5-2011

Examination of Chaotic Signal Encryption and Recovery for Secure Communication using Hybrid Acousto-optic Feedback

Monish Ranjan Chatterjee
University of Dayton, mchatterjee1@udayton.edu

Mohammed A. Al-Saedi
University of Dayton

Optical Engineering

SPIEDigitalLibrary.org/oe

Examination of chaotic signal encryption and recovery for secure communication using hybrid acousto-optic feedback

Monish R. Chatterjee
Mohammed Al-Saedi

SPIE

Examination of chaotic signal encryption and recovery for secure communication using hybrid acousto-optic feedback

Monish R. Chatterjee
Mohammed Al-Saedi
University of Dayton
Electrical and Computer Engineering Department
300 College Park
Dayton, Ohio 45469-0226
E-mail: monish.chatterjee@notes.udayton.edu

Abstract. Generation of chaos from acousto-optic (A-O)Bragg cell modulators with an electronic feedback has been studied for over 3 decades. Since an acousto-optic Bragg cell with zeroth- and first-order feedback exhibits chaotic behavior past the threshold for bistability, such a system was recently examined for possible chaotic encryption of simple messages (such as a low-amplitude sinusoidal signal) applied via the bias input of the sound cell driver. Subsequent recovery of the message signal was carried out via a heterodyne-type strategy employing a locally generated chaotic carrier, with threshold parameters matched to the transmitting Bragg cell. In this paper, we present numerical results and detailed interpretations for signal encryption and recovery under hybrid A-O electronic feedback using a heterodyne strategy. Important features of this setup, such as the system robustness in terms of parameter matching (feedback gain, dc bias, and time delay) are also examined in some detail. [DOI: 10.1117/1.3574106]

Subject terms: acousto-optics; Bragg regime; bistability; chaos; encryption; decryption; modulation; parameter matching.

Paper 100993PR received Nov. 29, 2010; revised manuscript received Mar. 14, 2011; accepted for publication Mar. 14, 2014; published online May 2, 2011.

1 Introduction

In an acousto-optic (A-O) modulator, an RF signal applied to a piezo-electric transducer, bonded to a suitable crystal, will generate an acoustic wave. It is well known that the acoustic wave acts like a "phase grating" that diffracts any incident laser beam into a number of diffracted orders. The Raman–Nath regime is characterized by multiple scattered orders while in the Bragg regime there are typically only two scattered orders (zeroth- and first- orders).[1]

Around 1978, it was reported that A-O devices with positive feedback gain exhibit bistability characteristics.[2] In an A-O device, the amplitude of the diffracted fields that operate in the Bragg regime, i.e., the zeroth- and first-orders, which appear at the output of the Bragg cell, are related through a set of coupled differential equations. In Refs. 3 and 4, Chrostowski and co-workers present experimental results for A-O bistability and chaos using an equivalent circuit model of the Bragg cell with feedback. In a standard setup, a Bragg cell is driven by an ultrasonic sound wave from an RF generator at 40 MHz, and the resulting sound grating diffracts an incident He–Ne laser beam into the first Bragg order under Bragg condition. The first-order is then picked up by a linear photodetector, fed to an amplifier, and then returned to the bias input of the RF generator. The arrangement is shown in Fig. 1. Nominally, the scattered light beam is intrinsically frequency or phase modulated (with the acoustic frequency). In typical waveform sources, the external bias input amplitude modulates the RF waveform. A plot of the first order intensity (I_1) versus the bias input $\hat{\alpha}_0$ yields the well known bistable and hysteretic behavior.[3,4] The bistability and hysteresis characteristics depend strongly on the feedback gain ($\tilde{\beta}$), the feedback time delay (TD), and the amplitude (I_{inc}) of the incident light. In this paper, we specifically focus on the behavior of the diffracted first-order light under feedback, operating in the chaotic regime, with or without (RF) signal modulation. Accordingly, in Sec. 2, we discuss the basic nonlinear feedback system and the associated chaos, as discussed in the literature. In Sec. 3, the hybrid A-O device and its dynamics are briefly presented. Details of the time behavior of the first-order detected light within, near, and off-chaos are discussed in Sec. 4. Some examples of chaotic encryption for simple, low bandwidth (BW) signals are presented and discussed in Sec. 5. Signal recovery via chaotic heterodyne and some results are discussed in Sec. 6. In Sec. 7, the performance of the chaotic encryption scheme is presented, specifically in terms of the robustness and reliability of the encryption scheme. Section 8 provides concluding remarks and ideas for future work.

2 Nonlinear Feedback System and Chaos

It is well known that the output scattered intensity in an A-O Bragg cell in the Bragg regime have the following amplitude solutions:[4]

$$E_1 = -jE_{\text{inc}} \sin\left(\frac{\hat{\alpha}_0 \xi}{2}\right), \tag{1a}$$

$$E_0 = E_{\text{inc}} \cos\left(\frac{\hat{\alpha}_0 \xi}{2}\right), \tag{1b}$$

which in the time domain correspond to the optical fields:

$$E_1(t) = E_{\text{inc}} \cos(\omega_1 t - \pi/2) \sin\left(\frac{\hat{\alpha}_0 \xi}{2}\right), \tag{2a}$$

$$E_0(t) = E_{\text{inc}} \cos\left(\frac{\hat{\alpha}_0 \xi}{2}\right) \cos(\omega_0 t), \tag{2b}$$

0091-3286/2011/$25.00

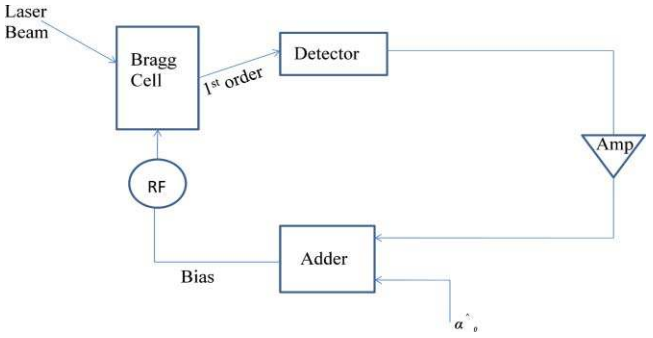

Fig. 1 An A-O modulator with first-order feedback in Bragg regime.

where the outputs are accessed at $\xi = 1$ (explained below); the frequencies $\omega_1 = \omega_i + \Omega$, and $\omega_0 = \omega_i$; ω_i and Ω are the incident optical and the RF (ultrasound) frequencies respectively; $\hat{\alpha}_0$ is the peak phase delay of the light through the acoustic medium; ξ is the normalized distance ($= z/L$, where L is the effective interactive length); and ω_0, ω_1 are the zeroth- and first- order optical frequencies.[4]

With feedback plus time delay, the corresponding first-order detected intensity (via an output photodetector) follows the nonlinear dynamical equation:

$$I_1(t) = I_{\text{inc}} \sin^2 \left\{ \frac{1}{2}[\hat{\alpha}_0(t) + \tilde{\beta} I_1(t - \text{TD})] \right\}, \tag{3}$$

where $\tilde{\beta}$ is the effective feedback gain, I_{inc} ($= E_{\text{inc}}^2$) is the incident intensity, and TD is the feedback delay time including photodetector conversion delay. It is the nonlinear dynamics of Eq. (3) that leads to mono-, bi-, and multistable behavior, followed by chaos in its various manifestations.[3] Several research groups have also investigated aspects and applications of acousto-optic bistability in the past 10 years or more.[5–7] Recently, Ghosh and Verma have conducted an analytical examination of the conditions for the onset of chaos in the A–O feedback system using the Lyapunov exponent.[8] The feasibility of operating the hybrid A–O devices in the chaotic regime, and treating the chaos as an equivalent information carrier which is then encrypted (modulated) by an information signal applied through the RF bias input, and thereafter recovering the message signal in a receiver using (as a first approach) a heterodyne detection method, has recently been explored with some success.[9,10]

2.1 *Signal Encryption in Chaos*

In 1963, Lorenz discovered that in a completely deterministic system of three ordinary differential equations, all nonperiodic solutions underwent irregular fluctuations, and were bounded but unstable.[11] Even though the concept of chaos as irregular periodic oscillations was originally introduced by Poincare,[12] in the modern context, Li and Yorke seemed to be the first to introduce the word "chaos" into the mathematical literature to denote the apparently random output of some mappings.[13] The usual approach to encrypt a signal in a chaotic system is to use a carrier wave of the same frequency as the chaotic signal, and then embed a signal within that carrier wave via amplitude modulation (AM). Presumably, adding this AM-carrier signal to the chaotic signal would then require decryption with the same chaotic signal for read out.[11] This can be expressed mathematically as follows. Assume an AM carrier wave (carrier frequency *fc,*, and modulation index m) to which we add a chaotic carrier, such that:

$$s_{\text{ch}}(t) = [1 + ms(t)]A_c \cos(2\pi f_c t) + A_{\text{ch}} \cos(2\pi f_{\text{ch}} t), \tag{4}$$

where A_c and A_{ch} are the amplitudes of the carrier and chaos, respectively. Assuming $f_{\text{ch}} = f_c$ and by taking $A_c + A_{\text{ch}}$ as a common factor in Eq. (4), we find:

$$s_{\text{ch}}(t) = (A_c + A_{\text{ch}}) \left[1 + \left(\frac{m A_c}{A_c + A_{\text{ch}}} \right) s(t) \right] \cos(2\pi f_{\text{ch}} t), \tag{5}$$

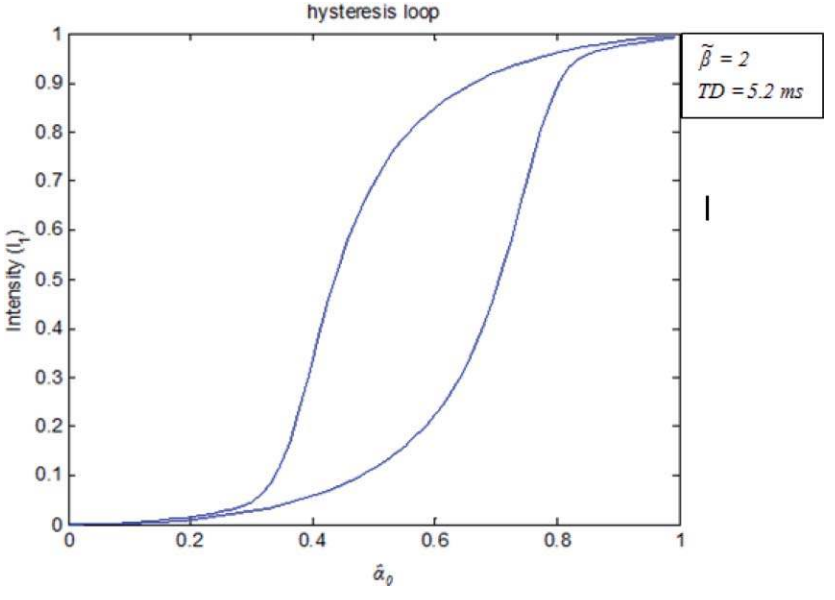

Fig. 2 Hysteresis loop.

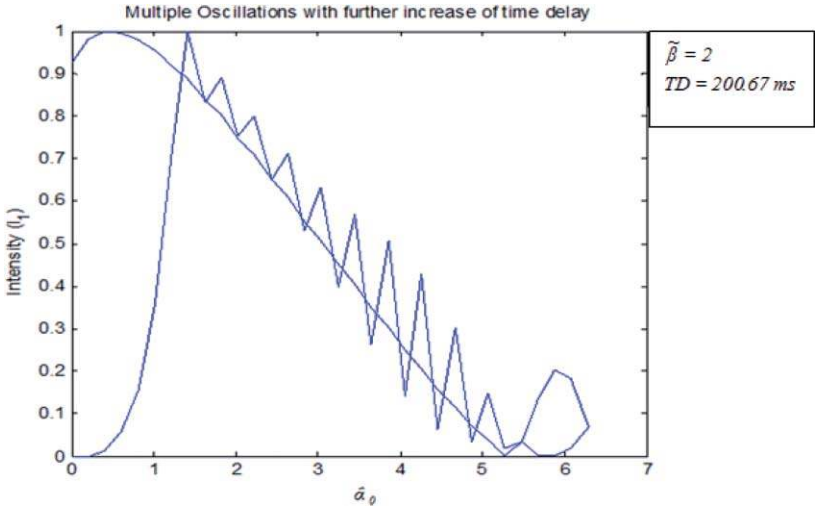

Fig. 3 Multiple/ multistable oscillations at $\tilde{\beta} = 2.41$ and TD = 200.67 ms.

or,

$$s_{\mathrm{ch}}(t) = \tilde{A}_c[1 + \tilde{m}s(t)]\cos(2\pi f_{\mathrm{ch}}t). \tag{6}$$

$\tilde{A}_c$ and $\tilde{m}$ given in Eq. (6) are the effective chaos carrier amplitude and modulation index which are given by:

$$\tilde{A}_c = A_c + A_{\mathrm{ch}};\ \tilde{m} = \frac{mA_c}{A_c + A_{\mathrm{ch}}}. \tag{7}$$

Incidentally, chaos as discussed in this paper manifests itself in a variety of nonlinear physical systems including nonlinear optical systems, involving laser light, optical image waveforms, and A-O. Chaos may also be generated in electronic circuits via nonlinear feedback. An excellent example of electronic chaotic behavior is found in the operation of Chua's circuit.[14,15]

2.2 *Signal Encryption in Chaotic Circuit and Self-Synchronization*

In 1993, Newell et al. reported the synchronization of two separate chaotic circuits.[16] These results were confirmed and the methodology improved on by Mozdy et. al in 1995.[17] A chaotic system is self-synchronizing if it can be decomposed into at least two subsystems: a drive system (transmitter) and a stable response subsystem (receiver) that synchronizes when the chaotic device signal is coupled with the locally generated (receiver) chaos signal.[18–21] As for the coupling, one has to distinguish between two different situations. When the evolution of one of the coupled systems is unaltered by the coupling, the resulting configuration is called unidirectional coupling or drive–response coupling. On the other hand, bidirectional coupling results when both systems are connected in such a way that they mutually influence each other's behavior.[18] Incidentally, the scheme described in this paper corresponds to a unidirectional coupling between the transmitter and the receiver, and hence the system possesses complete synchronization.

2.3 *Signal Encryption in Chaotic Optical System*

Ikeda (1979) predicted theoretically that bifurcation and chaos may appear in an optically bistable device using a ring cavity.[22] This effect was first observed in so-called hybrid bistable devices by Gibbs et al.[23] If the first order light in an A-O Bragg cell is detected, amplified, and fed back into the acoustic driver, the resulting hybrid device

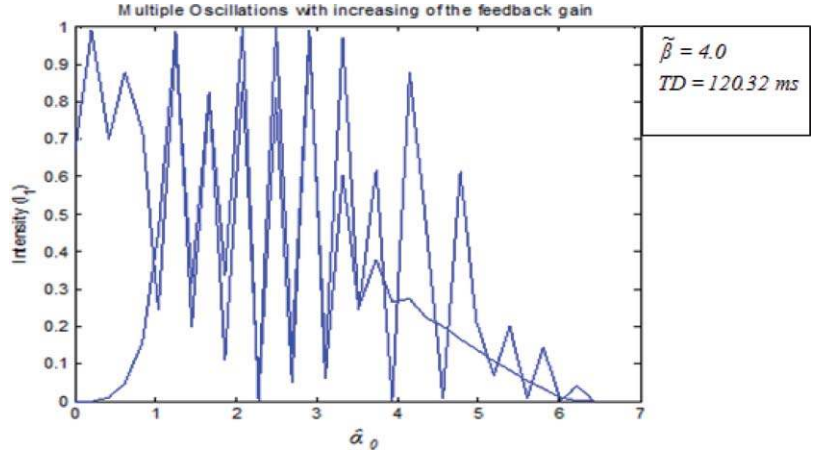

Fig. 4 Complete chaotic oscillation with value of $\tilde{\beta} = 4$.

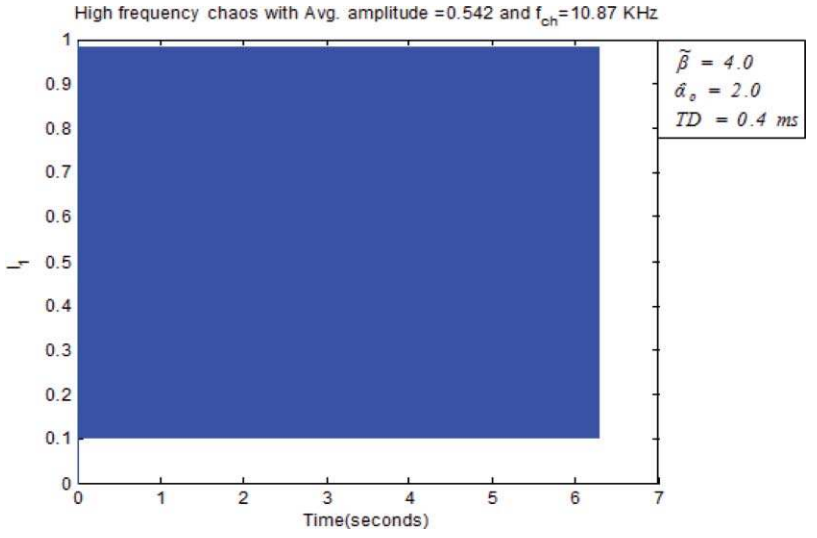

Fig. 5 High frequency chaos of 6.3 s.

exhibits optical bistability. The feedback makes the system inherently nonlinear and complex in terms of its space-time dynamics.[2,3,24] As mentioned in Ref. 4, optical bistability, possible multistability, and chaos may be generated for three fundamental types of tuning effects, viz., feedback gain, bias voltage, and input amplitude. In 2008, Chatterjee and Al-Saedi demonstrated that the chaotic signal in hybrid A-O feedback can be used for encryption and retrieval of signals through preliminary simulations.[25] The work presented in this paper expands on the earlier findings by driving the hybrid A-O system into chaos with a proper choice of the parameters $\tilde{\beta}$, $\hat{\alpha}_0$ and TD, and then encrypting the chaotic waveform with a message wave applied through the acoustic driver bias input. At the receiver end, a chaotic waveform is locally generated and multiplied by the modulated chaotic waveform coming from the transmitter. The resulting product waveform is passed through a low pass filter and subjected to a phase shift of 180° to retrieve the original signal. Clearly, this approach is based on the standard heterodyne detection technique associated with amplitude modulation, as implied through Eq. (6).

It must be noted here that the work discussed in this paper is primarily based on computer simulation experiments using MATLAB. Note also that the simulations accurately incorporate the necessary operational parameters (such as feedback gain, time delay, driver bias, and operations such as signal multiplication) of the actual physical system. Another important observation regarding the simulation experiments reported here is that in using Eq. (3) for the nonlinear feedback in the A-O system, all RF bias inputs become incorporated through the general phase shift parameter ($\hat{\alpha}_0$), and the process of detecting the first order light is incorporated through the photodetector output current, which is proportional to the intensity of the diffracted first-order light.

3 Hybrid A-O Device and its Chaotic Dynamics

In 1992, Chatterjee and Huang re-examined hybrid A-O bistability using a novel technique involving nonlinear dependant sources expressed as convergent power series expansions of one or more variables representing the output fields of a Bragg–domain hybrid A-O device with feedback.[6] It was shown that optical bistability, possible multistability,

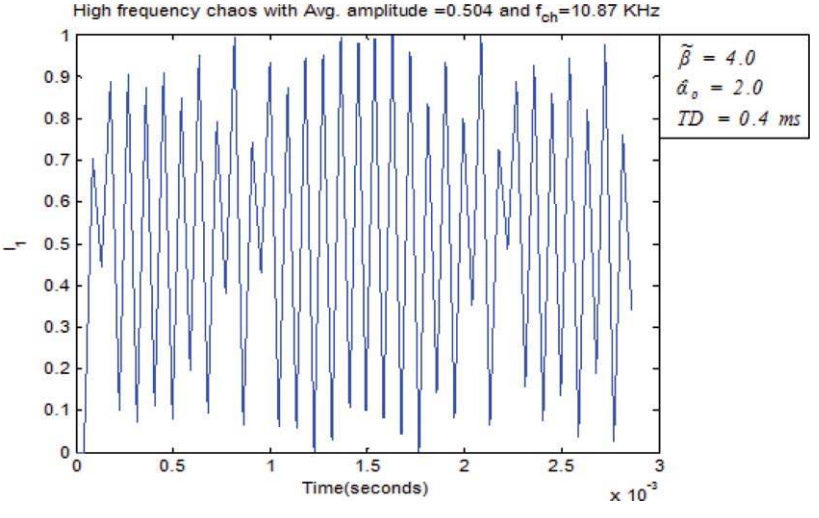

Fig. 6 High frequency chaos.

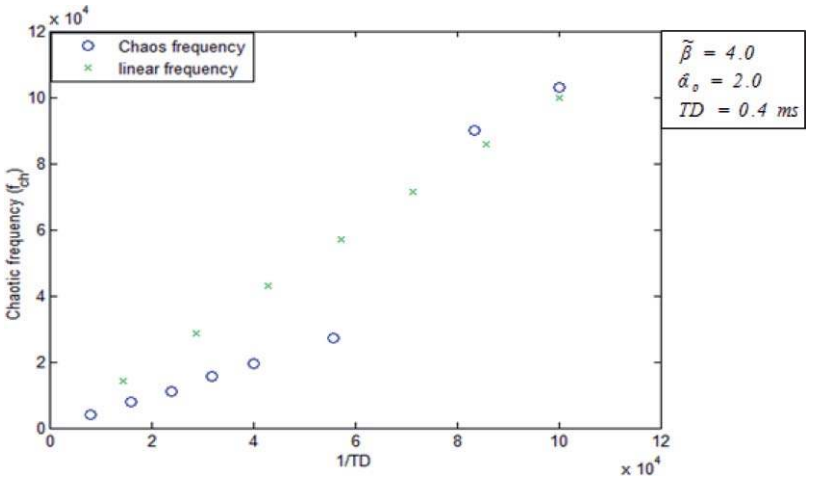

Fig. 7 The chaos frequency versus 1/TD and linear frequency.

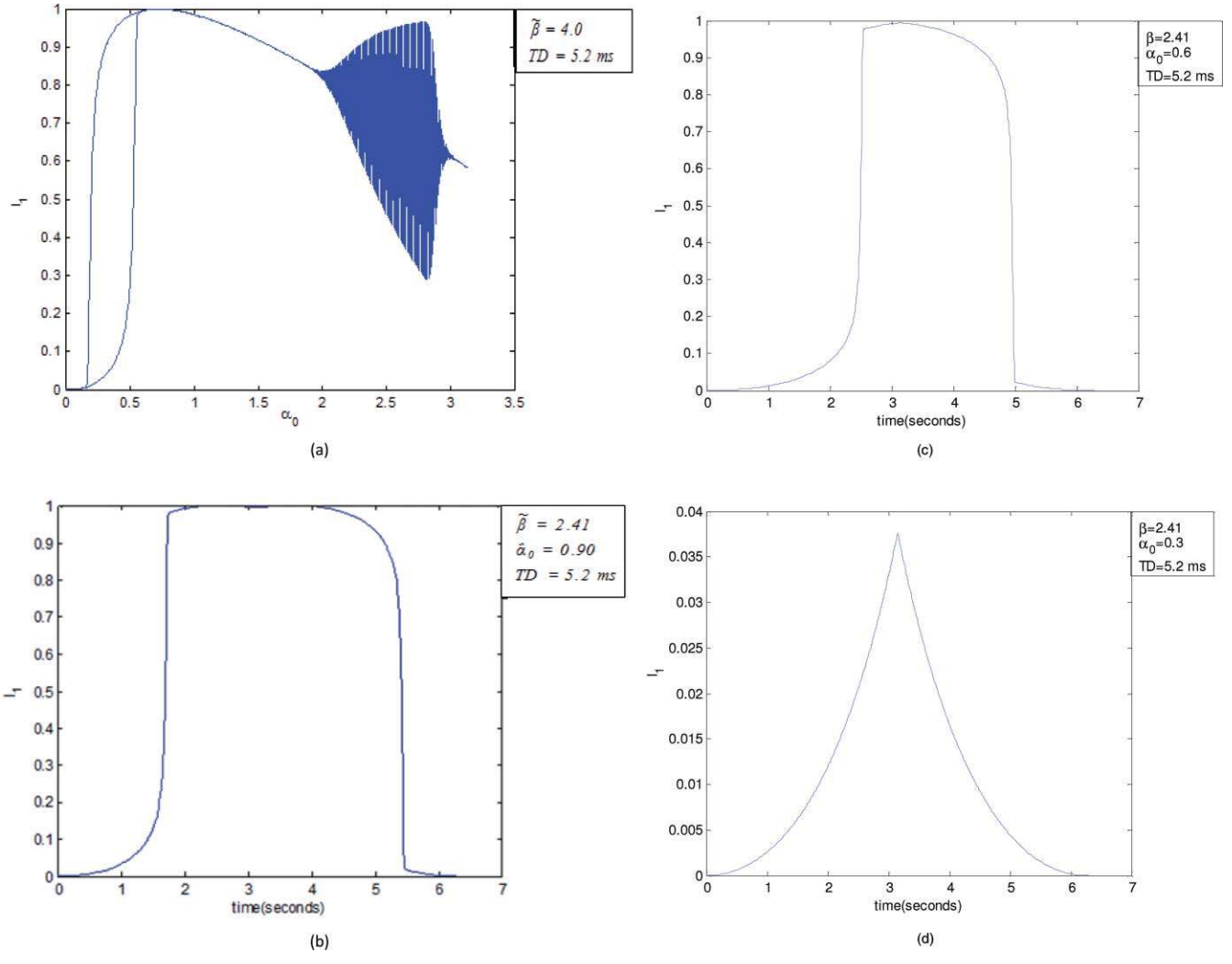

Fig. 8 (a) A bistable and chaotic profile for $\tilde{\beta} = 2.41$. (b) Time profile of I_1 in the upper monostable region. (c) Time profile of I_1 just past the bistable loop. (d) Time profile of I_1 within the bistable loop.

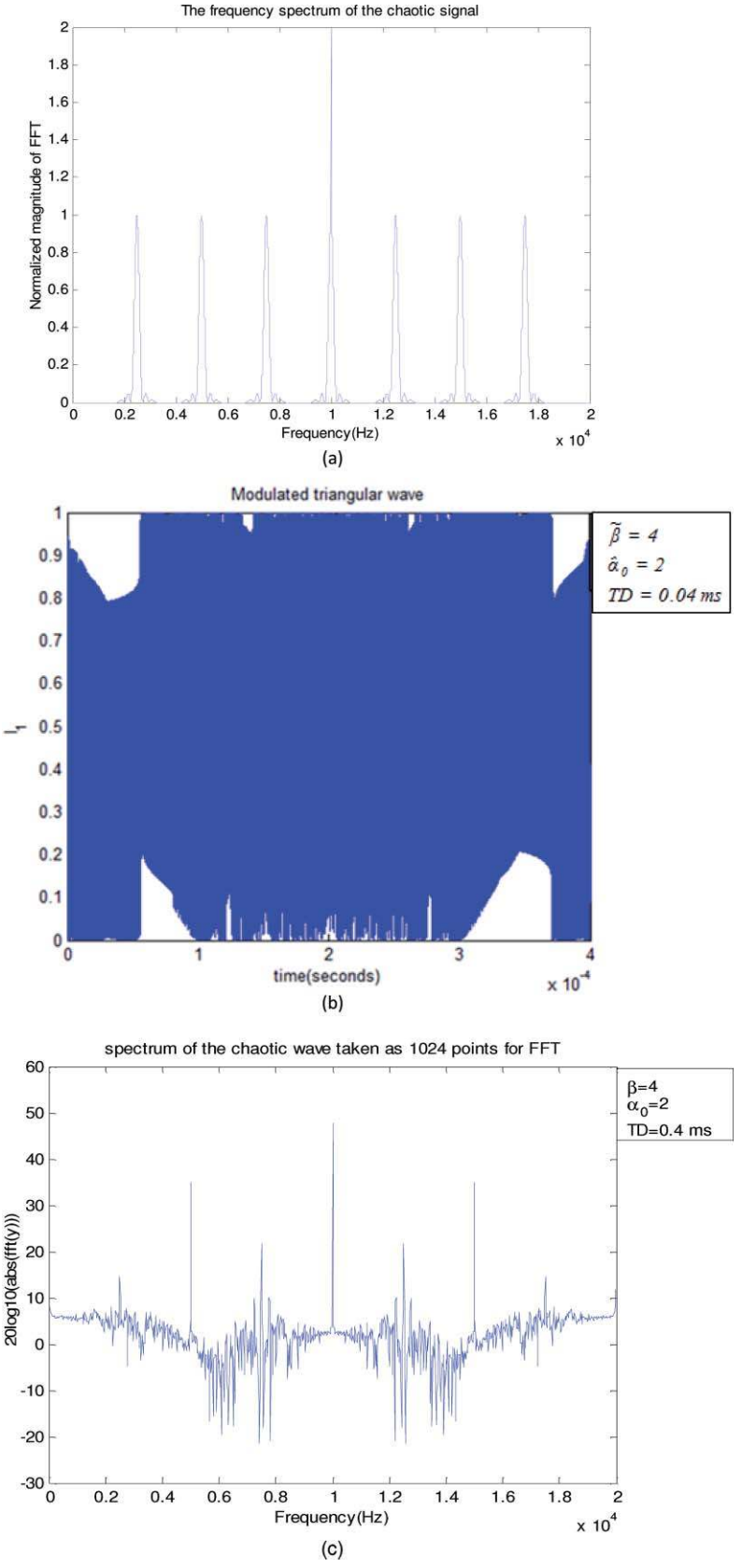

Fig. 9 (a) The frequency spectrum of a DSB signal with a 10 kHz carrier and 2.5 kHz triangular wave. (b) Modulated chaos waveform with an encrypted triangular wave. (c) The spectrum of the modulated chaotic signal.

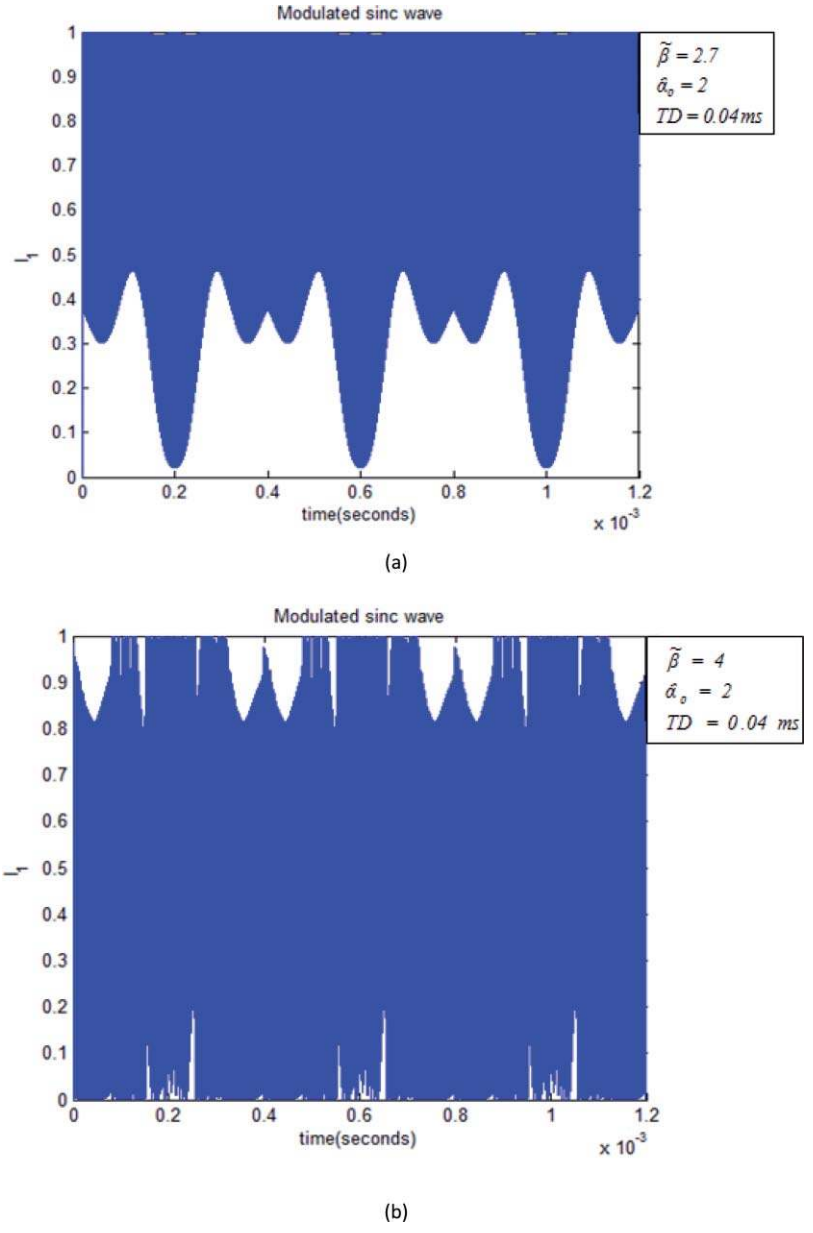

Fig. 10 (a) A modulated chaos wave a sinc function envelope. (b) Modulated sinc wave with $\tilde{\beta} = 4$ and $\hat{\alpha}_0 = 2$.

and chaos may be generated for three fundamental types of tuning effects, i.e., feedback gain, bias voltage, and input amplitude, thereby verifying earlier work.[2–4] In the simulation, E_{inc} is set to 1 for convenience. To study the bistable and chaotic behavior of the hybrid device, typically the input bias is increased from 0 to a maximum and subsequently decreased monotonically back to 0. A critical requirement for the formation of a hysteresis loop for I_1 is the presence of a finite TD in the feedback path of the system; without the delay, the hysteretic behavior does not occur.[6] Figure 2 shows the first-order Bragg intensity I_1 versus the bias voltage ($\hat{\alpha}_0$) which consists of a normal hysteresis loop with a finite TD. Decreasing the time delay and increasing the value of $\tilde{\beta}$ up to a value of 2.41, it is found that the hysteresis loop starts to move to the left, the area of the hysteresis loop increases and eventually additional loops begin to appear beyond the hysteresis loop. Increasing the time delay further for a relatively large fixed value of $\tilde{\beta}$ (at a threshold value of 2.41), clearly defined multistable loops emerge as can be seen in Fig. 3. Clearly, for a TD of 200.67 ms and a feedback gain of 2.41, we observe multistable oscillations beyond the bistable loop. Thereafter, increasing the value of $\tilde{\beta}$ to even higher values (say 4) with an arbitrary TD of 120.32 ms makes the system go into complete chaotic oscillations, as can be seen in Fig. 4. It must be emphasized that the chaotic oscillations shown in Fig. 4 represent variations of I_1 versus the bias voltage ($\hat{\alpha}_0$), and not versus time. In reality, once chaotic oscillations begin, the waveform of I_1 versus time is also expected to be oscillatory, as will be discussed further in Sec. 4.

4 Intensity (I_1) in Hybrid A-O Device in the Neighborhood of Chaos

In this section, we demonstrate the time-domain behavior of the first-order optical intensity (represented by the photode-

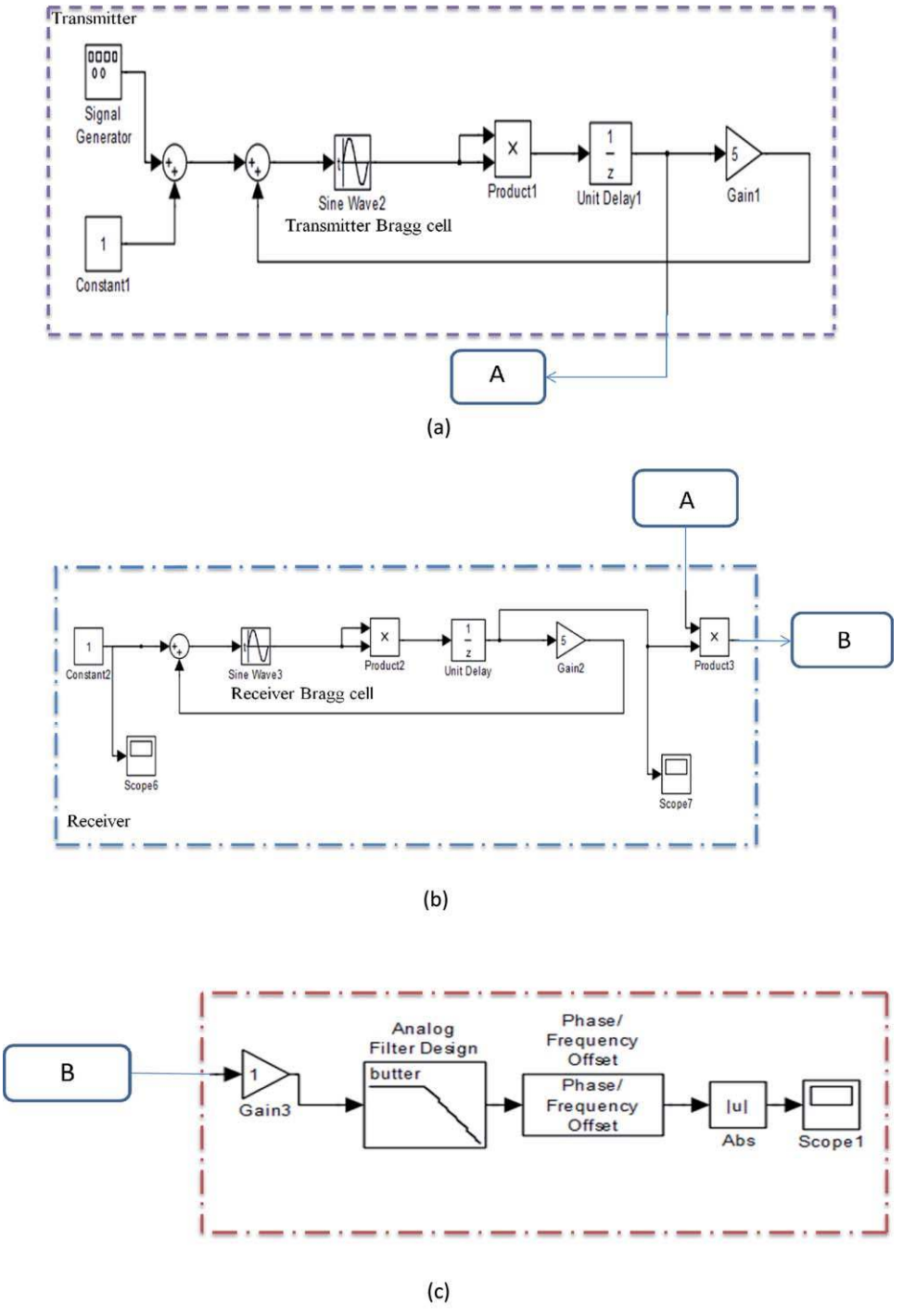

Fig. 11 (a) Schematic of the simulation setup showing components used in the numerical analysis of HAOF at the transmitter end. (b) Schematic of the simulation setup showing heterodyne components used in the numerical analysis of HAOF at the receiver input. ©(c) Schematic of the simulation setup showing amplifier, filter, and phase inverter modules at the receiver.

tected output) for the nonlinear A-O feedback system. To this end, we first develop a hybrid A-O feedback (HAOF) operation in deep chaos. In general, it is known that the HAOF device passes through a number of regions of stable behavior (monostable, bistable, and multistable) en route to chaos. Thus, any such device must operate above a certain threshold RF-driver bias ($\hat{\alpha}_0$) and feedback gain ($\tilde{\beta}$) before attaining the chaotic regime.

Thus, it is commonly observed that the output I_1 of the HAOF attains chaos only past a threshold gain ($\tilde{\beta}$) of 2.41. Likewise, for a high enough gain ($\tilde{\beta}>2.41$), it exhibits chaos only past a threshold bias voltage, typically greater than 1 ($\hat{\alpha}_0 > 1$). Hence, to demonstrate the $I_1(t)$ versus t characteristics, we choose a HAOF operation with $\hat{\alpha}_0 = 2$ and $\tilde{\beta} = 4$ (both well above the respective thresholds). In this chaotic region, the intensity I_1 begins to show oscillations with time, as

shown in Fig. 5. Clearly, an otherwise $\sin^2\{f[s(t)]\}$ function with time delay transforms into controlled chaotic oscillations, as predicted by dynamical theory, in this regime. We also observe that while the chaos frequency is not entirely constant, its average value corresponds approximately to the inverse of the TD in the feedback loop. Thus, as seen from Table 1, the average chaos frequency varies from around 500 Hz to 102 kHz for TD in the range between 2.1 and 0.01 ms. It turns out that the amplitude of the chaos waveform actually has low-level variations, such as seen in the short snapshot shown in Fig. 6. Thus, the chaos wave even without any bias signal input exhibits a low-level intrinsic amplitude modulation (AM). This explains the apparent drift of the average chaos frequency from 1/TD, as shown by the plot in Fig. 7. Another important factor we note from Fig. 7 is that as the TD reduces sufficiently (such that $f_{ch} \sim 100$ kHz or higher), the chaos frequency approaches more closely the value 1/TD (the 45° line in Fig. 7). However, even at higher chaos frequencies, there will continue to be low drifts around 1/TD due to the intrinsic AM effect. At higher values of TD we observe much higher departures of f_{ch} from 1/TD. This intuitively implies that the corresponding chaos wave is still not entirely stable and is experiencing a degree of turbulence.

We next explore the behavior of the HAOF at regions away from the chaotic regime. Thus, we examine I_1 versus time specifically in three nonchaotic regimes, 1. at the higher monostable point of the bistable loop; 2. within the bistable loop; and 3. the lower monostable point at the bistable loop. The time behavior in regions outside chaos within a bistable/chaotic regime is shown in Figs. 8(a)–8(d), in which $\tilde{\beta}$ is chosen to be 2.41 (the observed threshold for achieving chaos) and TD is 5.2 ms. From Fig. 8(a), we find that the system passes from bistability into chaos for $\hat{\alpha}_0 > 2.0$ (approximately). Obviously, within the strictly chaotic region, the time profile of I_1 would be oscillatory, as was shown in Figs. 56. However, when we graph the time profiles outside the chaotic regime, the chaotic oscillations disappear. This is clearly seen from Figs. 8(b)–8(d), where the profiles are graphed 1. at $\hat{\alpha}_0 = 0.9$, which is in the upper monostable region to the right of the bistable loop; 2. at $\hat{\alpha}_0 = 0.6$, which is in the upper monostable region immediately past the bistable loop; and 3. at $\hat{\alpha}_0 = 0.3$, which is within the bistable loop. In each case, we observe that the time profile is nonoscillatory.

Table 1 TD and the chaotic frequency (f_{ch}).

TD	f_{ch} kHz
1×10^{-5}	102.9
1.4×10^{-5}	100.003
1.8×10^{-5}	27.3
2.5×10^{-5}	19.4
3.14×10^{-5}	15.6
4.2×10^{-5}	11.04
6.3×10^{-5}	7.8
1.257×10^{-4}	4.1
2.1×10^{-3}	0.477

5 Chaotic Encryption Using HAOF Device

Until now, the chaos waveform has been studied for fixed (dc) acoustic bias voltages. However, in order to utilize chaos as a means of encrypting and safely transporting a signal waveform, one needs to examine further the time (as was presented in Sec. 4) and frequency behavior of the chaos. To our knowledge, such an examination of chaos versus time has not been undertaken within the HAOF literature, except for occasional references in nonlinear analyses. The average chaos frequencies in Table 1 were computed by finding several oscillation periods from zero crossings, and then taking the inverse of the average period. As seen earlier in Fig. 5, we find a relatively fast chaos waveform at 10.87 kHz with an average amplitude of 0.542 (recall that even with no ac bias input, the amplitude undergoes a low-level intrinsic AM) for $\hat{\alpha}_0 = 2$, $\tilde{\beta} = 4.0$. Note that the chaos waveform in Fig. 5 extends from 0 to 2π s.

Next, we investigate the effect on the chaotic HAOF output of a low-bandwidth ac input added to the RF driver bias. As was predicted in Sec. 2.1, [Eq. (6)], the presence of a low-BW ac signal at the bias input of the RF driver manifests itself approximately as an amplitude modulated chaos wave in the first-order intensity. To investigate whether the ac bias-driven chaos indeed turns into a somewhat random AM wave, we examine the resulting chaos waveform with a periodic triangular signal waveform of fundamental frequency 2.5 kHz, both temporally and spectrally. To this end, we first examine the frequency spectrum of a standard double sideband (DSB) waveform consisting of a 10 kHz carrier modulated by a 2.5 kHz periodic triangular wave, both with unit amplitudes. This spectrum, obtained using a 50 μs Hamming window (to allow a sufficient view of the spectrum in the frequency domain) and an fast Fourier transform (FFT) routine, is shown in Fig. 9(a).

In Fig. 9(b), we show the modulated chaos output versus time corresponding to a 2.5 kHz periodic triangular bias input of unit amplitude. Note that in this example, the triangular wave does not manifest itself in the chaos envelope, thus ensuring a proper encryption process. This will be discussed further later. The Fourier spectrum of the finite-duration chaos waveform (using an FFT routine) is shown in Fig. 9(c). In this spectrum, we find evidence that the modulated chaos exhibits several characteristics typical of an amplitude modulated waveform. Note that the central peak in the spectrum occurs around 10.5 kHz which is approximately the average chaos frequency of the given data. Assuming that the stable chaos is indeed represented as amplitude modulation (as suggested in Refs. 10–12), we expect spectral peaks distributed around the "chaotic carrier" in multiples of the fundamental signal frequency (2.5 kHz). Moreover, we note that the spectral peaks are slightly shifted from the expected locations; this behavior can be explained in terms of the intrinsic AM in stable chaos as was discussed before.

We next point out some important considerations in the encryption process. Obviously, if the time behavior of a modulated chaos wave is close to AM, we expect to see the signal waveform in the chaos envelope. This, however, is counterintuitive to the concept of encryption. To properly encrypt a signal, we need to "hide" all possible obvious signatures

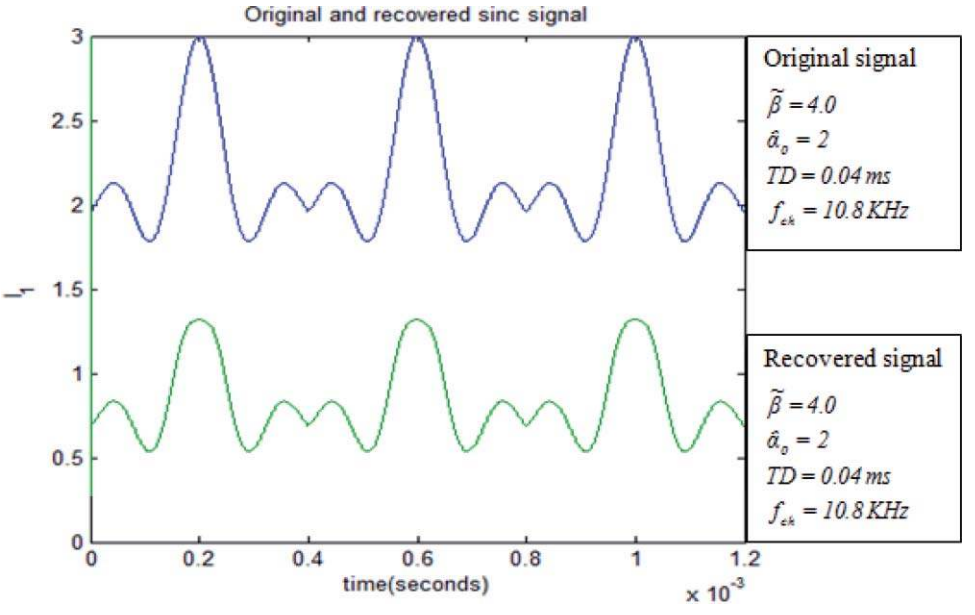

Fig. 12 Original and recovered sinc signal with matched parameters.

of the signal from the transmitted waveform. It turns out that for relatively lower feedback gains (within the chaotic regime), the chaos waveform tends to carry the information signal in the envelope. Such a case is illustrated in Fig. 10(a) for a sinc-function signal used to modulate a chaos wave with $\hat{\alpha}_0 = 2$ and $\tilde{\beta} = 2.7$, albeit with a 180 deg inversion. Clearly, at this value of $\tilde{\beta}$, the device is in deep chaos, yet the information is visible in the chaos envelope. When the feedback gain is increased to 4.0, as shown in Fig. 10(b), the sinc-waveform disappears completely from the envelope. Therefore, for all practical purposes, the information is now "hidden" or encrypted. Overall, it is observed in our simulations that information hiding may generally be accomplished in the chaotic system by choosing $\tilde{\beta} > 3.0$.

6 Signal Recovery Using Chaotic Heterodyne Strategy

We have seen in Sec. 5 that a stable chaos wave exhibits both intrinsic and extrinsic AM behavior corresponding to low-BW ac bias signals. Additionally, the modulated chaos, due to inherent amplitude and frequency drifts, has the ability to hide the information within its temporal characteristics. At

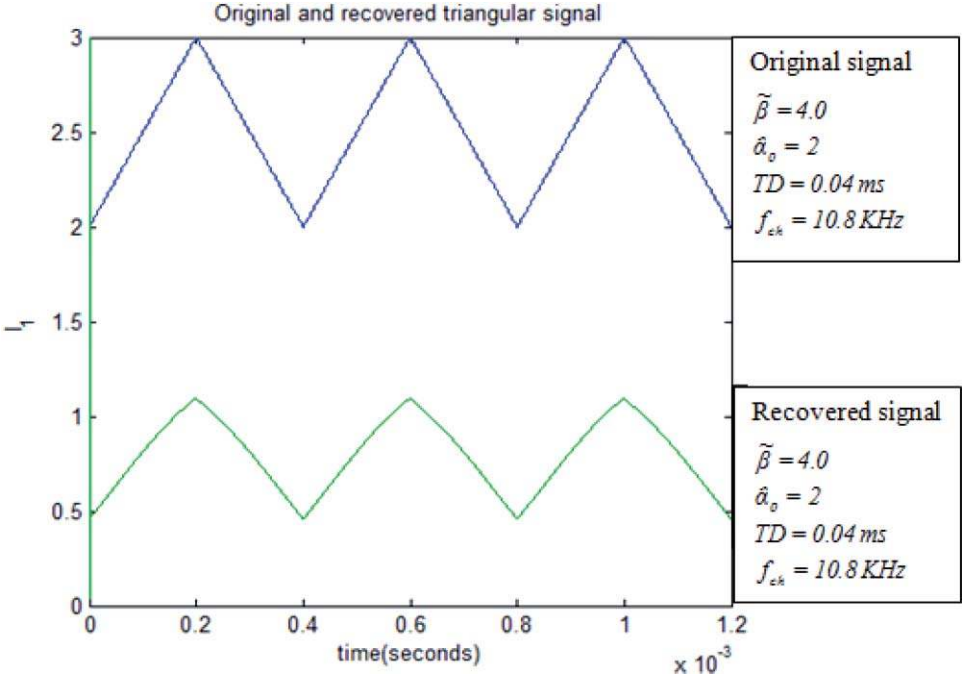

Fig. 13 Original and recovered triangular signal with matched parameters.

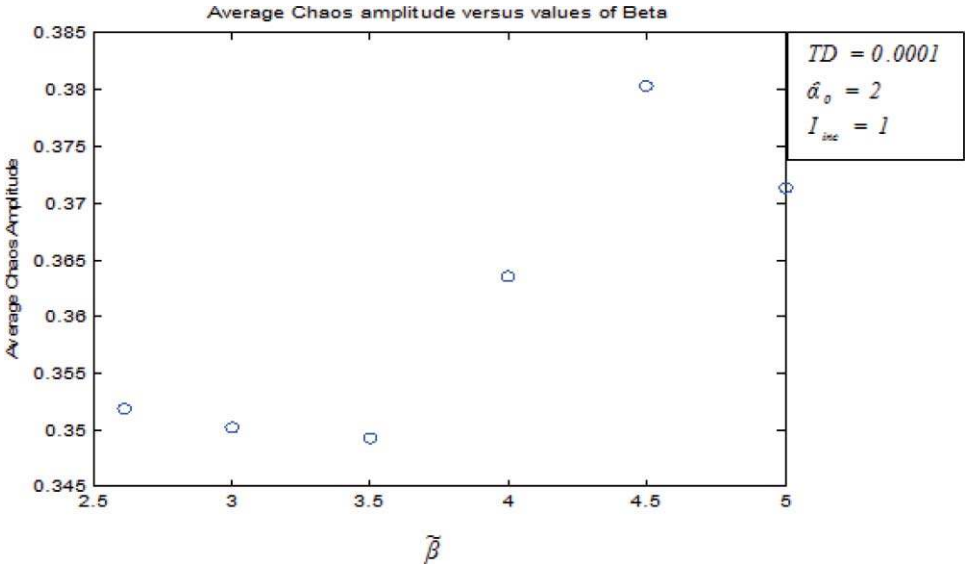

Fig. 14 Dependence of chaos amplitude on $\tilde{\beta}$.

the receiver end, the signal is recovered as follows. First, a local chaos wave is generated using a second Bragg cell with matched parameters $\hat{\alpha}_0$ (bias voltage), $\tilde{\beta}$ (feedback gain), and TD. The local chaos (which is a photodetected RF current corresponding to the first-order light) is then multiplied with the incoming photodetected modulated chaotic signal. The product waveform is then passed through a low pass filter (LPF) with cutoff frequency adjusted to accommodate the signal bandwidth. Nominally, the product spectrum would yield a response component in the neighborhood of twice the chaotic carrier which is eliminated by the LPF. Finally, one needs to carry out a phase shift of 180° along with appropriate dc level shifting to recover the message signal. This method is essentially a heterodyne scheme. A complete block diagram of the transmitter-heterodyne receiver scheme is shown in Fig. 11(a)–11(c). The block diagram shows an integrated transmitter-receiver system using the heterodyne concept. Figure 11(a) shows a block schematic of the transmitter representing the HAOF device. The summer at the front end adds the dc bias voltage to a possible ac signal. The second summer adds to the first the feedback obtained by detecting and amplifying the first-order scattered light. The resulting $\hat{\alpha}_{0,\text{total}}$ is then used to generate the first-order intensity with delay (expressed as $\sin^2$). The first-order is then passed through a delay unit (representing the photodetector output), and an amplifier in the feedback loop. Figure 11(b) represents the front-end of the receiver in a complete communication system involving the HAOF device. Accordingly, a local chaos wave matched to the transmitter parameters is then multiplied with the received modulated chaos wave from the transmitter (signal A). This process results in an effective heterodyne phenomenon. The output of the multiplier is labeled B, and continues into Fig. 11(c). Finally, Fig. 11(c) shows the heterodyne output (signal B) passing

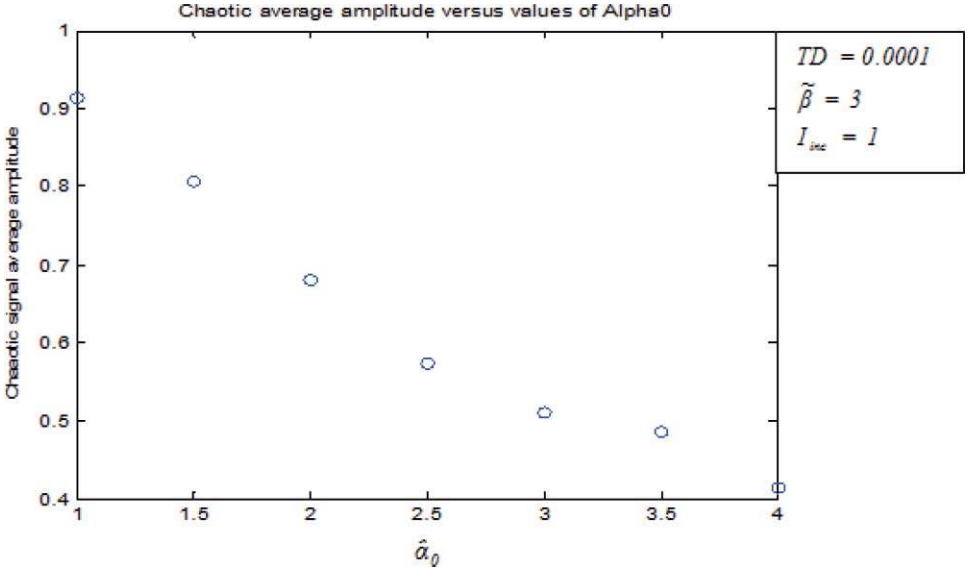

Fig. 15 Dependence of chaos amplitude on $\hat{\alpha}_0$.

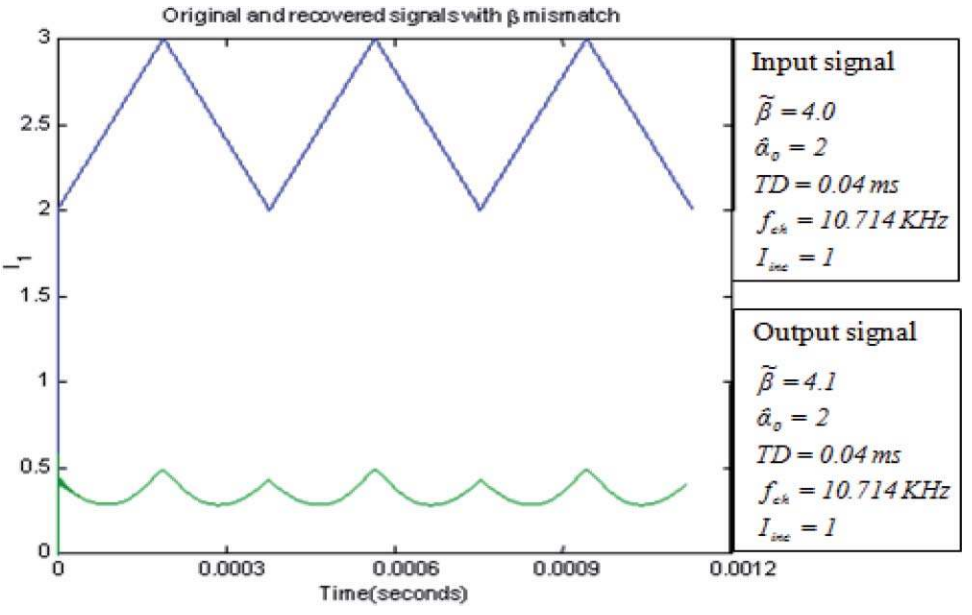

Fig. 16 Original and recovered triangle wave with $\tilde{\beta}$ mismatch.

through a low-pass filter and a phase inverter, whose roles are explained later. In Figs. 12 and 13, we show the input and final recovered waveforms using this scheme for two different signals, viz., a sinc and a triangular wave. Note that the input and the output message waveforms in Figs. 12 and 13 both exhibit dc level shifts. The input level shifts are caused by the (deliberate) addition of a dc bias voltage to the driver ac bias of the RF source in order to ensure chaotic operation over the entire range of ac variations. On the other hand, the level shift post-LPF is simply caused by the dc component inherent in product demodulation. Final signal restoration would simply involve canceling the dc shift of the LPF output. The matched parameters used in both the transmitter and receiver are $\hat{\alpha}_0 = 2$, $\tilde{\beta} = 4$, and TD $= 0.00004$ s. We note in this context that at a TD of 0.00004 s, the expected (ideal) average chaos frequency ought to be about 25 kHz. However, as was illustrated in Fig. 7, the actual chaos frequency in this region "drifts" from 1/TD, and therefore happens to be about 10.78 kHz. Clearly, this region of operation is not ideal (since it involves considerable intrinsic AM effects). However, it is encouraging that even in this relatively nonideal chaotic region, we are still able to encrypt and recover simple signal waveforms, thereby validating the basic operational principles. Obviously, in an ideal system with sufficient resources, one would reduce the feedback time delay such that the operating f_{ch} would increase to the 10 s of MHz or higher range, where the chaos itself would also follow the 1/TD line more closely. This will be in fact necessary in a practical system with arbitrarily large signal bandwidths.

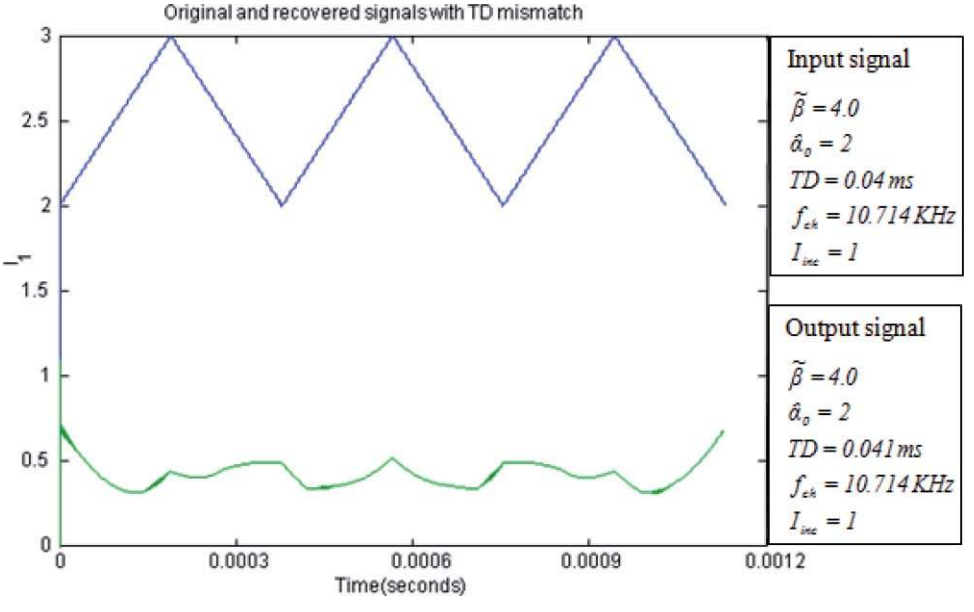

Fig. 17 Original and recovered triangle wave with TD mismatch.

Table 2 The tolerance estimates for the three matched parameters.

Parameters	Level	Thresholds for distortion	Percentage tolerance (%)	
$\tilde{\beta}$ (matched value = 4.0)	$\tilde{\beta}_{high}$	4.1	$\Delta\tilde{\beta}/\tilde{\beta} \times 100$	2.5
	$\tilde{\beta}_{low}$	3.9		2.5
$\hat{\alpha}_0$(matched value = 2.0)	$\hat{\alpha}_{0bias(high)}$	2.2	$\Delta\hat{\alpha}_0/\hat{\alpha}_0 \times 100$	10
	$\hat{\alpha}_{0bias(low)}$	1.8		10
TD (matched value = 0.04 ms)	TD_{high}	0.041 ms	$\Delta TD/TD \times 100$	2.5
	TD_{low}	0.039 ms		2.5

7 Robustness of Chaotic Encryption and Signal Recovery

To study the effect of feedback gain $\tilde{\beta}$ on the (unmodulated) chaos, the other system parameters ($\hat{\alpha}_0$ and TD) were fixed at $\hat{\alpha}_0 = 2$ and TD = 0.1 ms. It turns out that the chaos frequency does not change with $\tilde{\beta}$. However, $\tilde{\beta}$ does impact the chaos amplitude, which monotonically increases in an intermediate range (3.5 to 4.5); outside this range, it actually decreases with increasing gain, as shown in Fig. 14. To study the effect of the bias $\hat{\alpha}_0$, we assume $\tilde{\beta} = 3.0$, TD = 0.1 ms. It is found that $\hat{\alpha}_0$ has no effect on the chaos frequency. However, the average chaos amplitude appears to decrease monotonically with $\hat{\alpha}_0$, as can be seen from Fig. 15. We note further that both $\hat{\alpha}_0$ and$\tilde{\beta}$ exhibit individual thresholds (about 1.1 for $\hat{\alpha}_0$ and 2.41 for$\tilde{\beta}$) that need to be exceeded in order to drive the feedback system into chaos.

As shown earlier, the system in Fig. 11 is used to encrypt and decrypt/recover message signals with matched parameters between the transmitter and the receiver, examined via simulation experiments. In order for this encryption process to be reliable and relatively immune from hacking and piracy, we need to develop a system where the slightest parametric mismatch will destroy the signal recovery. Thus, the "matched parameters" serve as the decoding key in this system. Therefore, to evaluate the robustness of this matched-parameter system, we examine the recovery process under 1.$\tilde{\beta}$ mismatch; 2. TD mismatch; and 3. $\hat{\alpha}_0$ mismatch. Examples of the resulting impact on the quality of the recovered signal are presented below. As shown in Fig. 16, when $\tilde{\beta}$ is mismatched from 4.0 in the transmitter to 4.1 in the receiver, we see significant distortion upon recovery for the triangular wave with a mismatched $\tilde{\beta}$. A similar distortion occurs for about a 2.5% reduction of the matched parameter $\tilde{\beta}$ in the receiver. When the time delay in the receiver Bragg cell was increased to 0.041 ms for a matched value of 0.04 ms, we once again observe a distorted output, as shown in Fig. 17. Again, a similar distortion occurs when the delay at the receiver is reduced to 0.039 ms. Finally, when the receiver Bragg cell $\hat{\alpha}_0$ is increased to 2.2 for a matched value of 2.0, the recovered output falls apart, as shown in Fig. 18. Similarly, a reduction by 10% of the matched value also severely distorts the output signal. Table 2 summarizes the tolerance estimates for the three matched parameters. Overall, it appears that the feedback gain and the time delay have much

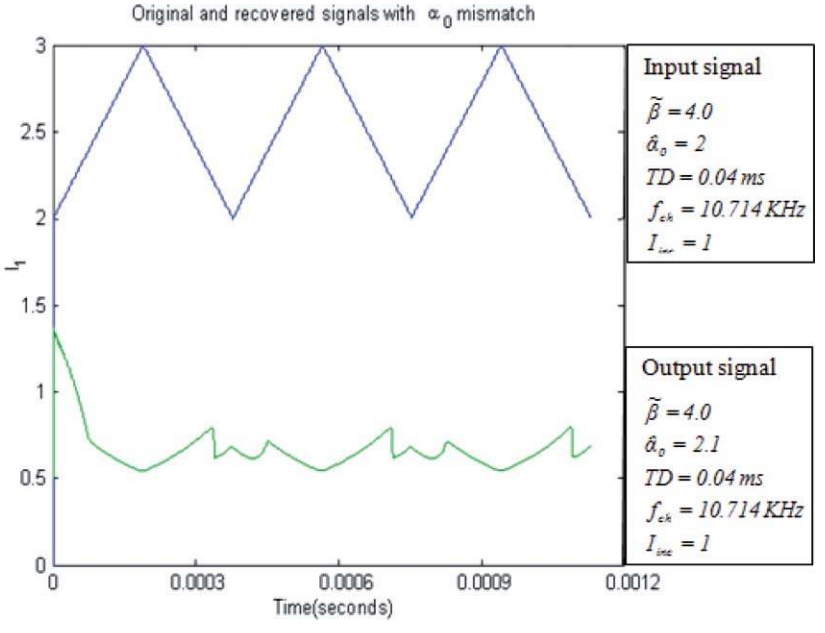

Fig. 18 Original and recovered triangle wave with $\hat{\alpha}_0$ mismatch.

lower tolerances than the bias voltage. While the tolerance ranges shown here (between 2.5% and 10%) may not appear to be sufficiently low, we must keep in mind that an actual physical recovery of an encrypted chaos would require all three parameters to be matched simultaneously, which is probabilistically a prohibitive task.

8 Concluding Remarks

In this paper, a chaotic heterodyne scheme for encrypting and decrypting/ recovering signals using chaos was examined under first-order A-O feedback. The operation of the system for relatively low-BW information is based on driving the feedback A-O system into chaos using proper choice of system parameters. At the receiver end, it is essential that the local Bragg cell have matched parameters in order to recover the original signal.

The effects of parameters such as bias driver ($\hat{\alpha}_0$), the feedback gain ($\tilde{\beta}$), and the TD on the chaotic amplitude and frequency were studied. The scheme robustness was discussed in relation to possible mismatch between the transmitter and the receiver Bragg cell parameters, taken one at a time. The results show that the recovery falls apart for percentage mismatch of the feedback gain and the time delay around 2.5% and for bias driver around 10%. Further and ongoing work includes analytic examination of the chaotic system, noise analysis, and developing a new general encryption system for higher BW and alternative recovery schemes.

Acknowledgments

The authors would like to acknowledge constructive discussions with Dr. Partha Banerjee and Dr. Anjan Ghosh on this research. M.A.S. would further like to express sincere appreciation for the financial support provided by Saudi Arabia Cultural Mission.

References

1. T.-C. Poon and T. Kim, *Engineering Optics with* MATLAB, 1st ed., World Scientific, Singapore (2006).
2. J. Chrostowski and C. Delisle, "Bistable piezoelectric Fabry–Perot interferometer," *Can. J. Phys.* **57**, 1376–1379 (1979).
3. J. Chrostowski and C. Delisle, "Bistable optical switching based on Bragg diffraction," *Opt. Commun.* **41**, 71–74 (1982).
4. J. Chrostowski, C. Delisle and R. Tremblay, "Oscillations in acousto-optic bistable device," *Can. J. Phys.* **61**, 188–191 (1983).
5. T.-C. Poon and S. K. Cheung, "Performance of a hybrid bistable device using an acoustooptic modulator," *Appl. Opt.* **28**, 4787–4791 (1989).
6. M. R. Chatterjee and J.-J. Huang, "Demonstration of acousto–optic bistability and chaos by direct nonlinear circuit modeling," *Appl. Opt.* **31**, 2506–2517 (1992).
7. Y. A. Abdelaziez, P. P. Banerjee and D. R. Evans, "Beam shaping by use of hybrid acousto-optic feedback," *Appl. Opt.* **44**, 3473–3481 (2005).
8. A. K. Ghosh and P. Verma, "Lyapunov exponent of chaos generated by acousto-optic modulators with feedback," *Opt. Eng.* **50**, 017005 (2011).
9. M. R. Chatterjee and M. Al-Saedi, "Examination of chaos-based encryption and retrieval in a hybrid acousto-optic device," Frontiers in Optics, OSA Technical Digest (CD), Paper No. FWC3, Rochester, NY (2008).
10. A. K. Ghosh, P. Verma, S. Cheng, R. C. Huck, M. R. Chatterjee, and M. Al-Saedi, "Design of acousto-optic chaos based secure free-space optical communication links," *Proc. SPIE* **7464**, 74640L (2009).
11. E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atoms. Sci.* **20**, 130–141 (1963).
12. F. Diacu and P. Holmes, *Celestial Encounters: The Origins of Chaos and Stability*, 1st ed., Princeton University Press, Princeton, NJ (1996).
13. T. Y. Li and J. A. Yorke, "Period three implies chaos," *Am. Math. Monthly* **82**, 985–992 (1975).
14. P. S. Lindsay, "Period-doubling and chaos in a driven anharmonic oscillator," *Phys. Rev. Lett.* **47**, 1349–1352 (1981).
15. L. O. Chua, "Chua's circuit: an overview ten years later," *J. Circuits Syst. Comput.* **4**, 117–159 (1994).
16. T. C. Newell, P. M. Alsing, A. Garrielides and V. Kovanis, "Synchronization of chaos using proportional feedback," *Phy. Rev. E* **49**, 313–318 (1993).
17. E. Mozdy, T. C. Newell, P. M. Alsing, V. Kovanis and A. Carrielides, "Synchronization and control in a unidirectional coupled array of chaotic diode resonators," *Phys. Rev. E* **51**, 5371–5376 (1995).
18. K. M. Cuomo, A. V. Oppenheim and S. H. Strogatz, "Synchronization of Lorenz- based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst.* **40**, 626–633 (1993).
19. N. Grass, W. Kinzel, I. Kanter, M. Rosenbluh and L. Haykovich, "Synchronization of mutually versus unidirectionally coupled chaotic semiconductors," *Opt. Commun.* **267**, 464–468 (2006).
20. S. Banerjee, D. Ghosh, A. Ray and A. R. Chowdhry, "Synchronization between two different time-delayed systems and image encryption," *Euro Phys. Lett.* **81**, 20006 (2008).
21. B.-L. Hao, *Chaos*, 1st ed. World Scientific, Singapore (1984).
22. K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Opt. Commun.* **30**, 257–261 (1979).
23. H. M. Gibbs, F. A. Hopf, D. L. Kaplan and R. L Shoemaker, "Observation of chaos in optical bistability," *Phys. Rev. Lett.* **46**, 474–477 (1981).
24. R. G. Harrison, W. J. Firth, C. A. Emshary and I. A. Alsaidi, "Observation of period doubling in all-optical resonator containing NH3 gas," *Phys. Rev. Lett.* **51**, 562–565 (1983).
25. M. Chatterjee and M. Al-Saedi, "Examination of chaotic signal encryption, synchronization and retrieval using hybrid acousto-optic feedback" in OSA FiO/LS/Meta/OF&T, 2008, pp. 6624–6624.

Monish R. Chatterjee received his BTech (Honors) degree from I.I.T., Kharagpur, India, in 1979, and the MS and PhD degrees from the University of Iowa, Iowa City, Iowa, in 1981 and 1985, respectively. He is currently a professor of Electrical and Computer Engineering at the University of Dayton, Dayton, Ohio. He was a faculty member in ECE at Binghamton University, State University of New York, from 1986 to 2002. He specializes in applied optics and has contributed over 100 papers to technical conferences, and published over 40 papers in archival journals and conference proceedings, and numerous reference articles on science. He is also active in the field of humanities, and is the author of three books of translation from his native Bengali.

Mohammed Al-Saedi received his BSEE and MSEE degrees in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 1995 and 2004, respectively. He is currently completing his research for the PhD degree at the University of Dayton, Dayton, Ohio. His areas of research interest include digital communications, signal processing, and nonlinear optics. His doctoral work has resulted in several conference presentations and articles in conference proceedings.