic behavior exhibited by a nonlinear discrete time dynamical system has been proposed. A chaotic cipher for digitized voice signals has been designed and the encryption and decryption processes have been tested on a sample voice signal, i.e., "hello". The nonlinear discrete-time dynamical system considered for encryption in the present paper is the Duffing's map which is a nonlinear differential equation of order two modeling an oscillator.**

***Index Terms*—Chaos, Nonlinear Dynamical System, Discrete Time Signal, Encryption and Decryption**

I. Introduction

Voluminous voice traffic moves over digital networks in this era of ubiquitous multimedia and wireless communication. The security threats involved in voice based communication systems include eavesdropping, modification, interruption / denial / abuse of service, social reputation threats, physical access threats, etc. Voice is extremely sensitive in defence related communication applications where it has operational implications. Other application domains where it is important to protect voice data include sensitive communications over IP systems, phone banking, interactive voice response systems, teleconferencing, stock market related telephony services, news, etc. The integrity of the voice data and the privacy concerns of the individuals involved need to be protected.

Ciphony [1] is a branch of cryptography which is concerned with securing voice communication through encryption over different voice communication modes like for example, telephony, radio, IP etc. Ciphony is very important in all forms of wired and wireless voice communication. It is used for ensuring the security and privacy of real-time and recorded voice signals. In digital ciphony, the focus is on sampled and quantized, i.e., digitized voice signals.

An emerging research area in cryptography is the exploration of the chaotic dynamics exhibited by nonlinear dynamical systems for encryption [2][3][4]. Some researchers have begun to explore the potential application of such chaos based encryption systems for ciphony. Many nonlinear systems exhibit chaotic dynamical behavior. This chaotic dynamical behavior has some very interesting statistical properties which make it well suited for the design of hard-to-crack ciphers in cryptography.

In this paper, a method for the encryption of recorded digitized voice signals using the chaotic dynamics which is exhibited by a nonlinear discrete time dynamical system is discussed. A proof-of-concept demonstration of the encryption and decryption of a digitized voice signal using a chaotic cipher has been carried out by the author.

Manuscript received Jan 05, 2016; revised Apr 08, 2016.
Manju Pandey is with the National Institute of Technology, Raipur, Chhattisgarh, India (e-mail: mpandey.mca@nitrr.ac.in).

II. Chaotic Sequences

A. Chaotic Dynamics and Maps

Chaotic dynamics is exhibited by certain nonlinear dynamical systems [2][3][4]. The dynamical behavior i.e., the behavior with respect to time, of systems which exhibit chaos is extremely sensitive to even infinitesimal changes in the initial conditions. This behavior is so pronounced that even in the absence of any random element or source of randomness, it becomes next to impossible to make any future predictions in the case of such systems. This is so even though the future states of these systems can be fully determined by their initial conditions. Even extremely small changes in the initial states of such systems are likely to produce large divergences as the time steps increase. In popular parlance, this behavior is known as the butterfly effect [5]. In technical terms, such behavior is referred to as deterministic chaos. There are examples of many model nonlinear systems [2] in physics, chemistry, biology, climate modeling, engineering, etc. which exhibit chaotic behavior.

A chaotic map is an evolution function that exhibits chaotic behavior. Chaotic maps may use continuous time or discrete time parameters. Discrete maps usually appear as iterated functions. Chaotic maps frequently appear in the study of dynamical systems.

B. Statistical Properties of Chaotic Sequences

Presented below are some of the statistical properties of chaotic dynamical systems and maps [6] which make them particularly well suited for the design of hard-to-crack cryptographic ciphers.

Ergodicity: An ergodic system is a dynamical system which exhibits the same behavior averaged over time as averaged over the space of all the system's states.

Determinism: A unique set of initial states leads to a

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

unique set of final states

Unpredictability: The output is unpredictable even if there are infinitesimal changes in the initial state

Aperiodicity: Systems exhibiting periodic behavior tend to repeat their dynamics after fixed intervals of time known as periods. The pseudo-random sequence generated by a nonlinear dynamical chaotic system is non periodic or aperiodic for all practical purposes whereas the relaxed requirement in cryptography is that of long periodicity.

Cryptography with chaos has been discussed in [7] and [8]. In [9] a chaos based image encryption system has been discussed.

III. METHOD

A. Voice Signal Acquisition

The voice signal taken for the study is a waveform recorded on a Microsoft® Windows® XP Personal Computer using the Sound Recorder® accessory. The PC is Lenovo® brand with the hardware based on the Intel® Pentium® Dual CPU E2160 @ 1.80 GHz with 2.99 GB of RAM. The default SoundMAX® Integrated Digital High Definition Audio Hardware has been used. The voice sample recorded is a simple "Hello" speech signal. An off-the-shelf Logitech® microphone which is part of a simple headphone set has been used for recording the "Hello" sound sample. This sample is stored, by default, by the Sound Recorder, in the Waveform Audio File i.e., WAVE format which is more commonly known as the WAV format, after its .wav extension.

The WAVE [10][11][12] sometimes referred to as Audio for Windows [13] is an audio file format standard defined by Microsoft and IBM. This standard has been defined for the storage of audio bitstreams on Personal Computers. This format uses the Resource Interchange File Format (RIFF) bitstream format method and stores the audio data on the secondary storage device in chunks. The WAV file format is the primary format used on Microsoft Windows systems for raw and usually uncompressed audio. The bitstream encoding method typically employed by this standard is the linear pulse-code modulation.

B. Waveform of Voice Signal

Fig. 1 shows 40000 time steps of the "Hello" voice signal between t=30,000 and t=70,000.

C. Duffing's Equation and Map

The Duffing equation models the Duffing oscillator [14]. It is a second order nonlinear differential equation which is applied for the modeling of certain damped and driven oscillators and has the following form

$$x'' + \delta x' + \alpha x + \beta x^3 = \gamma \cos(\omega t) \qquad (1)$$

where the unknown function $x = x(t)$ is the displacement at time t. x' is the first derivative of x with respect to time, i.e., velocity and x'' is the second derivative of x with respect to time, i.e., acceleration. The numbers $\delta, \alpha, \beta, \gamma, \omega$ are constants.

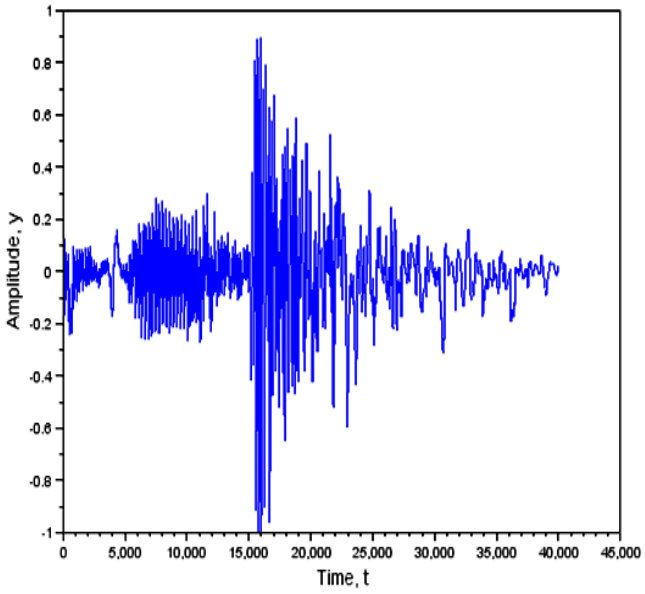

Fig. 1. 30,000-70,000 Time Steps of "Hello"

The Duffing map which is also known as the Holmes map is a nonlinear discrete time dynamical system. The Duffing map is a discrete version of the Duffing equation. The Duffing map transforms a point in the plane to a new point given by

$$x_{n+1} = y_n$$
$$y_{n+1} = -bx_n + ay_n - y_n^3 \qquad (2)$$

As can be seen from the above equations, there are two constants a and b which are usually set to a=2.75 and b=0.2 for chaotic behavior. The Duffing's map has been chosen in this work for the purpose of encrypting voice signals.

D. Duffing's Sequence

Fig. 2 shows the pseudo-random sequence generated by the y-variable in the Duffing's map. For the generation of this sequence the values of the constants are set as a=2.75 and b=0.2, and the initial values x(0)=0.1 and y(0)=0.1, respectively. Fig. 2 shows the first 500 time steps of the Duffing's sequence. Note the seemingly random behaviour of the sequence as well as the aperiodicity.

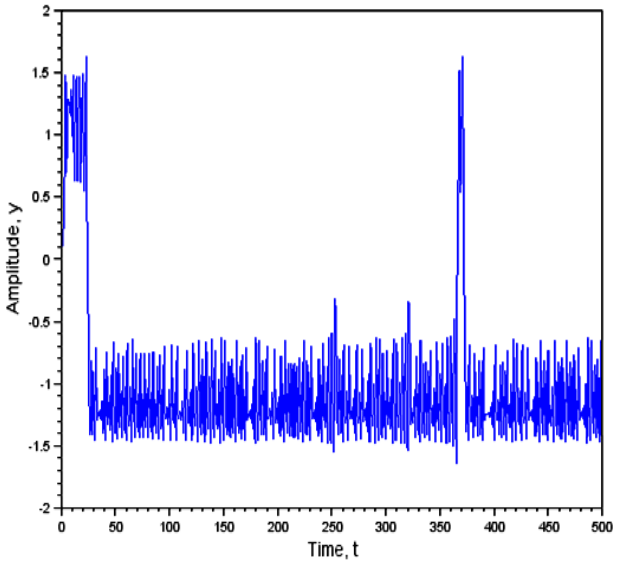

Fig. 2. First 500 time steps of Duffing's Sequence

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

IV. Results and Discussion

A. Encryption of Voice Signal

Fig. 3 depicts the encryption process of the voice signal through a simple block diagram. The encrypted sequence or signal **E**(t) is a linear addition of the voice sequence **V**(t) and the chaotic sequence, **C**(t). The encryption key or the cipher, K is used for generating the Duffing's chaotic sequence **C**(t). Additive mixing of the original voice signal, **V**(t) is done with Duffing's chaotic sequence **C**(t) in order to generate the encrypted voice signal, **E**(t).

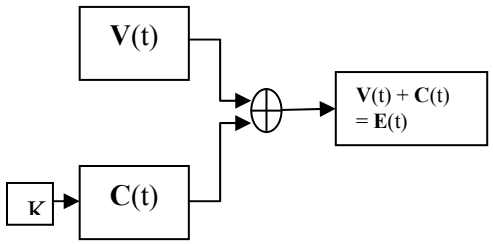

Fig. 3: Block Diagram of the Encryption Process

Fig. 4 depicts the encryption of the "Hello" voice signal with an equivalent number of time steps of the Duffing's map. Some 25000 time points are shown for clarity. This represents the encrypted voice signal. It is not possible for an attacker to recover the original voice signal v(t) from the encrypted signal e(t) which unless he knows the cipher or the key for decryption. Guessing the keys is extremely difficult for the attacker because of the unpredictability and aperiodic statistical properties of the Duffing's map. Therefore, even if the initial key guessed by the attacker is quite close to the actual keys, the butterfly effect will ensure that the system dynamics and the trajectories are vastly different making cryptanalysis almost impossible through a series of guesses. This combined with the ease of generation of the pseudo-random sequence and mixing it with the voice signal makes it a very powerful encryption method suited for ciphony applications.

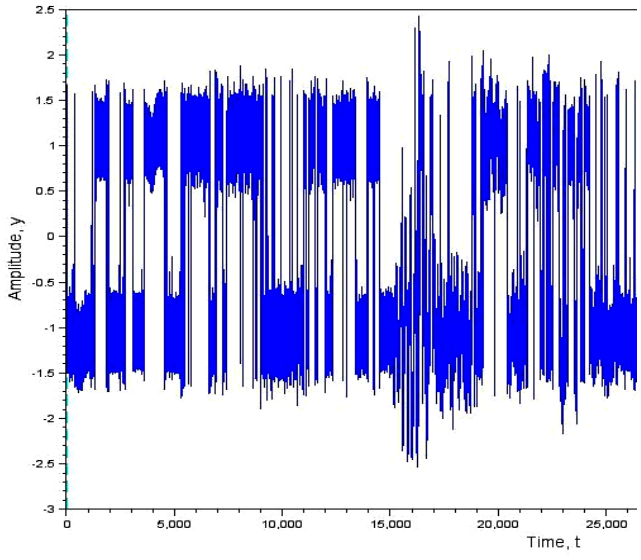

Fig. 4: "Hello" Signal on encryption with the Duffing's Map

B. The Chaotic Cipher

A chaotic map, like for example, the Duffing's map has to be agreed upon / exchanged by two communicating parties, say Alice and Bob. The key then comprises of the following parameters:

a. Values of the constant parameters in the chaotic model, like *a* and *b* in the Duffing's Map
b. Initial values of the variables, like x(0) and y(0) in the Duffing's Map

Fig. 5 shows the key/cipher construction in the case of the Duffing's map.

a=2.75	*b=0.2*	*x(0)=0.1*	*y(0)=0.1*

Fig. 5: Key construction in the case of Duffing's Map

C. Decryption

On the receiver's side, the encrypted voice signal can be decrypted by Bob by reversing the sequence of operations (see Fig. 6 for the block diagram). In this case Bob is required to run the Duffing's Map using the constant and initial values supplied to him in the key. Subsequently he has to recover the original voice signal by subtracting the Duffing's chaotic sequence from the encrypted signal.

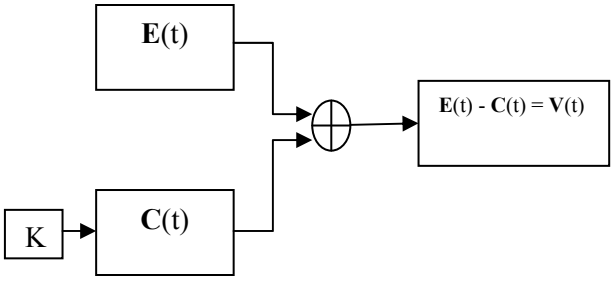

Fig. 6: Block Diagram of the Decryption Process

V. Conclusions

A chaotic cipher for voice signals based on the discrete time nonlinear dynamical Duffing Map has been designed. The encryption of a voice signal has been performed and is found to be working consistently. It is easy to decipher the original voice signal from the encrypted signal provided the key is known. The key in this case comprises of the values of the constants in the Duffing's Map and the initial values of the variables. This can be applied for end-to-end encryption in voice communication systems. It is very difficult for an eavesdropper to recover the original voice signal without knowing the key values initially. The choice of the chaotic map and the key requires further research. Further work is also required on the choice of a more sophisticated mixing model of the original voice signal with the chaotic sequence.

References

[1] Chandran, A.K., Sreedhar, S., 2014, Secure Speech with LFSR. International Journal of Research in Engineering and Technology, 3(1), 48-52
[2] Strogatz S., 1994, Non-Linear Dynamics and Chaos, Perseus Books, Massachusetts
[3] R. Devaney, 1992, A First Course in Chaotic Dynamical Systems, Perseus Books

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[4] Li, S., Mou, X, Cai, Y., 2003, Chaotic Cryptography in Digital World: State-of-the-Art, Problems and Solutions", http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=D81FB0027B692CBBC8B5D358D5C084FE?doi=10.1.1.5.9967&rep=rep1&type=pdf
[5] Boeing, 2015, "Chaos Theory and the Logistic Map". July 16, 2015, http://geoffboeing.com/2015/03/chaos-theory-logistic-map/
[6] Carmen, P.L., Ricardo, L.R., Notions of Chaotic Cryptography: Sketch of a Chaos based Cryptosystem, http://arxiv.org/ftp/arxiv/papers/1203/1203.4134.pdf
[7] Lawande, Q.V., et. al., 2005, Chaos-Based Cryptography: A New Approach to Secure Communications. BARC Newsletter, 58, 1-11
[8] Makris, G., Antoniou, I., June 2012, Cryptography with Chaos, Proceedings of the 5th Chaotic Modeling and Simulation International Conference, Athens, Greece
[9] Guan Z. H., Huang F., Guan W., 2005, Chaos-based image encryption algorithm. Physics Letters A, 346(1-3), 153-157
[10] IBM Corporation and Microsoft Corporation, August 1991, "Multimedia Programming Interface and Data Specifications 1.0", http://www.tactilemedia.com/info/MCI_Control_Info.html
[11] Library of Congress, Sept. 2008. "WAVE Audio File Format". http://www.digitalpreservation.gov/formats/fdd/fdd000001.shtml
[12] Microsoft Corporation, June 1999, "Waveform Audio File Format, MIME Sub-type Registration - INTERNET-DRAFT". IETF. http://tools.ietf.org/html/draft-ema-vpim-wav-00.
[13] "Information about the Multimedia file types that Windows Media Player supports". Microsoft Help and Support. Microsoft Corporation. (May 12, 2008). https://support.microsoft.com/en-us/kb/316992.
[14] Rand, R.H., 2005, Lecture Notes on Nonlinear Vibrations, http://www.math.cornell.edu/ ~rand/randdocs/nlvibe52.pdf W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)