12-2014

Improved Performance of Analog and Digital Acousto-Optic Modulation with Feedback under Profiled Beam Propagation for Secure Communication using Chaos

Fares S. Almehmadi
University of Dayton

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

Optical Engineering

OpticalEngineering.SPIEDigitalLibrary.org

Improved performance of analog and digital acousto-optic modulation with feedback under profiled beam propagation for secure communication using chaos

Fares S. Almehmadi
Monish R. Chatterjee

SPIE.

Improved performance of analog and digital acousto-optic modulation with feedback under profiled beam propagation for secure communication using chaos

Fares S. Almehmadi and Monish R. Chatterjee*
University of Dayton, Department of Electrical and Computer Engineering, 300 College Park, Dayton, Ohio 45469, United States

Abstract. Using intensity feedback, the closed-loop behavior of an acousto-optic hybrid device under profiled beam propagation has been recently shown to exhibit wider chaotic bands potentially leading to an increase in both the dynamic range and sensitivity to key parameters that characterize the encryption. In this work, a detailed examination is carried out vis-à-vis the robustness of the encryption/decryption process relative to parameter mismatch for both analog and pulse code modulation signals, and bit error rate (BER) curves are used to examine the impact of additive white noise. The simulations with profiled input beams are shown to produce a stronger encryption key (i.e., much lower parametric tolerance thresholds) relative to simulations with uniform plane wave input beams. In each case, it is shown that the tolerance for key parameters drops by factors ranging from 10 to 20 times below those for uniform plane wave propagation. Results are shown to be at consistently lower tolerances for secure transmission of analog and digital signals using parameter tolerance measures, as well as BER performance measures for digital signals. These results hold out the promise for considerably greater information transmission security for such a system. [DOI: 10.1117/1.OE.53.12.126102]

Keywords: acousto-optics; Bragg regime; Klein-Cook; profiled beams; chaos; encryption; decryption; modulation.

Paper 141415P received Sep. 10, 2014; accepted for publication Nov. 4, 2014; published online Dec. 3, 2014.

1 Introduction

By manipulating the interaction of light and sound, acousto-optic (A-O) devices are used to controllably diffract light beams for a variety of applications. A piezoelectric oscillator creates acoustic vibrations in a crystal which acts as a diffraction grating and causes the deflection of a light beam passing through the crystal. This deflection depends upon the light and sound frequencies, and various properties of the crystal. These variables are summarized by a unitless quantity known as the Klein-Cook parameter Q. In the Bragg mode of operation, in which only one diffracted order is produced, Q is larger than 8π.[1] This mode is utilized for signal processing applications such as laser beam deflection, modulation, and filtering. When used with a closed-loop feedback, a Bragg cell can produce a chaotic response useful for encryption and decryption of signals.[2]

In a closed-loop Bragg cell, a photodetector receives the diffracted light beam and the resulting electrical signal is amplified, added to a DC offset, and fed back into the acoustic driver for the piezoelectric device. Using the DC offset as an input and taking the output from the photodetector, the closed-loop system becomes a nonlinear signal processing device, capable of mono-, bi-, multistable, and chaotic behavior.[3–5] These characteristics can be utilized for signal processing applications including, in the case of chaos, encryption and decryption.[6]

The dynamic behavior for Bragg cells is characterized with the Lyapunov exponent (LE) or bifurcation maps. The LE is a function of Q, DC offset, feedback gain, and input beam intensity, and its value indicates whether or not the closed-loop behavior will be chaotic. A bifurcation map plots photodector output as a function of a single parameter, such as feedback gain, and it visually illustrates values of that parameter that lead to chaos.[7] Both techniques show that passbands of chaos appear at unpredictable intervals over the parameter space. Before chaos can be utilized for any application, it is necessary to know the locations and widths of these passbands.[8]

When the closed-loop Bragg-cell parameters are controlled to produce chaos, the photodetector output can be viewed as a chaotically modulated and encrypted version of the input signal. To recover the original input signal, a second Bragg cell with parameters matched to the first is used like a standard heterodyne receiver. The modulated signal is multiplied by the chaotic signal created by the receiver Bragg cell, and the product waveform is low-pass filtered and corrected for a 180 deg phase offset.[6] Any mismatch between the transmitter and receiver parameters (bias voltage, feedback gain, or time delay) causes demodulation to fail. In this way, the parameters act as an encryption key that must be known in order to recover the signal.

Most mathematical characterizations of the nonlinear properties of a closed-loop Bragg cell assume that the input beam of light is a uniform plane wave, and weak interaction theory is then used to describe the light and sound interaction within the crystal. This leads to common expressions for the diffracted light and these expressions are used for modeling chaos and creating simulations of encryption/decryption with this chaos. In recent work, it is shown that using a more realistic, nonuniform input light beam has a significant impact on the location and width of the chaotic passbands within the parameter space.[8] The present work applies new simulations of chaos using profiled input

*Address all correspondence to: Monish R. Chatterjee, E-mail: mchatterjee1@udayton.edu

0091-3286/2014/$25.00 © 2014 SPIE

beams to model the encryption and decryption of digital signals, and it measures the robustness of the encryption process to additive channel noise and parameter mismatch between the transmitter and receiver. We note here that alternative chaotic signal encryption techniques are also available. A common method involves chaos in optical fiber networks with encryption embedded using electro-optic delays. Such methods typically yield realizable bandwidths in the low-Gbps range.[9] In our work, the chaos frequency has been limited to about 10 MHz so that the affordable bit rates would be in the low Mbps range. However, technically, A-O Bragg cells may operate in the GHz range, whereby higher encryption bit rates may readily be realizable.

Section 2 presents A-O Bragg cell behavior for profiled input beams and describes the effect of the profile on the diffracted light. This modeling is necessary for studying the nonlinear dynamics of closed-loop systems, also presented in Sec. 2. Further details of the chaotic passbands in the parameter space and how these are used for encryption of signals is presented in Sec. 3. Results for encryption robustness to parameter mismatch are presented in Sec. 4, along with the effect of additive channel noise on the bit-error-rate for encrypted digital communication. Section 5 provides an interpretation of the significant results, and Sec. 6 summarizes the key points and discusses future modeling work.

2 Profiled Beams Through Hybrid A-O Feedback System

Figure 1 illustrates an A-O Bragg modulator with first-order feedback, although in this discussion the feedback loop will initially be ignored. At the left plane of the cell, a profiled input beam is nominally incident at the Bragg angle. The zeroth- and first-order scattered beam outputs from the cell are $E_0(r)$ and $E_1(r')$, where the coordinates r and r' are the transverse radial coordinates with respect to the direction of the incident field and the diffracted field, respectively. The parameter $\delta\phi_B$ is the angular deviation from the Bragg angle $\phi_B(\approx K/2k)$, and $\bar{K}$ is the acoustic wave vector.[9] With the plane wave angular decomposition theory, the profiled beam is decomposed into a spectrum of uniform plane wave components incident at an arbitrary angle $(1+\delta)\phi_B$ where δ is a dimensionless measure of angular deviation. For near-Bragg diffraction, expressions for the two scattered orders $\tilde{E}_0$ and $\tilde{E}_1$ are found using a pair of coupled differential equations. With these equations, a transfer function formalism is developed by Chatterjee et al. in order to model the diffracted orders for arbitrary input profiles.[10] Using this approach, either output profile is found by applying the inverse Fourier transform to the product of the incident spectrum $\tilde{E}_{inc}(\delta)$ and the transfer function $\tilde{H}(\delta)$, as indicated in Ref. 10:

$$E_{out}(r) = \int_{-\infty}^{\infty} \tilde{E}_{inc}(\delta)\tilde{H}(\delta)e^{-j\frac{2\pi}{\lambda}\delta\varphi_B r}\left(\frac{\phi_B}{\lambda}\right)d\delta. \quad (1)$$

In this equation, $E_{out}(r)$ is either the first- or zeroth-order output, depending on which transfer function is used. Both outputs are functions of the peak phase delay $\hat{\alpha}_0$ and the Klein-Cook parameter Q.

Using Eq. (1), diffracted outputs for various incident profiles $E_{inc}(r)$ were presented in previous works.[11] When the incident profile is a uniform plane wave, the shape of the output intensity along the optical phase shift axis is the well-known $\sin^2$ shape. The same is true for Gaussian input profiles, but only for relatively small Q values in the range of 20 to 50. For higher values of Q, the shape of the first-order intensity deviates significantly from the expected $\sin^2$-pattern. In addition, the output profiles for higher Q's also deviate from the expected Gaussian shape along the transverse radial coordinate.[11] These unexpected high-Q deviations from the standard theory for profiled input beams cause a significant impact in the closed-loop system (primarily due to the nonuniform output amplitudes) as discussed in Ref. 8. Since real laser beams are profiled, it is critical to understand and model these behaviors.[11]

For the full hybrid closed-loop A-O system, as shown in Fig. 1, the first-order diffracted light is collected by a photodetector whose output is then amplified and fed back into the acoustic driver. The photodetector current $I(t)$ exhibits nonlinear dynamics, including mono-, bi-, multistability, and chaotic behavior, first observed in 1978.[5] For a uniform plane wave input, the well-known analysis leads to an equation for $I(t)$.[5] A modified version of this equation, shown in Eq. (2), was developed to simulate and study the system for arbitrary profiled beams.[8]

$$I_{ph}(t) = \left| f\left(\frac{1}{2}\{\hat{\alpha}_0(t) + \tilde{\beta}[I_{ph}(t-TD)]\}\right)\right|^2. \quad (2)$$

In this equation, $\hat{\alpha}_0$ is the peak phase delay, $\tilde{\beta}$ is the feedback gain, and TD is the feedback time delay, which is due to the photodetector, amplifier, and the overall physics of the A-O cell.[5] The function f represents the observed output along the optical phase shift dimension for a nonuniform input profile.[8] Unlike the uniform plane wave case, there is no closed-form expression for f. For the simulations shown in this paper, f is determined numerically by assuming a Gaussian input profile.

3 Signal Encryption and Retrieval for Secure Communication

The behavior of the closed-loop system depends upon the four parameters $\hat{\alpha}_0$, $\tilde{\beta}$, TD, and Q, and for chaotic encryption applications, it is necessary to understand which combination of parameters produces chaos in the photodetector

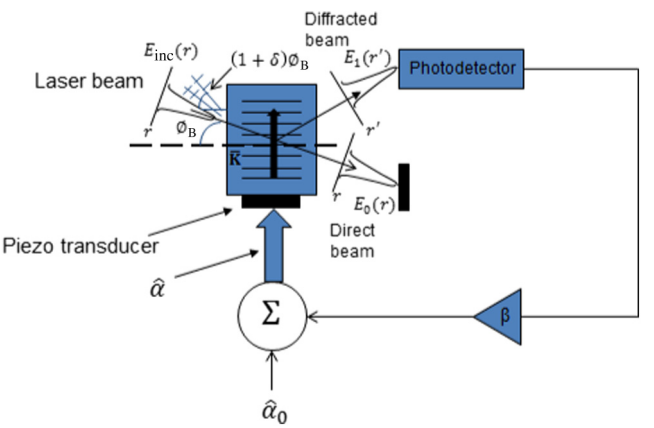

Fig. 1 Acousto-optic (A-O) closed-loop hybrid system with an arbitrary incident beam profile.

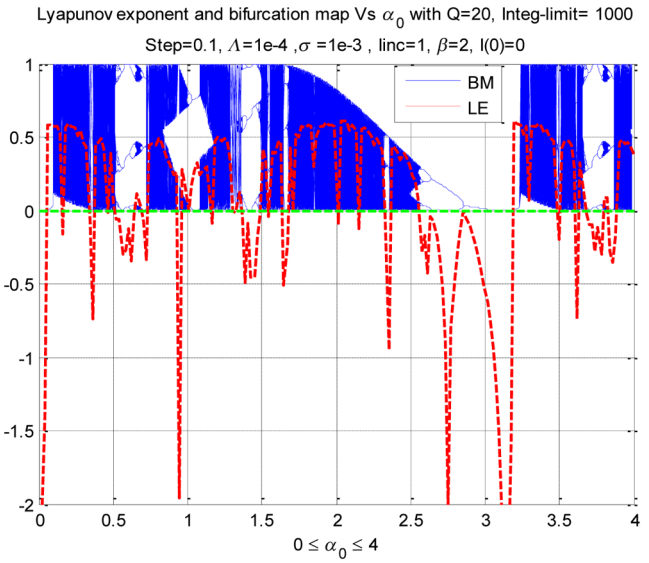

Fig. 2 Lyapunov exponent and bifurcation maps versus the optical phase shift when $\tilde{\beta} = 2$.

current. As previously shown, the threshold value of $\tilde{\beta}$ between bi stability and chaos is strongly affected by the profiled beam inputs.[8] Also, for constant values of $\tilde{\beta}$ and TD, the specific pattern of the chaos is a function of $\hat{\alpha}_0$. This pattern is characterized using two equivalent techniques: the LE and bifurcation maps. The LE models the incremental changes in photodetector intensity and the system is only chaotic if the LE is positive.[7] Bifurcation maps are plots of the photodetector output versus $\hat{\alpha}_0$, with other parameters constant, illustrating sudden changes in the dynamic behavior. An example of a bifurcation map plotted alongside the independently generated LE is shown in Fig. 2, and bands of chaos in the bifurcation map clearly coincide with positive LE values. These data are generated with a Gaussian input profile with parameter values as shown in this figure. The locations, amplitude, and widths of the passbands of chaos are sensitive to the value of $\tilde{\beta}$ and the chosen input profile.[8] When compared to a uniform plane wave input, the passbands of chaos for a Gaussian input profile exhibit greater sensitivity to $\tilde{\beta}$. These details are critical to use chaos for encrypting a signal and they indicate why the analysis of profiled beams is necessary.

To apply chaos as a means of encrypting a signal waveform $s(t)$, we apply this signal to the bias driver such that the peak phase delay has the form of $\hat{\alpha} = \hat{\alpha}_0 + s(t)$. The constant offset $\hat{\alpha}_0$ is chosen such that the photodector output is centered within a chaotic passband, and the range of $s(t)$ must be small enough to not drive the output beyond the passband. In this case, the chaotic photodetector current is viewed as a modulated and encrypted version of the input signal, and this can be securely transmitted through a channel. The recovery of $s(t)$ follows in the manner of a standard heterodyne receiver. A local chaos wave is generated using a second Bragg cell with all four parameters matched to the encryption cell. This local chaos is multiplied with the incoming modulated signal and the product waveform is then passed through a low-pass filter with cutoff frequency adjusted to accommodate the bandwidth of $s(t)$. Note that this bandwidth should theoretically be less than half the center frequency of the chaotic carrier to avoid aliasing, although in reality it is substantially smaller than the chaos center frequency. This frequency depends on the TD parameter through the equation $=(1/2 * \mathrm{TD})$. For the parameters used in this work, the chaos center frequency is in the range of 10 MHz. Figure 3 contains a block diagram of the complete transmitter and heterodyne receiver.

It can be expected that the signal $s(t)$ will modulate the chaotic carrier and behave as amplitude-modulation in some limit, and that the signal will appear in the carrier's envelope.[6] However, because of the random nature of the chaos, the proper choice of the parameter will cause the signal waveform to be completely hidden within the chaos and not be apparent in the envelope. In either case, demodulation requires the same random chaotic pattern used for modulation and this pattern is unique to the four key parameters used.

In recent work, simulations of the encryption system shown in Fig. 3 were developed in MATLAB and the results for several types of signals are presented here.[12] Profiled beams are used in the simulation, and this requires storing the (open-loop) output amplitudes in the first stage of the simulation, and in the second stage running the time-

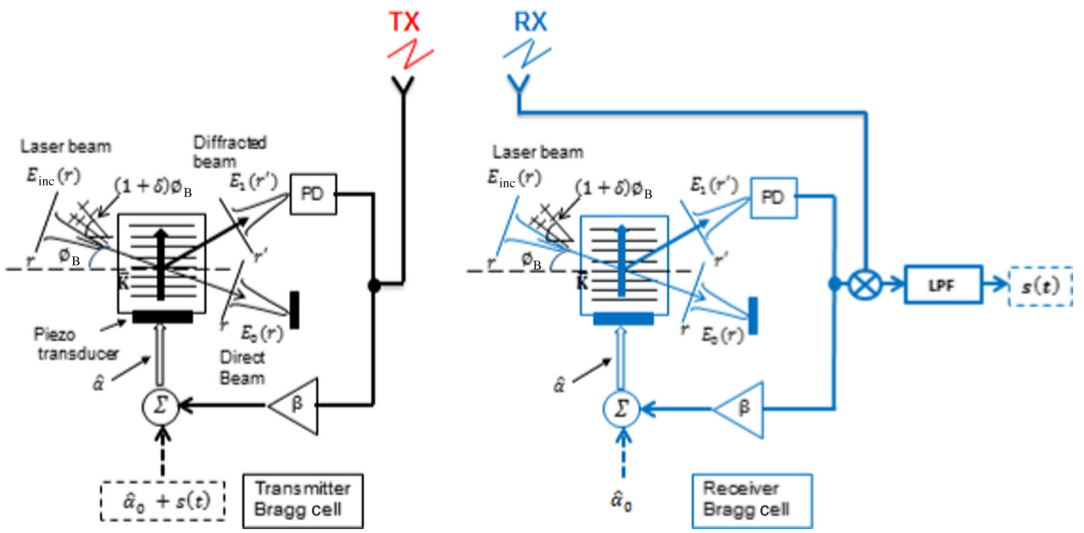

Fig. 3 Heterodyne scheme for encrypting and decrypting using A-O chaos.

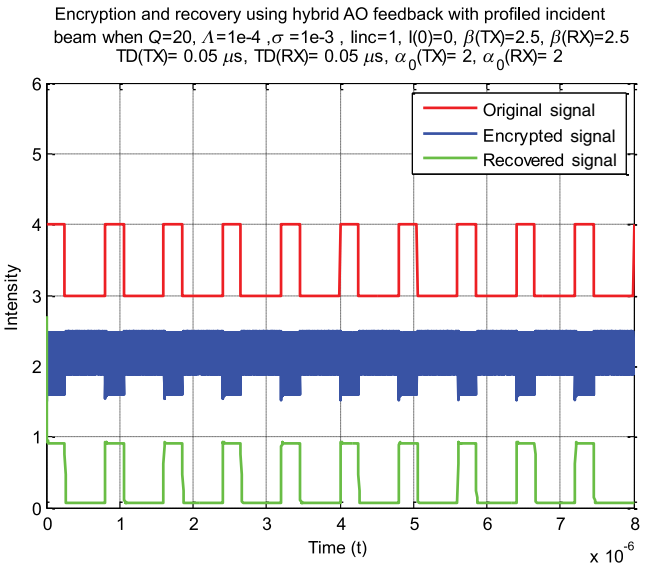

Fig. 4 Encryption and recovery of a square waveform using chaos.

dynamical quadratic map equation [Eq. (2)] numerically through iterations involving standard nonlinear dynamics. For these examples, the channel is assumed to be noiseless, exactly matched parameters are used, and the transmitter and receiver use identical input beam profiles. The first type of input signal $s(t)$ examined is a square wave with a frequency of a few MHz, illustrated in Fig. 4 along with the encrypted signal and recovered wave. The encrypted signal clearly has the original square wave in its envelope, illustrating that the system behaves as an amplitude modulator in this case.[6] This type of behavior, which occurs for relatively low feedback gains, is undesirable because the signal is apparent in the envelope and is, therefore, not effectively encrypted. A properly encrypted signal, in which the original is completely obscured within the modulated waveform, is achieved by sufficiently increasing the gain. This is shown with later simulation results.

Figure 5 shows the results for a second input signal, which is a 13-s audio clip with a 10-KHz bandwidth. The

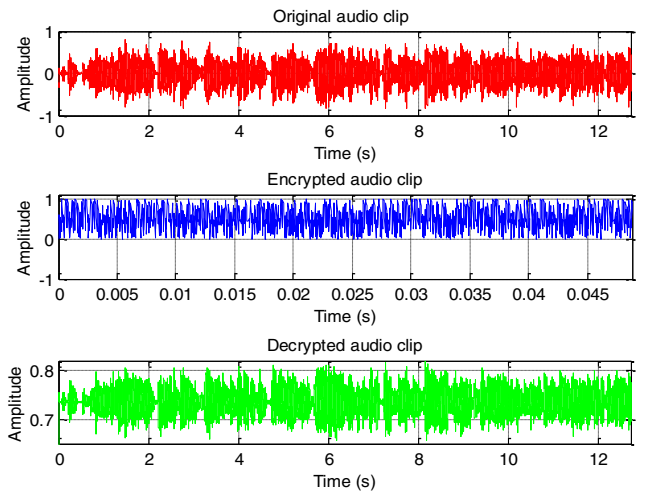

Fig. 5 Encryption and recovery of an audio signal using hybrid A-O feedback with profiled incident beam in the time domain when $Q = 20$, $\Lambda = 1e-4$; matched transmitter and receiver keys; $\tilde{\beta} = 3.4$, TD $= 0.05$ μs, $\hat{\alpha}_0 = 2$.

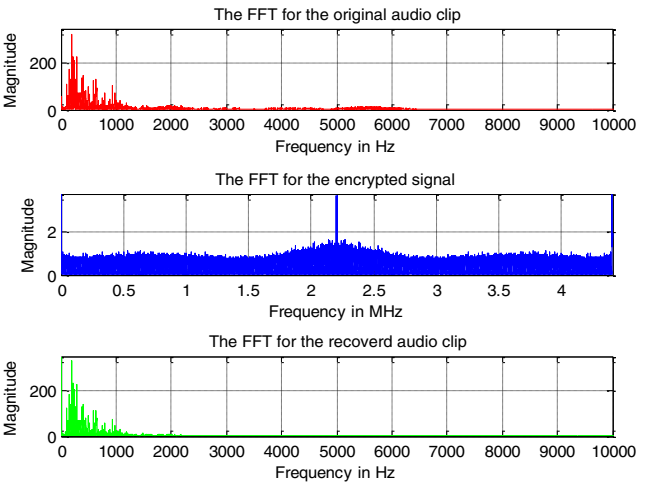

Fig. 6 Encryption and recovery using hybrid A-O feedback with profiled incident beam in the frequency domain when $Q = 20$, $\Lambda = 1e-4$; matched transmitter and receiver keys; $\tilde{\beta} = 3.4$, TD $= 0.05$ μs, $\hat{\alpha}_0 = 2$.

amplitudes for the original, encrypted, and reconstructed signals are plotted in the time domain. In this case, the set of parameters chosen produces complete encryption and the encrypted signal has no clear pattern to its envelope. The decrypted audio clip accurately reproduces the original sound. Figure 6 illustrates the encryption process in the frequency domain by showing the corresponding spectra for the original, encrypted, and reconstructed signals. The spectrum for the original audio signal is not at all apparent in the encrypted spectrum.

Figure 7 illustrates the third example of modulation and recovery, using an 8-bit pulse code modulation (PCM) representation of a sinc^2 waveform. The range of the original signal is divided into 256 uniform intervals, each interval corresponding to a unique byte, and samples of the original analog signal are quantized at a rate of 125 Hz. This creates a PCM version of the sinc^2 signal that is 1200 bits in length. This digitized version of the signal is shown in Fig. 7 along with its encrypted and recovered versions in analog form. The quantized signal is recovered by digitizing the recovered

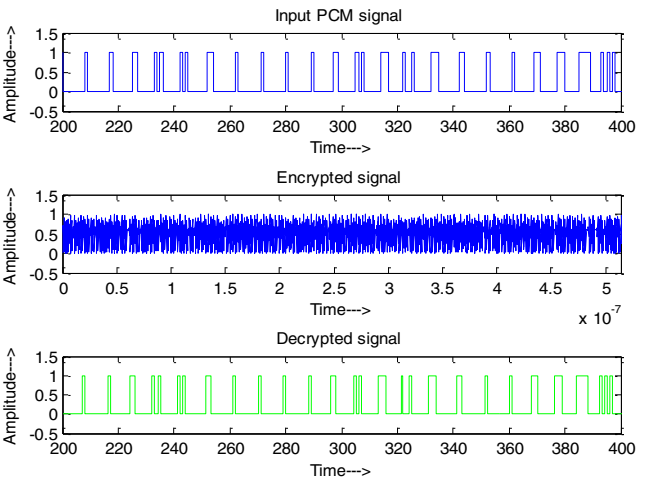

Fig. 7 Encryption and recovery of a PCM signal using hybrid A-O feedback with profiled incident beam when $Q = 20$, $\Lambda = 1e-4$; matched transmitter and receiver keys; $\tilde{\beta} = 3$, TD $= 0.05$ μs, $\hat{\alpha}_0 = 2$.

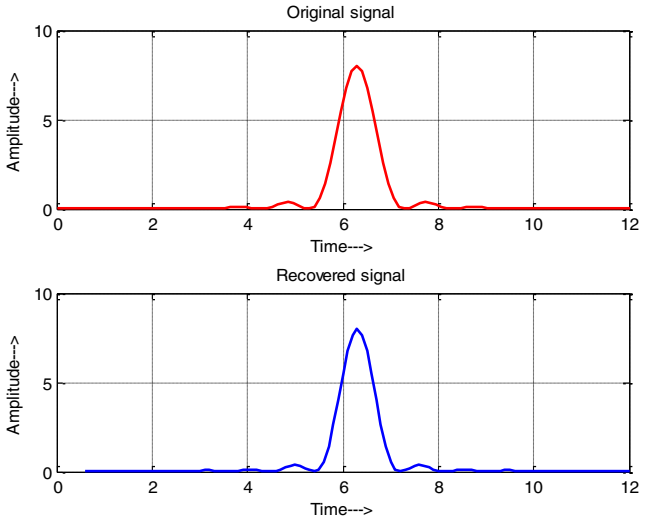

Fig. 8 Original analog and recovered quantized signals from the PCM transmission with no bit errors in the recovery.

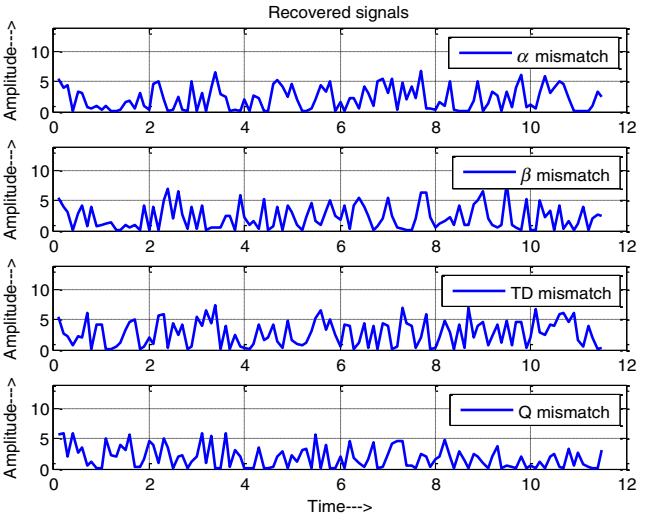

Fig. 9 Signal recovery with parameter mismatch using hybrid A-O feedback with profiled incident beam, assuming single-parameter mismatch, using 0.5% for $\hat{\alpha}_0$, 0.28% for $\tilde{\beta}$, 0.8% for TD, and 5% for Q.

signal through a rounding operation and mapping each byte of the result to the corresponding amplitude level. Figure 8 shows the original analog sinc[2] and its recovered quantized version, which appear identical at an 8-bit quantization. Since the transmitter and receiver use matched parameters and the same beam profile, there are no bit errors in this example.

4 Test of Robustness, Reliability and Parameter Tolerances

These tolerance thresholds for the parameters are summarized in Table 1. Together, the four parameters form an encryption key, and as the mismatch tolerances decrease, the key becomes stronger. To understand the effect of profiled beams on the key strength, the simulation using the PCM signal is conducted again, but with the uniform beam assumption and corresponding equations. For this case, the encrypted signal is independent of Q (assuming pure Bragg operation), which reduces the key to three parameters (also reducing its strength). The mismatched results are shown in Table 1, and clearly the simulation using profiled beams leads to a stronger encryption key due to the much smaller thresholds and the Q dependence in the profiled beam case. This shows that realistic profiled beams have the effect of strengthening the encryption. This is intuitive only in the sense that a profiled beam inherently offers variable amplitudes to the diffraction system, and this likely provides a higher degree of encryption for the highly amplitude-sensitive chaos wave.

Table 1 Approximate tolerances for the four encryption/decryption key values, comparing nonuniform beam to uniform beam simulations.

Key parameters	Encryption value	Measured tolerance for nonuniform beam (% diff)	Measured tolerance for uniform beam (% diff)
$\hat{\alpha}_0$	2.0	±0.5	±10
$\tilde{\beta}$	3.6	±0.28	±2.7
TD	0.05 μs	±0.8	±2.5
Q	20	±5.0	N/A

To quantify the effect of mismatch on bit errors, random sequences of bits are transmitted through the system at varying levels of mismatch, and the percentage of bits in error is then used to estimate bit error rate (BER). As before, only one parameter mismatch is considered at a time, the same beam profile is used at both receiver and transmitter, and there is no channel noise. To keep the simulation manageable, the random bit sequences were restricted to a length of one million. For each level of mismatch, the simulation is executed for both uniform and nonuniform beams. The results are summarized in two BER plots (one for each case) in Fig. 10 as a function of percent mismatch in $\tilde{\beta}$. As the mismatch approaches zero, both curves appear to indicate that BER approaches 10^{-6}, but this is an artifact caused by the restricted length of the bit sequences tested. Consistent with the results in Table 1, the BER curves illustrate that simulations with nonuniform beams result in a much greater sensitivity to mismatch. For the nonuniform case, a mismatch in $\tilde{\beta}$ of about 0.3% produces a BER of 10^{-4}. To reach this level of BER for the uniform case, a mismatch of greater than 2% is required.

The next simulation conducted for this work measures the effect of additive white Gaussian channel noise (AWGN) on the encryption/decryption process, assuming matched parameters in this case. Random bit sequences are encrypted transmitted with AWGN, decrypted, and bit errors are counted. The BER is measured as a function of the ratio of energy per bit (E_b) to noise power (with PSD $N_0/2$), and the BER curve is plotted on a logarithmic scale. This type of plot is a standard figure of merit for any digital communication system, and it allows the performance for a chaotic communication system to be compared to other designs.[13] For example, one simple digital communication scheme is binary phase shift keying (BPSK) where a positive DC voltage (say +V) represents 1 and a negative DC voltage

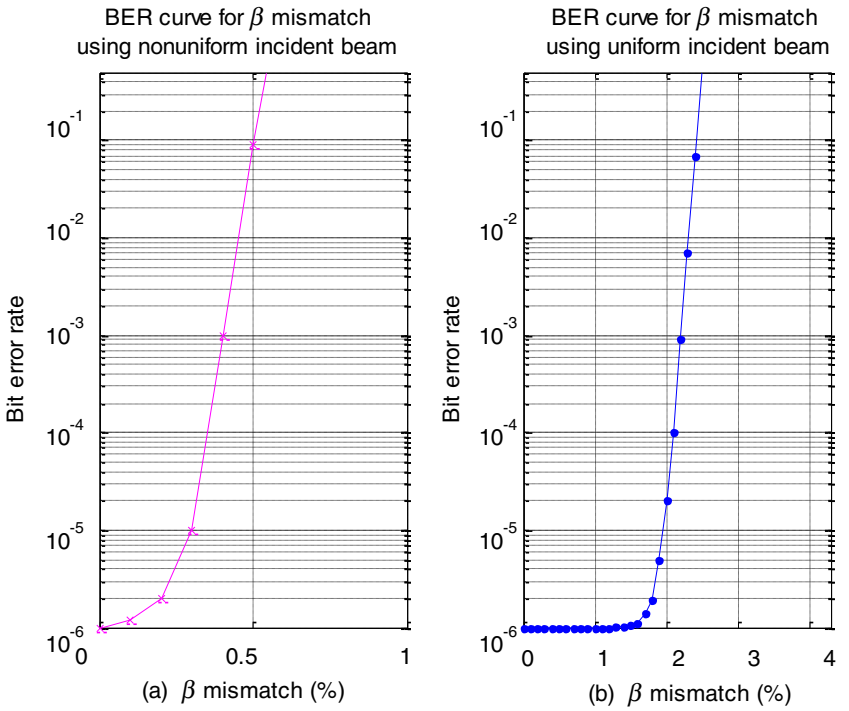

Fig. 10 Bit error rate (BER) curves for percent mismatch in $\tilde{\beta}$ for the nonuniform beam simulation (a) and the uniform beam simulation (b).

(−V) represents 0, and the detector makes bit decisions by comparing the received voltage to 0. For comparison, Fig. 11 shows the BER curve for the A-O chaotic system alongside the curve for a BPSK system. We note here that the BER is generated in the BPSK system through the AWGN channel noise; however, this system does not incorporate any chaotic encryption. Conversely, the encrypted A-O chaotic wave experiences BER via the presence of AWGN noise in the transmission channel. As might be expected, the complexity created by the (chaotic) encryption causes a gap between the curves indicating that greater energy per bit is required for the encrypted system in order to reach a given error rate. This gap can be viewed as the energy cost of encryption relative to BPSK, a cost inherent in generating the chaos. Overall, the increased signal energy demand placed by the chaotic encryption process may still be considered relatively marginal, especially in view of other modulation systems (such as ASK and FM) which in any event also do not provide any signal security.

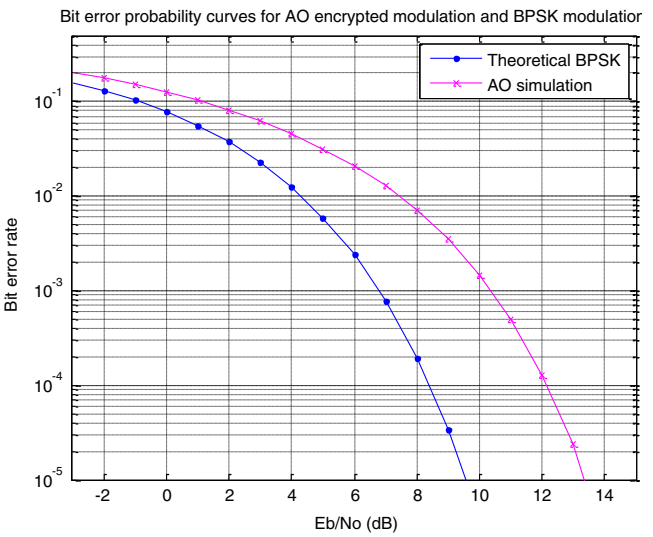

Fig. 11 BER curves for two digital communication systems: binary phase shift keying and A-O chaotic encryption system.

To explore the effect of parameter mismatch, the simulation with the PCM signal in Fig. 7 is demodulated with a chaotic signal in the receiver created with mismatched parameters. The mismatch is studied one parameter at a time, keeping the other three parameters matched. For example, the mismatch in $\hat{\alpha}_0$ is created by transmitting the PCM signal using $\hat{\alpha}_0 = 2.0$ and demodulating with $\hat{\alpha}_0 = 2.01$. The other three parameters are matched, using $\tilde{\beta} = 3.6$, TD $= 0.05$ μs, and $Q = 20$. The increase of 0.5% in $\hat{\alpha}_0$ creates bit errors causing the reconstructed sinc^2 to appear as noise, shown in Fig. 9. Bit-errors begin to appear with a $\hat{\alpha}_0$ mismatch in the range 0.3%, ruining the recovery. Mismatch for the other three parameters is similarly studied, and the noise-like reconstructions produced are also shown in Fig. 9. The level of mismatch for each parameter is selected to be the smallest that completely obscures the signal.

5 Interpretations

There is an enormous demand for tools and hardware for achieving reliable and secure communication, motivating the efforts for chaotic encryption described in this and other recent work. As illustrated, the smallest parametric mismatch (fractions of a percent for nonuniform beams) between the transmitter and the receiver HAOFs will destroy the signal recovery. These parameters together serve as a decoding key, and it is probabilistically unlikely that a hacker

could simultaneously guess all four elements of this key, especially with an infinitesimally small compound tolerance. Furthermore, the efforts to better model the physics of realistic laser beams used in the HAOF have naturally led to a stronger encryption key relative to simpler models that assume uniform plane wave beams. This is because real lasers have a nonuniform intensity profile which affects the shape of the diffracted beam profile and leads to dramatic changes in chaotic behavior. This suggests that the specific profile shape will also be an element of the encryption key, although the current work does not explore this idea. Generally, it is expected that modification to the model that more accurately represents the true physics will only serve to strengthen the encryption.

With the current model, Table 1 summarizes how the encryption key is made stronger by implementing profiled beams relative to uniform beams. This (generally significant) improvement to the model causes the encryption to be sensitive to Q and it decreases the thresholds for the other three parameters. The measured tolerance threshold for Q may appear weaker than the other parameters, but it still serves to significantly strengthen the key. Overall, the addition of Q to the key and the decreased thresholds lowers the probability of randomly guessing the encryption key by approximately three orders of magnitude.

To determine the thresholds presented in Table 1, the mismatch for each parameter is gradually increased, one at a time, and the reconstructed sinc^2 begins to deteriorate. The threshold for each parameter is determined by the amount of mismatch that qualitatively reduces the reconstruction to a noise-like signal. These noisy reconstructions are exhibited in Fig. 9. These thresholds will naturally be signal dependent, and the analyses here are intended to only show how the encryption is strengthened for one particular signal.

To explore the effect of mismatch on digital signals more quantitatively, Fig. 10 illustrates BER versus percent mismatch in $\tilde{\beta}$ for random bit sequences. BER estimates for both nonuniform and uniform beam simulations are shown, and sensitivity to mismatch is much greater for the nonuniform beam case. The curves indicate that for the uniform beam simulation, about a seven times greater mismatch in $\tilde{\beta}$ is required to produce the same BER obtained in the nonuniform simulation. This is consistent with the qualitative results summarized in Table 1. The greater sensitivity of BER to mismatch for the nonuniform beam simulation is also observed for the other three parameters.

As with any digital communication system, additive channel noise will reduce reliability, and this is commonly measured with BER plots as a function of the ratio energy per bit to noise power. Figure 11 compares the performance of the A-O encrypted system (assuming matched parameters) to a simple BPSK system. The curves have a similar shape, but the A-O encrypted system curve is shifted to the right of the BPSK curve, showing a loss of performance. This is expected due to the greater complexity of the encryption, and the gap between the curves can be interpreted as the cost of the encryption. Any given application for the system will have some BER requirement and fixed noise level, and a plot such as Fig. 10 shows how much the energy per bit would have to be increased to meet the requirement relative to BPSK system. Increasing the energy per bit is achieved by slowing the bit rate or by increasing the amplitude of the transmitted signal. Noise may also be introduced into the simulation via the photodetector or the feedback amplifier. Results for such tests are not reported in this paper. However, it may be noted that the feedback system is found to be relatively robust for low detector noise variances; beyond a threshold noise power, it is found that the BER increases sharply.

6 Conclusion

The propagation of a profiled optical beam through an A-O Bragg cell was previously examined using a transfer function formalism. The results showed dependence of the first-order scattered light on the effective Q, the acoustic wavelength and the profile shape. It is observed that for a large Q (greater than 50), the output profile begins to deviate from the uniform beam response, which strongly affects the closed-loop behavior of the device. In this work, the implications of these changes for encryption are explored in some detail by comparing simulations with nonuniform beams to simulations with uniform plane waves. The simulations transmit encrypted digital signals, using chaotic modulation and demodulation in the manner of heterodyne system. The robustness of the recovered signal to parameter mismatch is explored, and it is found that simulations with nonuniform beams produce a stronger encryption that simulations with uniform beams. This is because in order to accurately recover the encrypted signal, the parameters used in the encryption must each be known to within a fraction of a percent, and this threshold decreases significantly for nonuniform beams. Reliability in the presence of channel noise is also studied relative to a simple BPSK system, indicating the increased energy cost for encrypting a digital signal. Future work will consider practical signals with specifications for applications, further performance analysis of the current model, and other modifications to the model.

Acknowledgments

One of us (FSA) would like to express sincere appreciation for the financial support provided by the Saudi Arabia Cultural Mission. M.R.C. would like to thank the ECE Department, University of Dayton, for providing generous travel support that enabled dissemination of this work at multiple conferences.

References

1. S.-T. Chen and M. R. Chatterjee, "A numerical analysis and expository interpretation of the diffraction of light by ultrasonic waves in the Bragg and Raman-Nath regimes multiple scattering theory," *IEEE Trans. Educ.* **39**(1), 56–68 (1996).
2. A. Korpel, *Acousto-Optics*, 2nd ed., Marcel Dekker, New York (1997).
3. J. Chrostowski and C. Delisle, "Bistable piezoelectric Fabry–Perot interferometer," *Can. J. Phys.* **57**, 1376–1379 (1979).
4. J. Chrostowski and C. Delisle, "Bistable optical switching based on Bragg diffraction," *Opt. Commun.* **41**, 71–74 (1982).
5. P. P. Banerjee, U. Banerjee, and H. Kaplan, "Response of an acousto-optic device with feedback to time-varying inputs," *Appl. Opt.* **31**, 1842–1852 (1992).
6. M. Chatterjee and M. A. Al-Saedi, "Examination of chaotic signal encryption and recovery for secure communication using hybrid acousto-optic feedback," *Opt. Eng.* **50**, 055002 (2011).
7. A. K. Ghosh and P. Verma, "Lyapunov exponent of chaos generated by acousto-optic modulators with feedback," *Opt. Eng.* **50**, 017005 (2011).
8. F. S. Almehmadi and M. R. Chatterjee, "Numerical examination of the nonlinear dynamics of a hybrid acousto-optic Bragg cell with positive feedback under profiled beam propagation," *J. Opt. Soc. Am. B* **31**, 833–841 (2014).

9. M. C. Soriano et al., "Digital key for chaos communication performing time delay concealment," *Opt. Lett.* **36**, 2212 (2011).
10. M. R. Chatterjee, T.-C. Poon, and D. N. Sitter Jr., "Transfer function formalism for strong acousto-optic Bragg diffraction of light beams with arbitrary profiles," *Acustica* **71**, 81–91 (1990).
11. M. R. Chatterjee and F. S. Almehmadi, "Numerical analysis of first-order acousto-optic Bragg diffraction of profiled optical beams using open-loop transfer functions," *Opt. Eng.* **53**, 036108 (2014).
12. M. R. Chatterjee and F. S. Almehmadi, "Information encryption, transmission, and retrieval via chaotic modulation in a hybrid acousto-optic Bragg cell under profiled beam illumination," *Proc. SPIE* **9216**, 92160S (2014).
13. J. E. Gilley, *Bit-Error-Rate Simulation Using Matlab*, Transcrypt International, Inc. (2003).

Fares S. Almehmadi received his BSEE degree in electrical engineering from Umm Al-Qura University, Saudi Arabia, in 2009, and the MSEE degree from the University of Dayton in 2011. He is currently completing his research for the PhD degree at the University of Dayton. His areas of research interests include acousto-optic interactions, nonlinear optics, signal processing, and digital communications. His doctoral work has resulted in three conference presentations and proceedings articles, and two journal papers.

Monish R. Chatterjee received the MS and PhD degrees from the University of Iowa in 1981 and 1985, respectively. He is currently a professor of electrical and computer engineering at the University of Dayton. He has contributed over 150 papers to archival journals and conference proceedings. He is a senior member of the IEEE and the OSA, a member of SPIE and Sigma Xi, and a fellow of the Golden Key Honor Society.