International Journal of
Applied Mathematics,
Electronics and Computers
ISSN: 2147-8228 http://ijamec.atscience.org
Advanced Technology and Science
Original Research Paper

Chaotic Encryption Based Data Transmission Using Delta and Delta-Sigma Modulators

Günyaz Ablay*[1]

Accepted 3rd September 2016

Abstract: Delta and Delta-Sigma modulation methods have been getting a great interest recently due to the great progress in analog-digital very large scale integration technology. Since the outputs of these methods are digital, the data can be securely encrypted using very simple standard hardware. In this work, a chaotic random bit generator based approach for encrypting digital data of the delta and delta-sigma modulators is studied. The chaotic bit generation can easily be implemented in the digital hardware of the modulators due to simplicity of the chaotic dynamics. The randomness of the generated chaotic bits are proved with visual and statistical tests. The security of the proposed approach is evaluated via key space estimation based attacks. The efficiency of the methods is validated with simulations.

Keywords: *Chaos, delta modulation, delta-sigma modulation, random bits, cryptography, communication.*

1. Introduction

The delta (Δ) and delta-sigma (ΔΣ) modulators offer simple, efficient methods for telecommunication and signal processing applications. The Δ modulation systems have gained significance in recent years due to their very simple hardware structure, digital transmission and easy to add adaptive features. In addition ΔΣ modulators have noise shaping feature that makes them well-suited for low-frequency, high-accuracy measurements. There are many applications of Δ modulators including reliable voice communications, analog-to-digital signal conversion, performing audio delay lines, telemetry systems and feedback power control in code-division multiple-access radio communication systems [1]–[5]. The Δ modulation systems, a type of variable structure control, are also getting a special interest in the control community [6]–[10]. Other recent studies on Δ modulators have been focused on multibit modulation, chaotic modulation, chaotification and tone suppression in communications [11]–[17]. The digital output of the Δ modulation systems can be encrypted by using chaotic systems. Since chaotic dynamics have strong similarities with the cryptography, e.g. aperiodicity, deterministic dynamics, ergodicity and sensitivity to initial conditions, they have recently been utilized in cryptosystems [18]–[23]. To encrypt the Δ modulation systems, while the required random bits can be generated from a hardware-based generator (e.g., using thermal noise [24] and radioactive decay [25]) or from software-based generators (e.g., linear congruential generators [26]), chaotic systems are very simple to realize and offer a hybrid structure with the features of hardware and software based approaches [27]–[30]. The number of the chaotic systems have been increased over time in the literature, which allows us to benefit from chaotic dynamics for generating efficient chaotic random bits for use in cryptographic applications [31]–[35].

In this work, a chaotic random bit generator is developed and integrated into the Δ and ΔΣ modulators for data encryption. The goal is to provide security in such systems during data transmissions. The Δ modulation systems offer low cost solutions with a strong immunity against crosstalk and noise in the transmission line, and integration of the chaos into these systems will enhance reliability and security.

In the following sections, the delta modulation methods are overviewed and a chaotic map based encryption scheme is applied to digital outputs of the Δ and ΔΣ encoders.

2. Chaotic Data Encryption For Δ And ΔΣ Modulation

Chaotic systems are able to provide diffusion and confusion, i.e., hiding and spreading plaintext over the ciphertext, and for this reason have potential applications in some functional blocks of communication systems including encryption, modulation and compression. By considering a delta modulation scheme, the chaotic random bits can easily be used for encrypting digital plaintext for secure communications. Figure 1 shows a chaos based digital data encryption and decryption approach for Δ modulators.

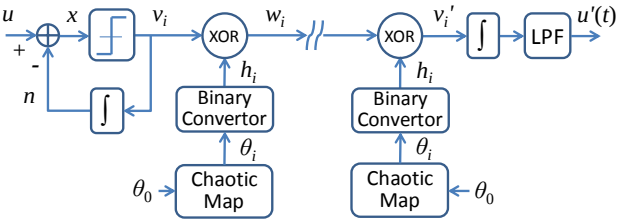

Figure 1. Chaos based encryption for delta modulation system

Similarly, the chaotic bits can also be incorporated into digital output of the ΔΣ modulator and demodulator systems for securing the data as illustrated in Figure 2. In data encryption the exclusive-or (XOR) logical function is used. The Δ modulated signals are easily demodulated at the receiver by using a low pass filter, but now with the chaotic encryption, it is not possible to extract message without correct chaotic decrypter with correct initial conditions and parameter values.

It is interesting to note that many applications have statistically smaller amplitudes at higher frequencies, e.g. voice communications, an integrator time constant of around 1ms is satisfactorily reproduce voice in a 3kHz bandwidth [3]. Hence, applications of delta modulation include telecommunications, secure communications, audio delay lines and voice input/output in data processing. The delta modulation systems offer simple, robust and low cost solutions for such applications.

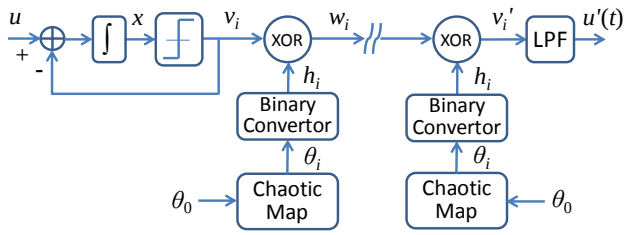

Figure 2. Chaos based encryption for delta-sigma modulation system

2.1. Δ and ΔΣ Modulators

Today, digital techniques are dominating signal processing. The Δ modulation systems have an important place in the digital signal processing area with simple, efficient solutions. For example the ΔΣ analog-to-digital converters are ideal for many applications whose signal frequencies vary from dc to several hundred megahertz. These approaches are composed of an oversampling modulator followed by a digital filter that together generates a high-resolution digital data streams. Typically, a Δ modulator with one bit quantization requires a resolution on the order of 14–20 bits (e.g., around 100 kbit/s for a voice bandwidth of 4 kHz). The main working principle of the Δ modulator is illustrated in Figure 3. The modulator is simply a sampled data system employing a negative feedback loop via integration. A one-bit quantizer (or comparator) senses if the instantaneous level of the analog input is greater or less than the feedback signal and produces a continuous non-return-to-zero digital data stream. The negative feedback loop integrates the digital data to form an approximation of the input signal. It is also quite simple to demodulate the input signal by using an identical integrator and a low pass filter (LPF). The ΔΣ modulator has a simpler structure at the demodulator by having only a low pass filter.
By considering Figure 1, the equations of the delta modulator are given by

$$\dot{x}(t) = \dot{u}(t) - \delta \,\text{sign}(x(t)) \tag{1}$$

where $u(t)$ is the input signal, $n(t)$ is the integrator output, $x(t)$ is the error signal and the quantization level is given by $\pm\delta$. The sign(.) function is defined by $\text{sign}(x) = 1$ if $x \geq 0$, and $\text{sign}(x) = -1$ if $x < 0$. In order to make the Δ modulator function correctly, the error must be forced to zero in finite time by the feedback signal. To find stability conditions of the Δ modulator, if we define a positive definite Lyapunov function as

$$L = x^2 / 2 \tag{2}$$

Then, the time-derivative of (2) can be written as

$$\dot{L} = x\dot{x} = x\left(\dot{u} - \delta \,\text{sign}(x)\right) \leq -\left(\delta - |\dot{u}|\right)|x| \tag{3}$$

Thus, the modulator is stable if the following condition holds

$$\delta > \max|\dot{u}(t)| \tag{4}$$

The equivalent condition for the discrete-time (sampling) implementations is given by

$$\delta f_s > \max|\dot{u}(t)| \tag{5}$$

where f_s is the sampling frequency. Equation (5) shows that the Δ modulator produces a binary coded output from the time-derivative of the analog input signal.

For ΔΣ modulators seen in Figure 2, since the input signal first passes through an integrator, then the governing equation can be written as

$$\dot{x}(t) = u(t) - \delta \,\text{sign}(x(t)) \tag{6}$$

Similar to (2), if the Lyapunov stability is applied, one can easily obtain the following stability condition

$$\delta f_s > \max|u(t)| \tag{7}$$

Therefore, the ΔΣ modulators have noise suppression advantage compared to Δ modulators because the quantization level is proportional to the amplitude of the input signal (while δ is proportional to the derivative of the input signal in Δ modulators). This noise-shaping feature of the ΔΣ modulators is well suited to signal processing applications, e.g. communication and digital audio.

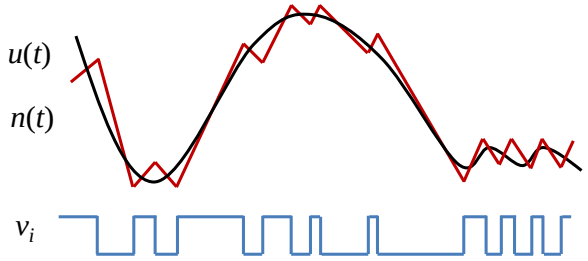

Figure 3. Delta modulation technique

The input message signal is oversampled in the Δ and ΔΣ modulations in order to increase correlation between samples as illustrated in Figure 3. For this reason there are two types of quantization errors: the slope overload distortion (too small δ or sampling) and granular noise (too large δ or sampling). The integrator with a fixed slope may not track the large and high frequency signals, which can cause the slope overload distortion as a critical drawback of the system. The slope overload distortion is eliminated if the condition (5) or (7) is satisfied for the related modulator type. There exist adaptive algorithms for adjusting quantization step size to eliminate quantization errors of the Δ modulator systems. On the other hand, the performance of these modulators is dependent on the quantization and channel noise. The quantization noise averages to zero and can be defined by its root mean square (rms) value for a dynamic input signal by considering its limits $\pm\delta/2$. Thus, the quantization error $x(t)$ is given by

$$x_{rms} = \sqrt{\frac{1}{\delta}\int_{-\delta/2}^{\delta/2} x^2(t)dx(t)} = \frac{\delta}{\sqrt{12}} \tag{8}$$

The noise level is equal to quantization noise of an analog-to-digital converter. For rms value of the input signal $u(t)$, the signal-to-noise ratio (dB) can be given by

$$\text{SNR}(dB) = 20\log\left(\frac{u_{rms}}{x_{rms}}\right) = 20\log\left(\sqrt{12}\,\frac{u_{rms}}{\delta}\right) \tag{9}$$

These results are valid only for uniformly distributed quantization noise and the effect of the slope overload distortion is ignored. The quantization noise remains the same at the demodulator.

2.2. Chaotic Random Bit Generation

Many chaotic systems are available in the literature to serve as a source for chaotic random bit generations for use in encryption/decryption algorithms. For such applications both

continuous-time and discrete-time chaotic systems can be utilized, but the discrete maps are preferred because of their convenience for digital realizations and superior performances. To acquire random bits in a fast, simple way, the robust chaotic maps can be used since they do not have any periodic windows in a large parameter range of the chaotic behaviour. Robust chaotic maps are defined with piecewise linear and discontinuous maps whose Lyapunov exponents are positive throughout the chaotic parameter range [36]. In addition these maps are able to provide statistically uniformly distributed random numbers, which is critical to generated random bits without performing any de-skewing method. Consider a symmetric tent map described by

$$\theta_{i+1} = 1 - \eta|\theta_i| \tag{10}$$

where $\eta = 1.9999$. To show the existence of chaos in the system for $1 < \eta \leq 2$, the Lyapunov exponent and bifurcation diagram of the system are given in Figure 4 for η versus θ_i. The map has a positive Lyapunov exponent (LE) when $\eta > 1$ with a maximum value 0.672. The bifurcation diagram shows that the map has chaos without any periodic windows for a wide range of parameter variations. The map exhibits a robust chaos since the Lyapunov exponent is always positive in the chaotic region.

Even though, statistical tests are not enough to determine the quality of the randomness, they are needed to get an idea. The randomness features of (10) can be evaluated with the visual and test statistics based methods. Visualization is a quick way to get rough information about the chaotic random sequences. The bifurcation diagram and the histogram plot are used for visual evaluations. Figure 5 displays a histogram plot of the chaotic map for 100 categories. The histogram plot shows a uniform distribution over the ± 1 range. This means that the chaotic map with the selected parameter value generates a uniformly distributed random sequence.

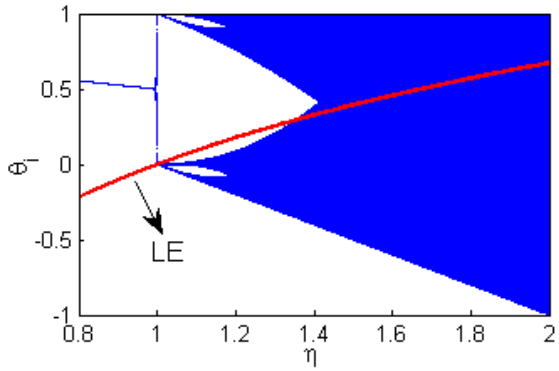

Figure 4. Bifurcation diagram and Lyapunov exponent.

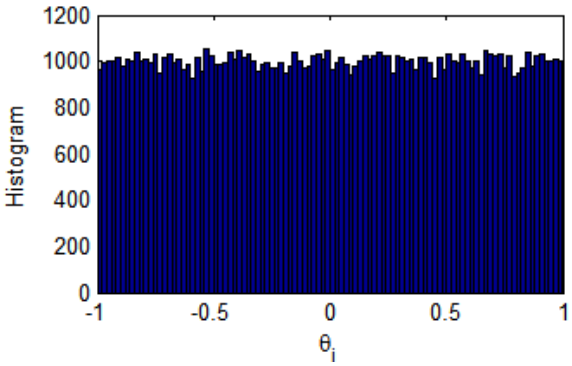

Figure 5. Histogram plot.

Now, since we verify that the chaotic map provides uniformly distributed random numbers, we can generate bits (or binary sequences) from this chaotic map by using a simple comparator defined by

$$h_i = \begin{cases} 1, & \theta_i \geq 0 \\ 0, & \theta_i < 0 \end{cases} \tag{11}$$

The usage of a comparator is a simple, efficient and convenient way to generate binary values from the chaotic source [37]. The chaotic random bits should also be evaluated with some qualitative statistical tests to confirm that the generated random bits are unbiased, uncorrelated random bits. To assess the randomness of the generated random bits, many statistical tests are available in the literature including monobit, serial, overlapping template matching, cumulative sum, poker, autocorrelation, runs, discrete Fourier transform (spectral) and frequency within a block (or block frequency) tests [38]–[40]. These tests are used to determine whether the chaotic random bits are unbiased and uncorrelated. That is to say, the chaotic random bits h_i with security bound S bits should include unbiased bits (probability of 0 and 1 must be equal) and undistinguished bits without performing at least 2^S operations [41]. Even though the statistical tests alone are not enough for such evaluations, it is nice to see that the chaotic bits pass all these statistical tests. Note that for practical applications, application specific tests are usually carried out for randomness analysis. The statistical test results are given in Table 1. It is clear that all tests are successfully passed, and for this reason, the robust chaotic map (10) with the binary converter algorithm (11) produces a highly-satisfactory random bits for use in cryptosystems.

Table 1. Statistical evaluation of the chaotic random bits

Test Name	Test Values	Statistics	Result
Monobit	$q < 3.8415$	$1x10^{-6}$	*success*
Block frequency	$q > 0.01$	0.886	*success*
Runs	$q > 0.01$	0.785	*success*
Fourier transform	$q > 0.01$	0.939	*success*
Autocorrelation	$\|q\| < 1.96$	-1.0135	*success*
Serial	$q < 0.01$	$1x10^{-8}$	*success*
Overlapping	$q > 0.01$	0.998	*success*
Cumulative sums	$q > 0.01$	0.4354	*success*
Poker	$q < 14.067$	9.136	*success*

3. Simulation Results

The Matlab/Simulink based numerical simulation results are given in Figures 6-7. Figure 6 shows the chaotic data encryption in Δ modulator based data transmission results. The message signal which includes ASCII codes of "chaos" is seen in Figure 6a. The digital output of the Δ modulator is displayed in Figure 6b, where there are some windows in the modulated signal. This digital signal can easily be demodulated with an integrator and low-pass filter. To encrypt the modulator output bits, the XOR logic function is used for the chaotic bit sequence and the modulator bits, namely,

$$w_i = v_i \otimes h_i \tag{12}$$

Figure 6c shows the encrypted modulator output bits, which does not have any visual pattern. The same chaotic bit generator is used in the demodulator to decrypt the original modulator output bits and then Δ demodulator is employed to extract the original message signal. The recovered message signal is seen in Figure 6d. which shows a perfect recovery. The security of the scheme is tested with the use of Δ demodulator, low pass filtering and estimated key sequence based tests. In Figure 6e, the test result

for a wrong chaotic key sequence is illustrated. In this test, the same chaotic map and binary convertor algorithm is used. The initial condition of this eavesdropping system is assumed to be estimated with a very small initial condition error, e.g., $\gamma = \theta_0 - \theta_0' = 1\text{x}10^{-7}$, and it is seen in Fig. 6e that the message cannot be recovered. The chaotic maps in the transmitter and receiver must be exactly the same with the same parameters and initial conditions to generate the correct key sequence and to decrypt the correct message.

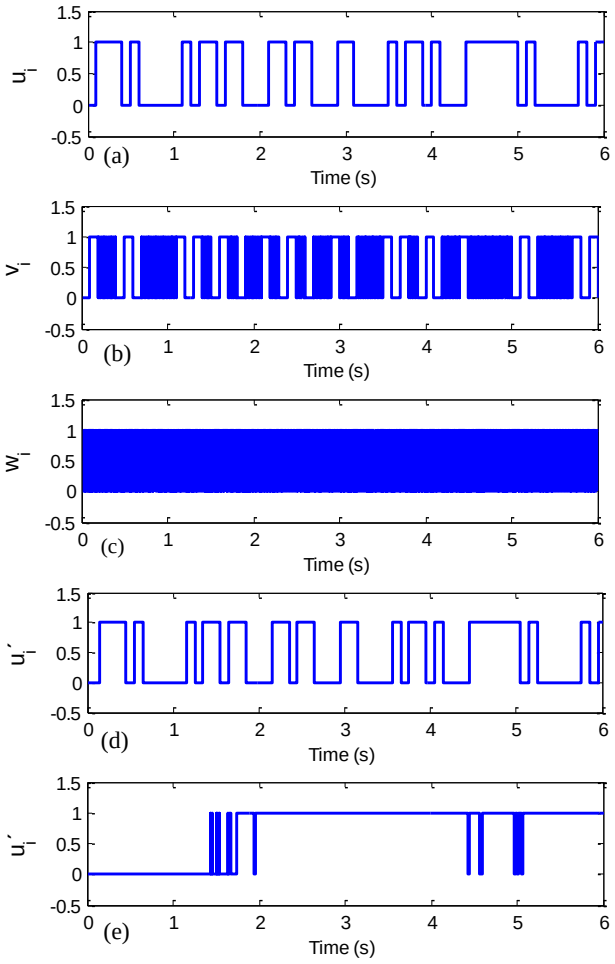

Figure 6. (a) Message bits. (b) Digital delta modulator output. (c) Chaotic bits based encrypted message (transmitted bits). (d) Recovered message bits. (e) Recovered message bits for a wrong chaotic key sequence.

Similarly, the numerical simulation results for the ΔΣ modulator based data transmission are given in Figure 7. The waveform of the first-order ΔΣ modulator is illustrated in Figure 7b when the input signal is a sinusoid as given in Figure 7a. It is should be noted that the modulator performs both the sampling and the quantization operation in this example, which is typical in practical circuit implementations. The ΔΣ modulator output shows that the output is either plus or minus full scale and when the sinusoidal input to the modulator is close to the full scale, the output is either positive or negative during the cycle. It is seen that the local average of the modulator output follows the input signal. When the input signal is around zero, the modulator output changes fast between $\pm\delta$ with nearly zero mean. Therefore, the input signal can easily be recovered by using a low pass filter as demodulator. On the other hand, the chaotic bits based encryption of the modulator output removes all the modulator patterns as seen in Figure 7c. The recovered input signal is seen in Figure 7d. which shows an excellent recovery. To evaluate security of the approach, the test result for a wrong chaotic key sequence is shown in Figure 7e. In this test, the same chaotic map and binary convertor algorithm is used with a very small initial condition error, e.g., $\gamma = \theta_0 - \theta_0' = 1\text{x}10^{-7}$. It is clear from Figure 7e that the message cannot be recovered with such a very small estimation error.

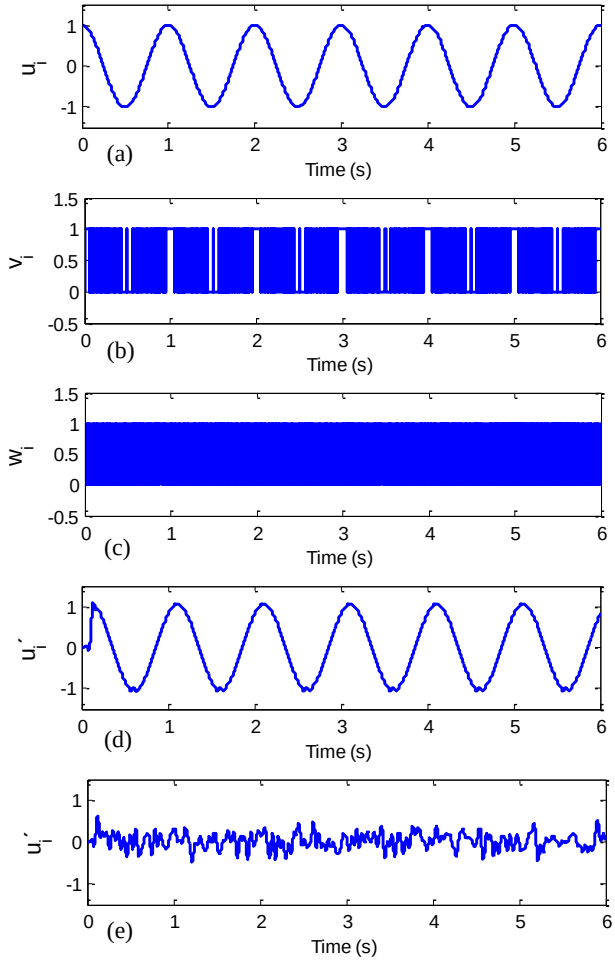

Figure 7. (a) Message signal. (b) Delta-sigma modulator output. (c) Transmitted bits. (d) Recovered message signal. (e) Recovered message bits for a wrong chaotic key sequence.

4. Conclusion

A chaotic random bit generator based data encryption scheme is designed for digital transmission through delta and delta-sigma modulators. The practically proven technology of the delta modulation systems are used in many signal processing and communication applications with the developments in mixed signal integrated circuits. The implementation of the chaotic encryption is able to provide security for such systems. The approach allows us to benefit from the advantages of the delta modulation techniques and chaos theory. The randomness of the robust chaotic map based random bits are evaluated with qualitative statistical tests. The security of the delta modulation systems under chaotic encryption is tested with low pass filtering and key space estimation based attacks, and it is shown that the methods are highly secure and reliable. The use of chaos in securing delta modulation approaches provides a good option to be considered as a framework for the next generation communication and data transmission systems.

Acknowledgements

This work was supported by Research Fund of the Abdullah Gül

University under project number FAB-2015-4.

References

[1] Zrilic D. G. Circuits and Systems Based on Delta Modulation: Linear, Nonlinear and Mixed Mode Processing. Springer, 2006.

[2] Liberti J. and Rappaport T. S. Smart Antennas for Wireless Communications: IS-95 and Third Generation CDMA Applications, 1 edition. Upper Saddle River, NJ: Prentice Hall, 1999.

[3] Intersil Corporation, Delta Modulation For Voice Transmission. Intersil Corporation, Application Note, AN607.1, 2000.

[4] Rodenbeck C. T., Tracey K. J., Barkley K. R., and DuVerneay B.B. Delta Modulation Technique for Improving the Sensitivity of Monobit Subsamplers in Radar and Coherent Receiver Applications, IEEE Trans. Microw. Theory Tech., vol. 62, no. 8, pp. 1811–1822, Aug. 2014.

[5] Comaniciu C. and Mandayam N. B. Delta modulation based prediction for access control in integrated voice/data CDMA systems, IEEE J. Sel. Areas Commun., vol. 18, no. 1, pp. 112–122, Jan. 2000.

[6] Sira-Ramírez H. Sliding Mode Control: The Delta-Sigma Modulation Approach, 1st ed. Basel: Birkhäuser, 2015.

[7] Hu T., Lin Z., and Qiu L. Stabilization of exponentially unstable linear systems with saturating actuators, IEEE Trans. Autom. Control, vol. 46, no. 6, pp. 973–979, Jun. 2001.

[8] Elia N. and Mitter S. K. Stabilization of linear systems with limited information, IEEE Trans. Autom. Control, vol. 46, no. 9, pp. 1384–1400, Sep. 2001.

[9] Brockett R. W. and Liberzon D. Quantized feedback stabilization of linear systems, IEEE Trans. Autom. Control, vol. 45, no. 7, pp. 1279–1289, Jul. 2000.

[10] Liberzon D., Switching in Systems and Control. Springer Science & Business Media, 2012.

[11] Chong K. S., Zahedi E., Gan K. B., and Ali M. A. M. Evaluation of the Effect of Step Size on Delta Modulation for Photoplethysmogram Compression, Procedia Technol., vol. 11, pp. 815–822, 2013.

[12] Feely O. Nonlinear dynamics of discrete-time circuits: A survey, Int. J. Circuit Theory Appl., vol. 35, no. 5–6, pp. 515–531, Sep. 2007.

[13] Johnson T., Sobot R., and Stapleton S. CMOS RF class-D power amplifier with bandpass sigma–delta modulation, Microelectron. J., vol. 38, no. 3, pp. 439–446, Mar. 2007.

[14] Kuang W. V. and Wight J. 1-bit digital tuning of continuous-time filter by the use of unstable sigma-delta modulation, in IEEE International Symposium on Circuits and Systems, 2009. ISCAS 2009, 2009, pp. 41–44.

[15] Liang X., Zhang J., and Xia X. Improving the Security of Chaotic Synchronization With a -Modulated Cryptographic Technique, IEEE Trans. Circuits Syst. II Express Briefs, vol. 55, no. 7, pp. 680–684, Jul. 2008.

[16] Xia X. and Chen G. On delta-modulated control: A simple system with complex dynamics, Chaos Solitons Fractals, vol. 33, no. 4, pp. 1314–1328, Aug. 2007.

[17] Reiss J. D. and Sandler M. B. The benefits of multibit chaotic sigma delta modulation, Chaos Interdiscip. J. Nonlinear Sci., vol. 11, no. 2, pp. 377–383, Jun. 2001.

[18] Hussain I. and Gondal M. A. An extended image encryption using chaotic coupled map and S-box transformation, Nonlinear Dyn., vol. 76, no. 2, pp. 1355–1363, Jan. 2014.

[19] Lynnyk V., Sakamoto N., and Čelikovský S. Pseudo random number generator based on the generalized Lorenz chaotic system, IFAC-Pap., vol. 48, no. 18, pp. 257–261, 2015.

[20] Park M., Rodgers J. C., and Lathrop D. P. True random number generation using CMOS Boolean chaotic oscillator, Microelectron. J., vol. 46, no. 12, Part A, pp. 1364–1370, Dec. 2015.

[21] Cicek I., Pusane A. E., and Dundar G. A novel design method for discrete time chaos based true random number generators, Integr. VLSI J., vol. 47, no. 1, pp. 38–47, Jan. 2014.

[22] Kocarev L. and Lian S. Chaos-based cryptography theory, algorithms and applications. Berlin: Springer, 2011.

[23] Martínez-González R. F., Díaz-Méndez J. A., Palacios-Luengas L., López-Hernández J., and Vázquez-Medina R. A steganographic method using Bernoulli's chaotic maps, Comput. Electr. Eng., 2016.

[24] Ranasinghe D. C., Lim D., Devadas S., Abbott D., and Cole P. H. Random numbers from metastability and thermal noise, Electron. Lett., vol. 41, no. 16, pp. 13–14, Aug. 2005.

[25] Walker J. HotBits: Genuine Random Numbers, 2016. [Online]. Available: https://www.fourmilab.ch/hotbits/.

[26] Kroese D. P., Taimre T., and Botev Z. I. Handbook of Monte Carlo Methods, 1 edition. Hoboken, N.J: Wiley, 2011.

[27] Öztürk I. and Kılıç R. A novel method for producing pseudo random numbers from differential equation-based chaotic systems, Nonlinear Dyn., vol. 80, no. 3, pp. 1147–1157, Feb. 2015.

[28] Romero N., Silva J., and Vivas R. On a coupled logistic map with large strength, J. Math. Anal. Appl., vol. 415, no. 1, pp. 346–357, Jul. 2014.

[29] Wang X. and Bao X. A novel block cryptosystem based on the coupled chaotic map lattice, Nonlinear Dyn., vol. 72, no. 4, pp. 707–715, Jan. 2013.

[30] Alvarez G. and Li S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, Int J Bifurc Chaos Appl Sci Eng, vol. 16, no. 8, p. 2129, 2006.

[31] Strogatz S. H. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering, Second Edition, Second Edition edition. Boulder, CO: Westview Press, 2014.

[32] Sprott J. C. Chaos and Time-Series Analysis, 1 edition. Oxford ; New York: Oxford University Press, 2001.

[33] Ablay G. Chaotic map construction from common nonlinearities and microcontroller implementations, Int. J. Bifurc. Chaos, vol. 26, no. 7, p. 1650121, 2016.

[34] Ablay G. Novel chaotic delay systems and electronic circuit solutions, Nonlinear Dyn., vol. 81, no. 4, pp. 1795–1804, May 2015.

[35] Ablay G. Chaos in PID Controlled Nonlinear Systems, J. Electr. Eng. Technol., vol. 10, no. 4, pp. 1843–1850, 2015.

[36] Simpson D. J. W. On the relative coexistence of fixed points and period-two solutions near border-collision bifurcations, Appl. Math. Lett., vol. 38, pp. 162–167, Dec. 2014.

[37] Mansingka A. S., Affan Zidan M., Barakat M. L., Radwan A. G., and Salama K. N. Fully digital jerk-based chaotic oscillators for high throughput pseudo-random number generators up to 8.77 Gbits/s, Microelectron. J., vol. 44, no. 9, pp. 744–752, Sep. 2013.

[38] Marsaglia G. Random Number Generators, J. Mod. Appl. Stat. Methods, vol. 2, no. 1, May 2003.

[39] Menezes A. J., van Oorschot P. C., and Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996.

[40] Naccache D. Cryptography and Security: From Theory to Applications: Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday. Springer, 2012.

[41] Katz J. and Lindell Y. Introduction to Modern Cryptography: Principles and Protocols, 1 edition. Boca Raton: Chapman and Hall/CRC, 2007.