8-2014

Information Encryption, Transmission, and Retrieval via Chaotic Modulation in a Hybrid Acousto-optic Bragg Cell under Profiled Beam Illumination

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

Fares S. Almehmadi
University of Dayton

Information encryption, transmission, and retrieval via chaotic modulation in a hybrid acousto-optic Bragg cell under profiled beam illumination

Monish R. Chatterjee[1*] and Fares S. Almehmadi[1]

[1]University of Dayton, Dept. of ECE, 300 College Park, Dayton, OH 45469-0232

*corresponding author

Email: mchatterjee1@udayton.edu

ABSTRACT

In recent work, the propagation of a profiled optical beam through an open-loop acousto-optic Bragg cell was examined using a transfer function formalism. The device was also studied under closed-loop via intensity feedback, and shown to exhibit more extended chaotic band responses, thereby potentially increasing the dynamic range and parameter sensitivities of any applied signal and the device operation respectively. In this paper, simple low- to mid-RF signals (periodic waveforms and low BW audio) are transmitted through the closed-loop system and the resulting encryption and recovery at the receiver are examined especially from the perspective of overall robustness of the system.

Keywords: acousto-optics, Bragg regime, scattering, Gaussian, Klein-Cook, chaos, encryption, decryption, modulation.

1. INTRODUCTION

Acousto-optic (A-O) devices can controllably diffract light beams, using the interaction of light and sound. An input light beam passes through a crystal in which acoustic vibrations are made with a piezoelectric device. These vibrations act as a diffraction grating, causing input beam deflection. A-O cells are frequently used in signal processing applications, including laser beam deflection, modulation, filtering, and encryption/decryption when used with feedback [1]. The characteristics of the deflection depend upon the light and sound frequencies and crystal properties. These variables are summarized by a unitless quantity known as the Klein-Cook parameter Q. In the Bragg mode of operation, Q is larger than 8π, and the cell produces only one diffracted order [2].

To create a closed-loop system from such a Bragg cell, the diffracted beam is collected by a photodetector, whose output is amplified, added to a dc offset, and fed back to the acoustic driver for the piezoelectric device. As a signal processing device, the input signal is applied to the dc offset, and the output signal is taken from the photodetector. The behavior of the resulting system exhibits nonlinear dynamics, including mono-, bi-, multistable and chaotic behavior [3-5]. These dynamic properties are useful for many signal processing applications including signal encryption and decryption [6].

Two techniques are used to characterize the chaotic behavior of such A-O systems: the Lyapunov exponent and bifurcation maps. The Lyapunov exponent quantifies whether the system is chaotic or not, as a function of Q, the dc bias, feedback gain and input light intensity. Bifurcation maps are plots of photodetector output versus the optical phase shift or feedback gain, and they visually show the threshold between bistability and chaos [7]. When using either technique to study A-O feedback behavior, chaotic bands appear at unpredictable intervals over the parameter ranges. In order to use such passbands of chaos for encryption, it is critical to know what combination of parameters produces chaos [8].

Optics and Photonics for Information Processing VIII, edited by Abdul A. S. Awwal, Khan M. Iftekharuddin, Mohammad A. Matin, Andrés Márquez, Proc. of SPIE Vol. 9216, 92160S © 2014 SPIE
CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2064112

In order to use chaos to encrypt a signal, the signal is applied to the bias driver in the feedback loop. The output of the photodetector is a chaotically encrypted version of the input signal, which will be transmitted through a channel. This chaotic signal has an amplitude that is related to the input signal amplitude via the RF oscillator. At the receiver, in order to demodulate this signal, a matched A-O feedback loop is used in the manner of a standard heterodyne detector. If there is a mismatch in any parameter (bias voltage, feedback gain, and time delay), ideally demodulation fails. The locally generated chaos is then multiplied with the incoming photo-detected modulated chaotic signal. The product waveform is then passed through a low pass filter (LPF) with cutoff frequency adjusted to accommodate the signal bandwidth, and corrected for a 180º phase shift [6].

Previous analysis of closed-loop nonlinear properties utilizes the assumption of a uniform plane wave input light beam, and uses weak interaction theory to describe the light and sound interaction. These analyses lead to commonly used expressions for Bragg diffraction, which were used to model chaos and thereafter use it to encrypt/decrypt low frequency signals [6]. Recently published work has demonstrated that the uniform beam assumption does not capture the effect of realistic profiled beams. The chaotic behavior for a non-uniform profiled beam is shown to be significantly different, and a simulation of chaos using non-uniform profile beams was recently developed. It is shown that the location and width of the passbands of chaos are sensitive to input beam profiles [8]. The present work uses this simulation to encrypt and decrypt audio and PCM signals, and analyzes the sensitivity of the encryption.

An overview of first-order A-O Bragg diffraction, in open-loop operation, is presented in section 2, describing the significance of using profiled optical beams. In section 3, the nonlinear dynamics for closed-loop operation are described, including the conditions necessary for chaos and utilizing the chaos for encryption. Encryption results for periodic, audio and PCM signals are presented in section 4 along with an analysis of the robustness of the encryption to mismatch between transmitter and receiver parameters. The final section summarizes the main results and provides concluding remarks along with a discussion of future encryption work involving a wider variety of signals.

2. First-order A-O Bragg diffraction with profiled optical beams under open-loop propagation

An A-O modulator is shown in Fig.1 with first-order feedback, illustrating two scattered orders created by an arbitrary input profile. This section studies the open-loop characteristics the device such that the feedback loop is ignored. The profiled input light is incident nominally at the Bragg angle at the left plane of the cell. 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 zeroth- and first-order scattered outputs are $E_0(r)$ and $E_1(r')$, $\delta\phi_B$ is the angular deviation from the Bragg angle $\emptyset_B(\approx K/2k)$, and $\bar{K}$ is the acoustic wave vector [9]. Using plane wave angular decomposition theory, a profiled beam is represented as a spectrum of its constituent uniform plane wave components incident at an arbitrary angle $(1+\delta)\phi_B$ where δ is a dimensionless measure of angular deviation. A set of coupled differential equations leads to expressions for the two scattered orders $\tilde{E}_0$ and $\tilde{E}_1$ for near-Bragg diffraction [5]. Using these expressions, a transfer function formalism is developed by Chatterjee *et*. al [9]. An inverse Fourier transform is applied to the product of the incident spectrum $\tilde{E}_{\text{inc}}(\delta)$ and the transfer function $\tilde{H}(\delta)$, as shown in eq.1 [9]. In this equation, $E_{out}(r';r)$ is either the first- or zeroth-order output, depending on the transfer function used, $\emptyset_B$ is the Bragg angle of the sound cell, and lambda is the wavelength. The output spectra are functions of the peak phase delay $\hat{\alpha}_0$ and the Klein-Cook parameter Q.

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

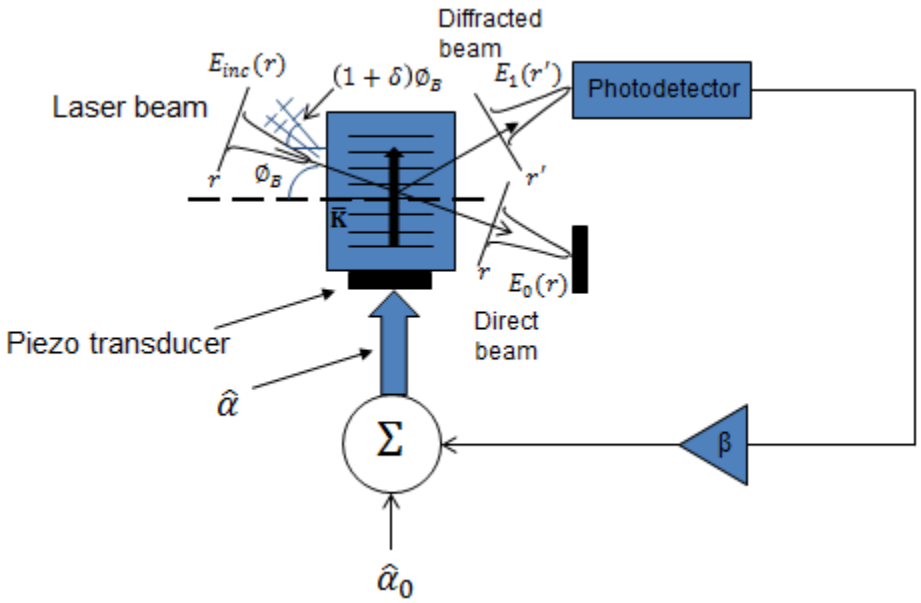

Fig.1. A-O closed-loop hybrid system with an arbitrary incident beam profile.

Previous work presented results using eq.1 with various incident profiles $E_{inc}(r)$. For a uniform plane wave input profile, the results indicated the well-known ($\sin^2$- in intensity) shape in the diffracted output along the optical phase shift axis. With a Gaussian input profile, the diffracted output is similar only at relatively small values of Q (typically about 20-50). At higher Qs, on the other hand, it is found that the first-order intensity deviates substantially from the expected $\sin^2$-pattern. Additionally, the output profiles at higher Qs are also found to deviate from the Gaussian shape [10]. Figure 2 displays these characteristics showing the output intensity profile along the peak phase delay $\hat{\alpha}_0$ for three different values of Q.

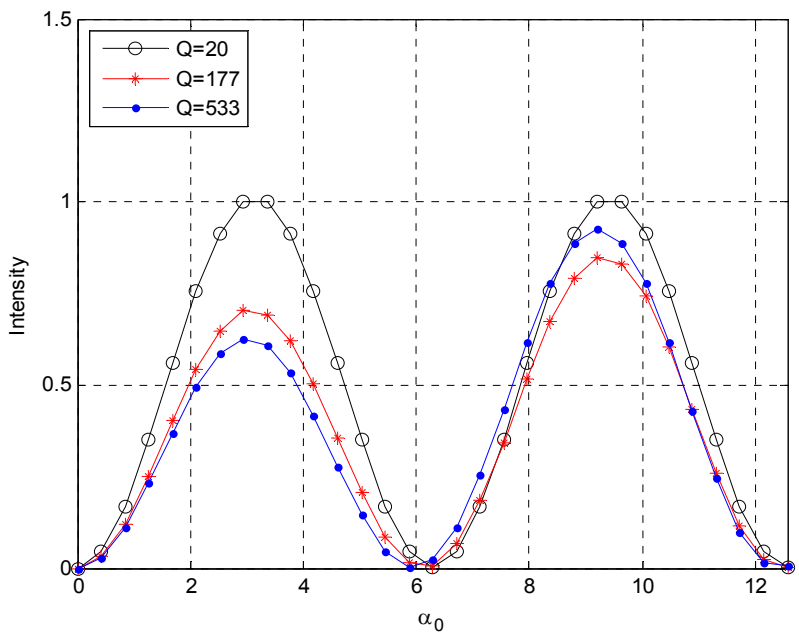

Fig.2. First-order intensity Bragg diffraction versus the optical phase shift for Q=20, 177, and 533.

As is clearly visible in Fig.2, unexpected deviations from the standard theory occur at higher Q values. The curve for Q=20 appears consistent with uniform plane wave inputs, although the impact is significant in the closed-loop system (primarily due to the non-uniform output amplitudes) as is discussed in [8]. The $\hat{\alpha}_0$ intensity profile deviates from the standard $\sin^2$ behavior as Q increases, showing that the curve for Q=533 clearly no longer exhibits the uniform plane wave characteristics. In general, the diffracted outputs for non-uniform incident beams deviate significantly from uniform plane wave behavior, which has a strong effect on the nonlinear dynamics of the A-O hybrid feedback system. Since real laser beams are profiled, it is critical to understand and module these behaviors. [10]

3. Characterizing chaotic behavior of closed-loop A-O systems with profiled beams

The hybrid closed-loop A-O system, as shown in Fig.1, is created by passing the first order diffracted light into a photodetector, whose output is amplified and fed back into the acoustic driver. The photodetector current $I(t)$ exhibits nonlinear dynamics, including mono, bi-, multistabilty, and chaotic behavior which was first observed in 1978 [5]. If a uniform plane wave input is assumed, then well-known analysis leads to an expression of $I(t)$ [5]. To understand the effect of profiled beams, a modified version of this equation was developed and used to simulate the system for arbitrary profiled beams [8]. Equation 2 contains this expression, where the function f represents the observed output along the optical phase shift dimension for a non-uniform input profile [8].

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

The function f, an example of which is shown in Fig.2, has no closed-form expression, unlike the uniform plane wave case where f is replaced by the sine-profile. For the simulation shown in this paper, a Gaussian input profile is used to numerically determine f. In this equation, $\hat{\alpha}_0$ is the peak phase delay, $\tilde{\beta}$ is the feedback gain, and TD is the feedback time delay. The time delay is due to the photodetector, amplifier, and the overall physics of the A-O cell [5].

In order to use the closed-loop system for encryption applications, it is necessary to understand which combination of parameters produces chaos in the photodetector current. It was previously shown that the threshold value of $\tilde{\beta}$ between bistabilty and chaos is strongly affected by profiled beam inputs [8]. Furthermore, for fixed values of $\tilde{\beta}$ and TD that produce chaos, the specific pattern of the chaos is a function of $\hat{\alpha}_0$. This pattern can be characterized using two equivalent techniques, namely Lyapunov exponent and bifurcation maps. The Lyapunov exponent is a parameter used in modeling the incremental changes in photodetector intensity, and it is useful here because the system is only chaotic if the LE is positive [7]. Bifurcation maps are plots of the photodetector output versus peak phase delay, with other parameters constant, illustrating sudden changes in the dynamic behavior.

Figure 3 contains an example of a bifurcation map plotted alongside the Lyapunov exponent, showing bands of chaos whenever the LE is positive. Both plots are generated independently and they are in close agreement. A Gaussian input profile was used to generate these data with parameter values as shown in the figure. The locations, amplitude, and width of these bands are sensitive to the value of $\tilde{\beta}$ [8]. Furthermore, when compared to a uniform plane wave input, there is a greater number of passbands of chaos and the general characteristics of chaos exhibit greater sensitivity to $\tilde{\beta}$. These factors are critical to using chaos for encrypting a signal, and they indicate why the analysis of profiled beams is necessary.

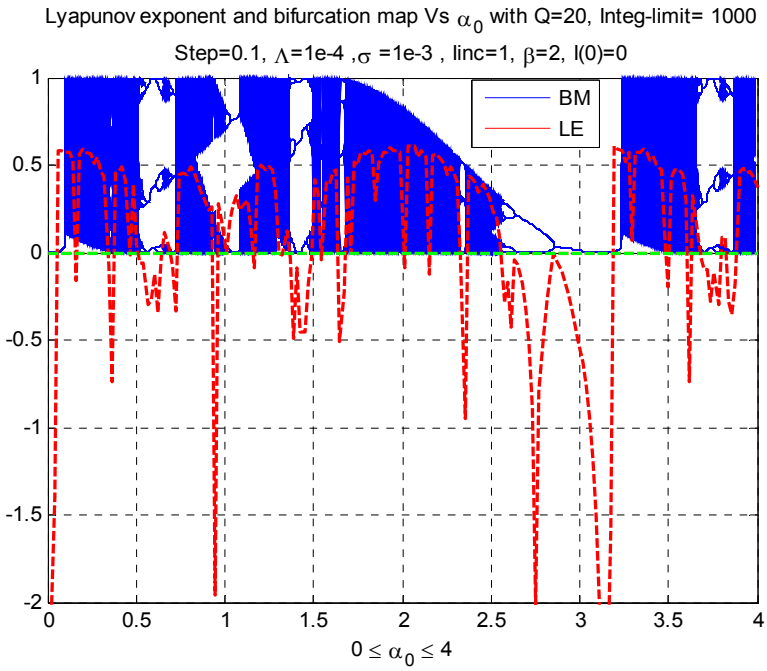

Fig.3. Lyapunov exponent and bifurcation maps versus the optical phase shift when $\tilde{\boldsymbol{\beta}}$=2.

In order to utilize chaos as a means of encrypting and securely transporting a signal waveform $s(t)$, we apply the signal to the bias driver such that the peak phase delay has the form of $\hat{\alpha} = \hat{\alpha}_0 + s(t)$. The dc offset $\hat{\alpha}_0$ is chosen to be at the center of a chaotic passband, and the range of $s(t)$ does not exceed the width of the passband. With this arrangement, the chaotic photodetector current is a modulated version of the input signal which is transmitted through a channel. At the receiver end, the signal is recovered (in the manner of standard heterodyne detection) as follows. First, a local chaos wave is generated using a second Bragg cell with matched parameters $\hat{\alpha}_0$, $\tilde{\beta}$, and TD. The local chaos (which is a photo-detected RF current corresponding to the first-order light) is then multiplied with the incoming photo-detected modulated chaotic signal. The product waveform is then passed through a low pass filter (LPF) with cutoff frequency adjusted to accommodate the signal bandwidth. A complete block diagram of the transmitter-heterodyne receiver scheme is shown in Fig.4.

It is expected that the signal $s(t)$ will modulate the chaotic carrier (AM in some limit), such that the signal will appear in the envelope of carrier [6]. However, since the chaos behaves as a random carrier, with the proper choice of parameters, the signal waveform may be completely hidden within the chaos, instead of appearing in the chaos envelope. In either case, to demodulate and retrieve the signal, the same random chaotic pattern is needed, generated using the same set of the *key* parameters. In terms of the bandwidth of $s(t)$, it should be less than half the center frequency of the chaotic carrier to avoid aliasing (in reality, this should be substantially smaller than the carrier). The chaos frequency depends on the TD through the equation $= \frac{1}{2*TD}$. In this work, the chaos frequency is in the range of 10 MHz.

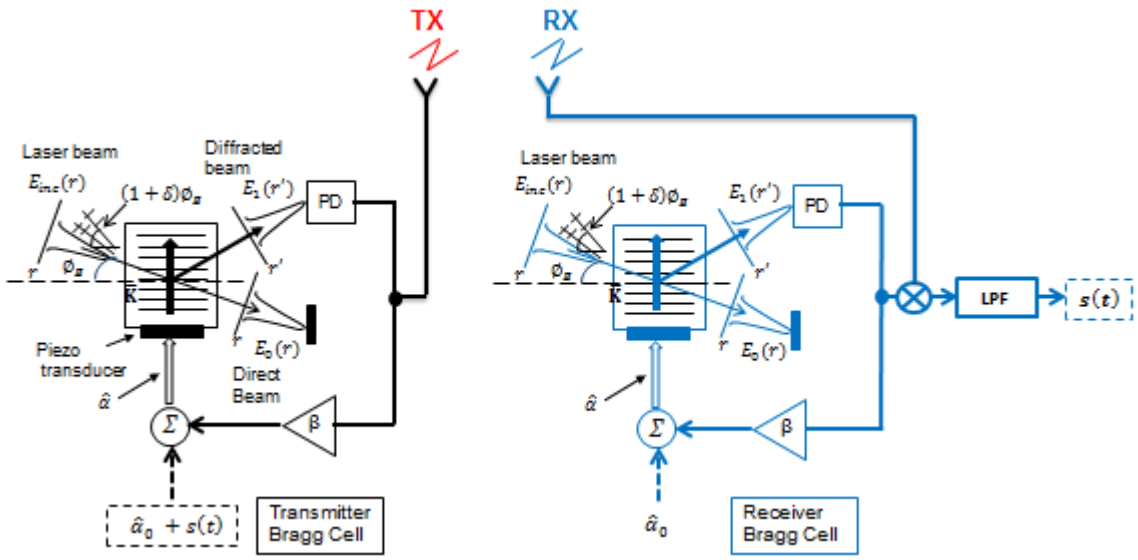

Fig.4. Heterodyne scheme for encrypting and decrypting using A-O chaos.

4. Simulation results and interpretations

A simulation of the encryption system shown in Fig.4 is implemented in Matlab and the results for several types of signals are presented in this section. Profiled beams are used in the simulation, which requires storing the (open-loop) output scattered amplitudes and thereafter running the time-dynamical quadratic map equation (eq.2) numerically through iterations involving standard nonlinear dynamics. The channel is assumed to be noiseless, and exact matched parameters (and additionally, identical input profiles) are used in both transmitter and receiver. The first type of input signal $s(t)$ examined is a periodic square wave with a frequency of a few MHz. Figure 5 illustrates the original square wave signal, the encrypted signal, and the recovered wave. The encrypted signal clearly has the original signal in its envelope, which is because the system is expected to be an amplitude modulation in some limit [6]. The simulation shows that for relatively low feedback gains, the chaos waveform tends to carry the information signal in the envelope, in which case the system does not effectively encrypt the signal. To properly encrypt a signal, we need to hide all possible obvious signatures of the signal from the transmitted waveform, which can be achieved by sufficiently increasing the gain. This is shown with later simulation results.

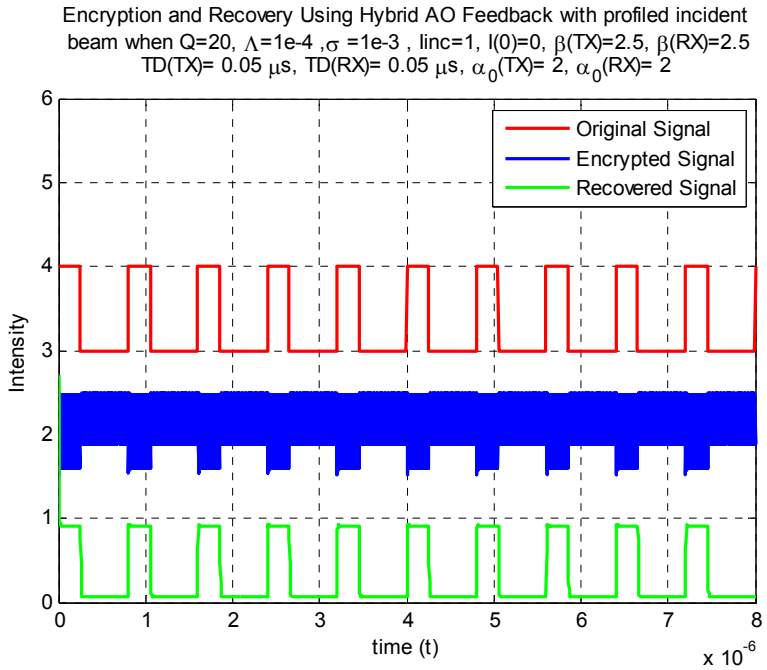

Fig.5. Encryption and recovery of a square waveform using chaos.

The second input signal $s(t)$ examined is a short audio clip 13 seconds in length with a BW of 10 KHz. The original, encrypted, and recovered signals are shown in time in Fig.6, and frequency in Fig.7. The set of parameters chosen produces complete encryption, such that the envelope no longer shows the original signal. The recovered audio clip very accurately reproduces the original signal. The encryption is also evident in the frequency domain, where the spectrum of the original audio signal is not apparent in the spectrum of the encrypted signal.

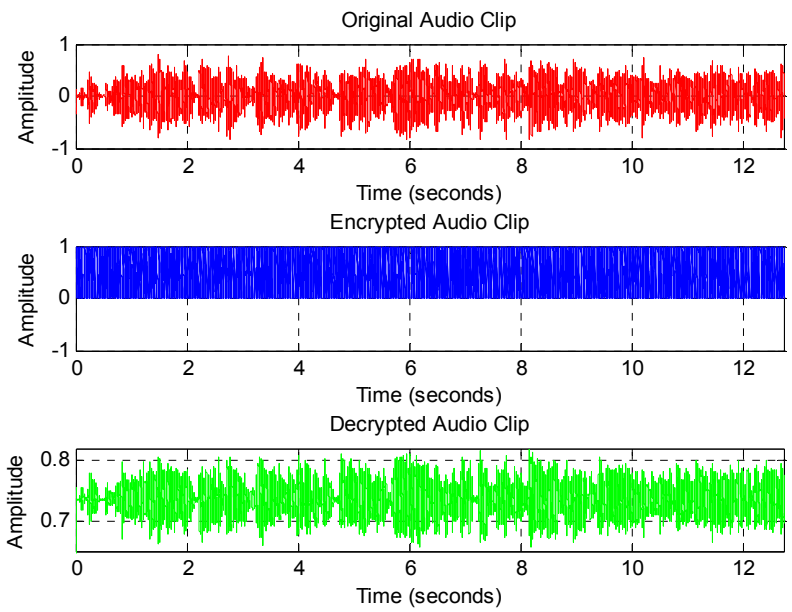

Fig.6. Encryption and recovery using hybrid AO feedback with profiled incident beam when Q=20, Λ=1e-4 , $\tilde{\boldsymbol{\beta}}$ (TX)=3.4, $\tilde{\boldsymbol{\beta}}$ (RX)=3.4, TD(TX)= 0.05 μs, TD(RX)= 0.05 μs, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$(TX)= 2, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$ (RX)= 2.

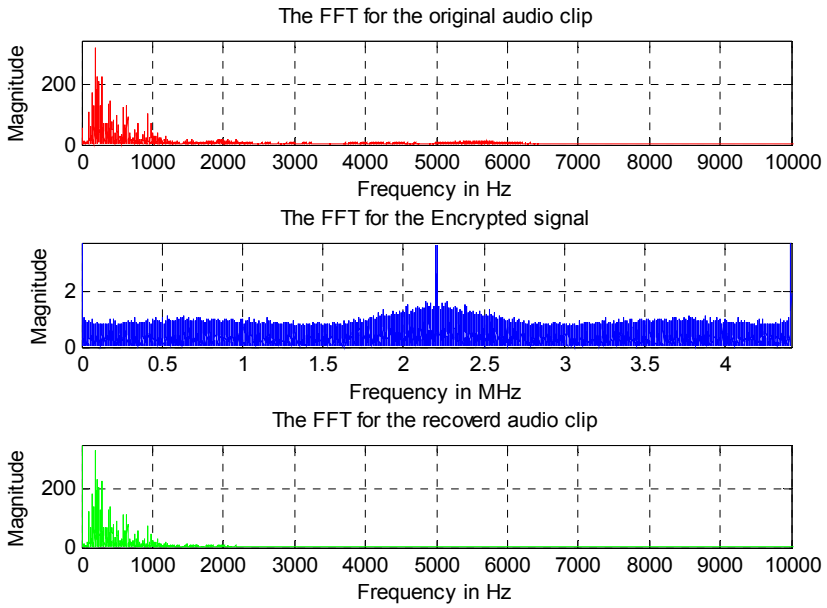

Fig.7. Encryption and recovery using hybrid AO feedback with profiled incident beam when Q=20, Λ=1e-4 , $\tilde{\boldsymbol{\beta}}$ (TX)=3.4, $\tilde{\boldsymbol{\beta}}$ (RX)=3.4, TD(TX)= 0.05 μs, TD(RX)= 0.05 μs, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$(TX)= 2, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$ (RX)= 2.

The third example considered is an 8-bit PCM representation of a sinc^2 waveform. The digitized signal is shown in Fig.8 along with its encrypted and recovered versions, with no bit errors. Figure 9 shows the original analog sinc^2 and its recovered quantized version. To study the effect of parameter mismatch, the same PCM signal is transmitted with $\tilde{\beta}$=3.6 and received with $\tilde{\beta}$ =3.61. This increase of 0.28 % creates bit errors causing the reconstructed sinc^2 to appear as noise, shown in Fig.10. Bit-errors begin to appear with a $\tilde{\beta}$ mismatch in the range 0.1 percent. This slight mismatch ruins the recovery, demonstrating that the system in Fig.4 is used to encrypt and decrypt message signals with closely matched parameters. Thus, the "matched parameters" serve as the decoding key in this system. To completely evaluate the robustness of this matched-parameter system, the recovery process should be examined under mismatch for all three parameters. This preliminary work examined $\tilde{\beta}$ mismatch only. Figure 10 illustrates the effect of a 0.28 % increase in $\tilde{\beta}$, which create significant distortion, and a similar distortion occurs for a 0.28 % *reduction* of the matched parameter $\tilde{\beta}$ in the receiver. This level of sensitivity is an order of a magnitude lower than results found using uniform input beams [6]. This is due to the fact that profiled beams are used in this simulation.

These results indicate how difficult it would be to recover the original signal from its chaotic version. Not only is $\tilde{\beta}$ needed to within a fraction of a percent, the other two feedback parameters ($\hat{\alpha}_0$ and TD) must also be known to a similar precision. In addition, the sensitivity of the chaos to profiled beams means that the Q parameter will realistically also be necessary for decryption. The sensitivity of the encryption/decryption process to Q is not apparent if A-O Bragg cell is studied under the assumption of a uniform input beam. In addition to this, profiled beam analysis shows an increased sensitivity to the feedback parameters.

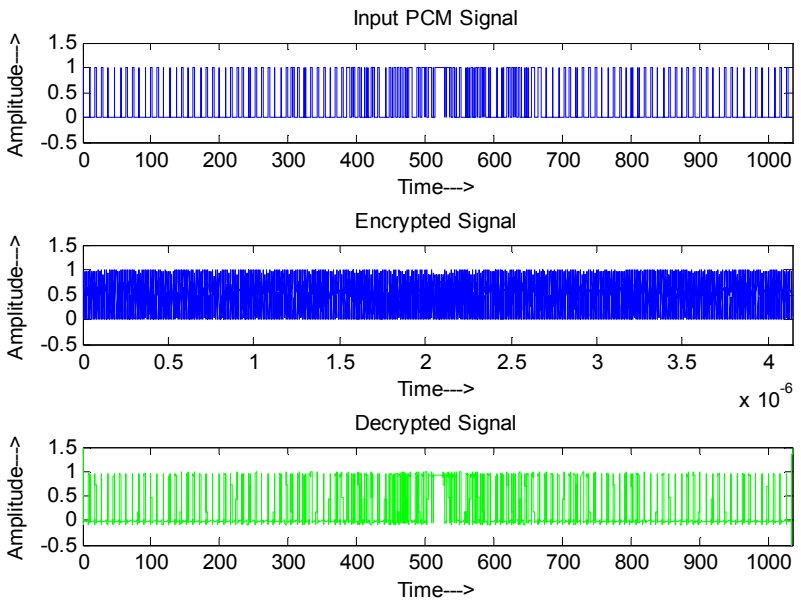

Fig.8. Encryption and recovery using hybrid AO feedback with profiled incident beam when Q=20, Λ=1e-4 , $\tilde{\boldsymbol{\beta}}$ (TX)=3, $\tilde{\boldsymbol{\beta}}$ (RX)=3, TD(TX)= 0.05 μs, TD(RX)= 0.05 μs, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$(TX)= 2, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$ (RX)= 2.

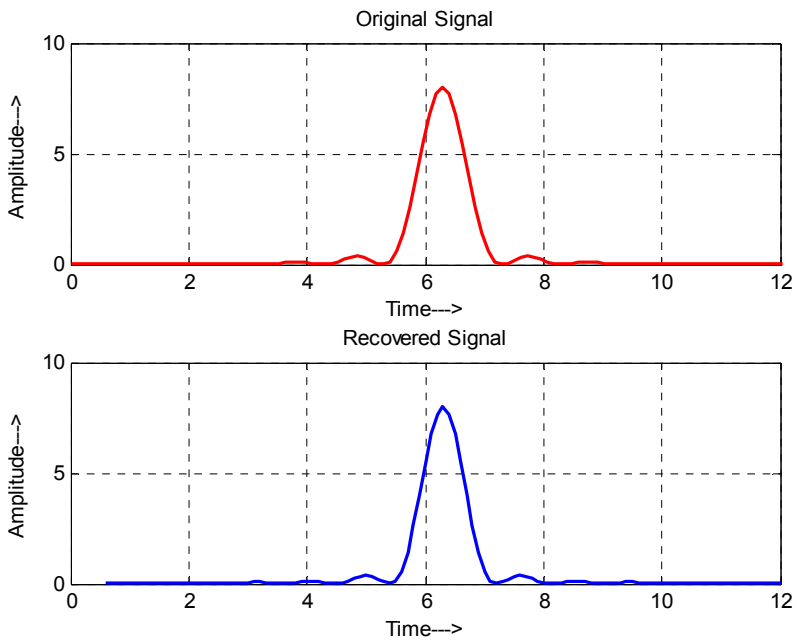

Fig.9. Encryption and recovery using hybrid AO feedback with profiled incident beam when Q=20, Λ=1e-4 , $\tilde{\boldsymbol{\beta}}$ (TX)=3, $\tilde{\boldsymbol{\beta}}$ (RX)=3, TD(TX)= 0.05 μs, TD(RX)= 0.05 μs, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$(TX)= 2, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$ (RX)= 2.

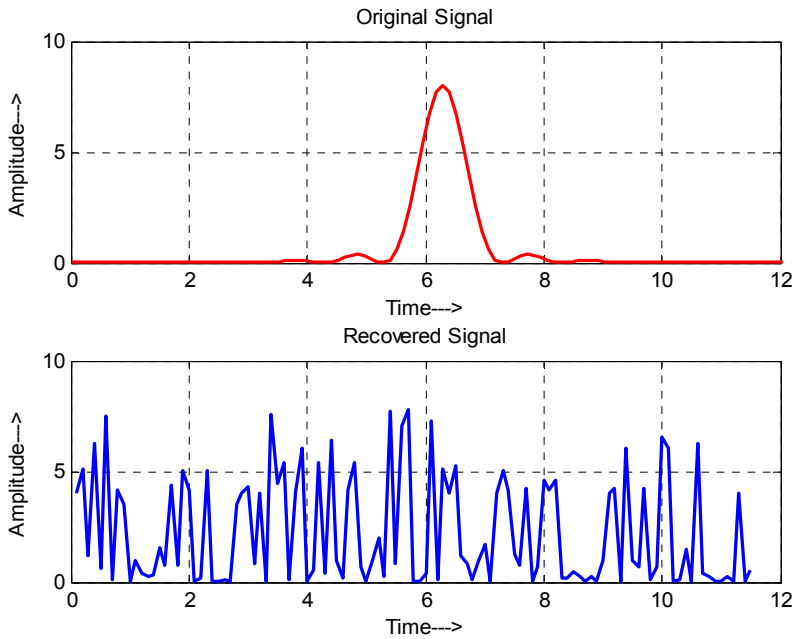

Fig.10. Encryption and recovery using hybrid AO feedback with profiled incident beam
when Q=20, Λ=1e-4 , $\tilde{\boldsymbol{\beta}}$ (TX)=3.6, $\tilde{\boldsymbol{\beta}}$ (RX)=3.61, TD(TX)= 0.05 μs, TD(RX)= 0.05 μs, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$(TX)= 2, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$ (RX)= 2.

5. Conclusion

Recently, the propagation of a profiled optical beam through an open-loop acousto-optic Bragg cell was examined using a transfer function formalism based on the angular spectra. The results have shown dependence on the effective "Q", the acoustic wavelength and the profile width. Oddly, under large Q (greater than 50) conditions, the output profile begins to deviate from the uniform beam response. The device is also studied under closed-loop via intensity feedback, and shown to exhibit more extended chaotic band responses, thereby potentially increasing the dynamic range and parameter sensitivities of the device and any applied signals. The closed-loop is simulated via storing the (open-loop) output scattered amplitudes and thereafter numerically executing the time-dynamical quadratic map equation. In this paper, we apply simple low- to mid-RF signals including periodic waveforms, low BW audio, and PCM signals through the acoustic path which then propagate through the Bragg cell, effectively modulating/encrypting the chaotic output emanating from the device when operated within the chaotic regime. The encrypted signals are transmitted, and thereafter received and demodulated using a heterodyne strategy. The resulting encryption and recovery at the receiver are examined especially from the perspective of overall accuracy and robustness of the system. 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. Because of the profiled input beams, the chaos is a function of not only the feedback parameters (gain, time delay, and peak phase shift), but also the Q parameters that characterizes the A-O cell. This analysis indicates that realistic A-O Bragg cells, which must involve profiled beams, create stronger encryption than analyses assuming non-uniform input beams would suggest. This is because Q must be known for the decryption if profiled beams are used, acting as a fourth element of the encryption/decryption keys. Together, these four parameters and their precise tolerances form a robust system because simultaneously guessing all of them is statistically unlikely.

REFERENCES

1. A. Korpel, "Acousto-Optics," 2nd edition, Marcel Dekker, New York, (1997).

2. 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. on Education, 39, issue 1, 56-68 (1996).

3. J. Chrostowski and C. Delisle, "Bistable piezoelecβc 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, 55002-1 – 055002-14 (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.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).

10. 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).