4-2012

Information Encryption and Retrieval in Mid-RF Range using Acousto-optic Chaos

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

Abhinay Kundur
University of Dayton

Information encryption and retrieval in mid-RF range using acousto-optic chaos

Monish R. Chatterjee[1*] and Abhinay Kundur[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, low-frequency AC signal encryption, decryption and retrieval using system-parameter based *keys* at the receiver stage of an acousto-optic (A-O) Bragg cell under first-order feedback have been demonstrated [1,2]. The corresponding nonlinear dynamics have also been investigated using the Lyapunov exponent and the so-called bifurcation maps [3]. The results were essentially restricted to A-O chaos around 10 KHz, and (baseband) signal bandwidths in the 1-4 KHz range. The results have generally been satisfactory, and parameter tolerances (prior to severe signal distortion at the output) in the ±5% - ±10% range have been obtained. Periodic AC waveforms, and a short audio clip have been examined in this series of investigations. Obviously, a main drawback in the above series of simulations has been the low and impractical signal bandwidths used. The effort to increase the bandwidth involves designing a feedback system with much higher chaos frequency that would then be amenable to higher BW information. In this paper, we re-visit the problem for the case where the feedback delay time is reduced considerably, and the system parameters in the transmitter adjusted in order to drive the system with a DC driver bias into chaos. Reducing the feedback time delay to less than 1 μs, an average chaos frequency of about 10 MHz was achieved after a few trials. For the AC application, a chaos region was chosen that would allow a large enough dynamic range for the width of the available passband. Based on these dynamic choices, periodic AC signals with 1 MHz (fundamental) bandwidth were used for the RF bias driver (along with a DC bias). A triangular wave and a rectangular pulse train were chosen as examples. Results for these cases are presented here, along with comments on the system performance, and the possibility of including (static) images for signal encryption. Overall, the results are encouraging, and affirm the possibility of using A-O chaos for securely transmitting and retrieving information in the mid-RF range (a few 10s of MHz).

Keywords: Acousto-optics, chaos, feedback, encryption, nonlinear dynamics, passbands, RF signals, LP filters, image transmission, parameter tolerance.

1. INTRODUCTION AND BACKGROUND

It is well known that the bistability, hysteresis and chaotic characteristics of an A-O hybrid feedback device in the first-order feedback regime depend strongly on the feedback gain ($\tilde{\beta}$), the feedback time delay (TD), the amplitude (I_{inc}) of the incident light, the initial value of the intensity ($I_1(0)$) and the effective bias voltage ($\hat{\alpha}_0$). Using the chaotic properties of the hybrid acousto-optic feedback device (HAOF), Chatterjee and Al-Saedi recently reported that it is possible to *encrypt* relatively low-bandwidth signals (in the few KHz range) within the chaos wave, and subsequently transmit, receive, heterodyne, filter and recover the message signal from this chaotically encrypted carrier [1,2]. It has been shown that secure information communication for a few simple test signals applied through the acoustic bias input is possible with the HAOF device with reasonably narrow parameter (or decryption key) tolerances.

Mobile Multimedia/Image Processing, Security, and Applications 2012, edited by
Sos S. Agaian, Sabah A. Jassim, Eliza Yingzi Du, Proc. of SPIE Vol. 8406, 840608
 · doi: 10.1117/12.919982

The main drawback of the previous work, even if shown to satisfy the requirements for encryption and retrieval, has been the low bandwidth of operation. To make the information bandwidth more realistic, in this paper we present results from HAOF simulations with feedback delays in the μs to sub-μs range. The operational (DC) parameters are chosen such that the resulting dynamical behavior in the chaotic regime exists over a relatively wide passband. The choice of the passband and parameters then enables determination of the corresponding (AC) signal amplitude and frequency. Our aim in this paper is to realize chaos at frequencies approaching 10s of MHz, so that signals with practical bandwidths, including those for video signals, might be encrypted and transmitted. The resulting design and simulation results are presented in section 2. System parameter tolerances are investigated and reported in section 3.

2. CHAOS IN THE MID-RF FREQUENCY RANGE

2.1 Realizing chaotic oscillations at 10 MHz or higher

The initial task at this stage was to simulate and realize chaos in the HAOF system in the MHz frequency range. The main bottleneck in the previous attempts at obtaining chaos in the RF range was that for feedback delays in the μs or lower range, the corresponding computation time tended to become quite large. In the current work, it was decided to attempt running chaos simulations for sub- μs delays by using a reasonably fast laptop or tablet PC. The machine used had a 4 MHz RAM, and yielded results in a relatively short amount of time (typically several minutes). Fig.1 shows the HAOF schematic at the transmitter. An A-O optic cell operating in the Bragg regime has the first-order light detected by a photodetector (note that this process yields an output current related to the intensity of the first order light, thereby eliminating (or suppressing) the optical frequency (which is nominally shifted from the incident optical frequency by the RF/ultrasonic frequency). The detected current is then amplified (gain $\tilde{\beta}$) and returned to the bias driver input of the RF source. The effective detection and return time delay per pass is TD seconds.

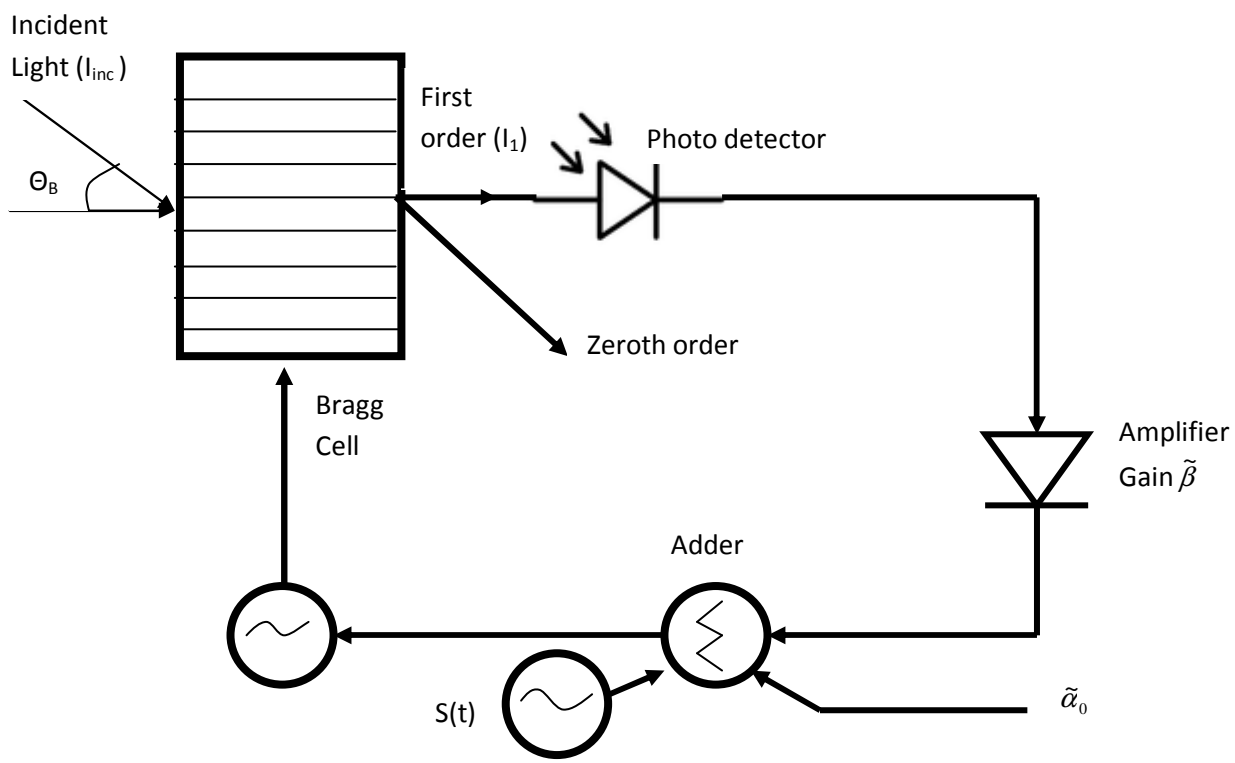
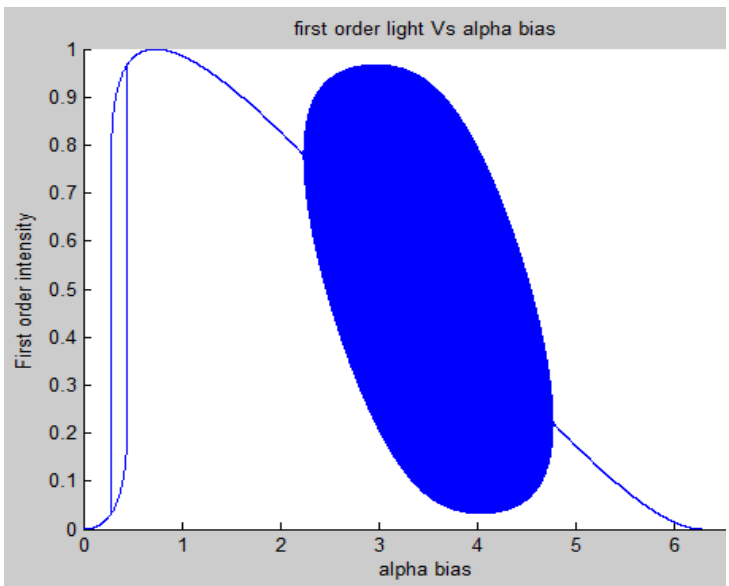


Fig.1. Schematic diagram of A-O Bragg cell with first-order feedback and bias inputs.

We note that the bias input in this system consists of three signals- (i) a DC bias signal that establishes the operating point for the chaotic wave; (ii) a feedback signal derived from the photodetected, amplified and delayed first-order scattered optical output; and (iii) an information signal, S(t), applied to the bias input of the RF.



TD=100ns

$\tilde{\beta}$ = 2.41

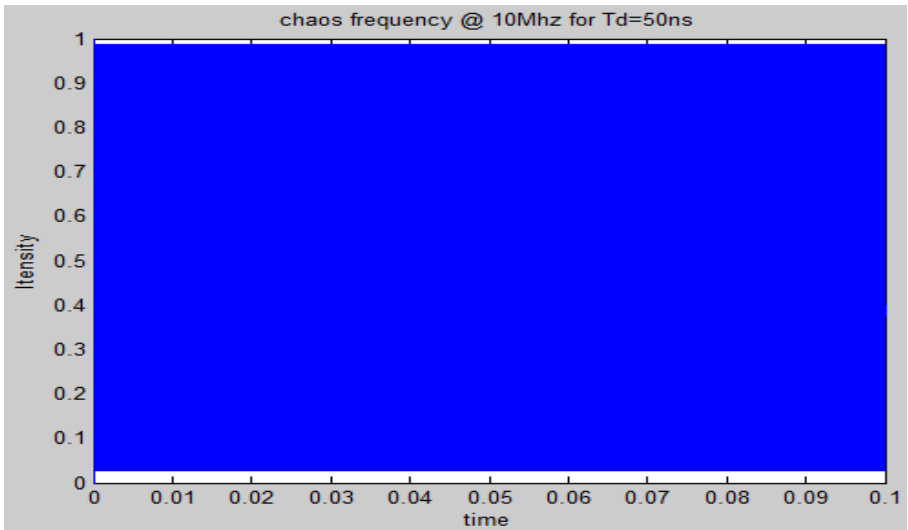
I_{inc}=1

$I_1(0)$=0

Fig.2. First order intensity of HAOF device near the chaotic threshold, showing monostable, bistable and chaotic characteristics.

Fig.2 shows a typical photocurrent under feedback for the case of $\tilde{\beta}$ = 2.41, and a time delay of 100 ns. The initial intensity is taken to be 0, and the incident light amplitude is 1. In this case, we observe four regimes of operation relative to $\hat{\alpha}_0$ - (i) monostable in the range 0 to about 0.25; (ii) bistable from 2.5 to about 0.4; monostable again between 0.4 to about 2.5 (in some cases, this regime is multistable), and finally *chaotic* between 2.5-4.7. For signal modulation purposes, our interest will be in the chaotic region ($\hat{\alpha}_0 > 2.5$). The choice of TD = 100 ns ensures that the average chaos frequency will be about 10 MHz.

Shown in Fig.3 is the chaos waveform versus time for the case TD = 50 ns, $\tilde{\beta}$ = 4.0, I_{inc} = 1, $I_1(0)$ = 0, and $\hat{\alpha}_0$ = 2.0. It turns out that this set of values satisfies the condition for chaos with a wide passband. We note that the waveform is uniformly shaded; this is because the horizontal axis (time) does not allow details in the range of 100 ns (the average chaos period). In Fig.4, however, with the horizontal axis scaled to 1.5 μs, we see details of the chaos, with about 15 cycles; hence the *average* chaos period is about 0.1 μs, indicating an average chaos frequency of about 10 MHz. We also note that the chaos amplitude is non-uniform, as has been reported in earlier work [2].



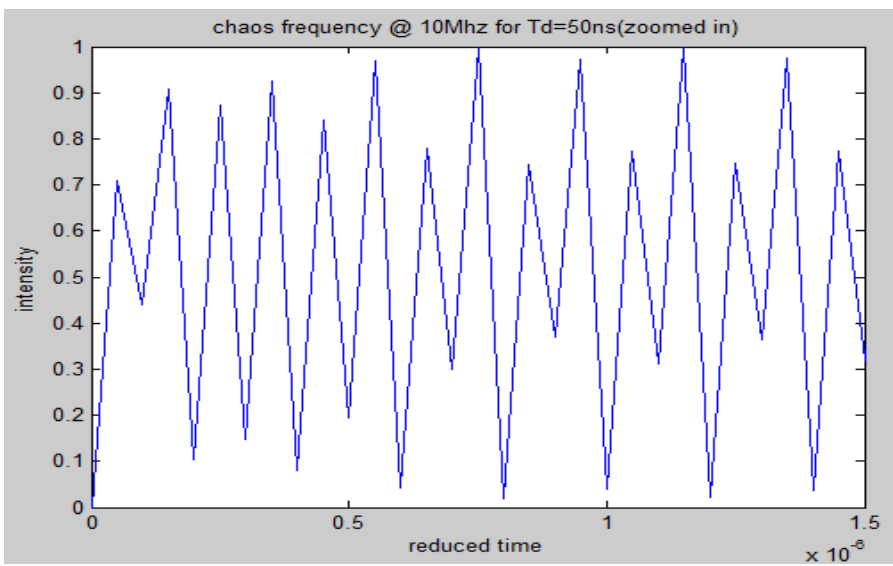
$\tilde{\beta} = 4$

$\hat{\alpha}_0 = 2$

$I_{inc} = 1$

$I_1(0)=0$

Fig.3. Chaos frequency of 10MHz @time delay=50ns



$\tilde{\beta} = 4$

$\hat{\alpha}_0 = 2$

$I_{inc} = 1$

$I_1(0) = 0$

Fig.4. Zoomed graph of chaotic oscillations showing non-uniform cycles.

In Fig.5, we show a plot of the average chaos frequency, obtained by averaging over the simulation plots, versus the quantity 1/2TD. The calculated frequency is compared with the 45° line, and the results are found to coincide almost identically, indicating thereby that the chaos frequency in a given chaotic regime is about 1/2TD, which is half the value that was estimated previously. This has been verified elsewhere in the literature [4].

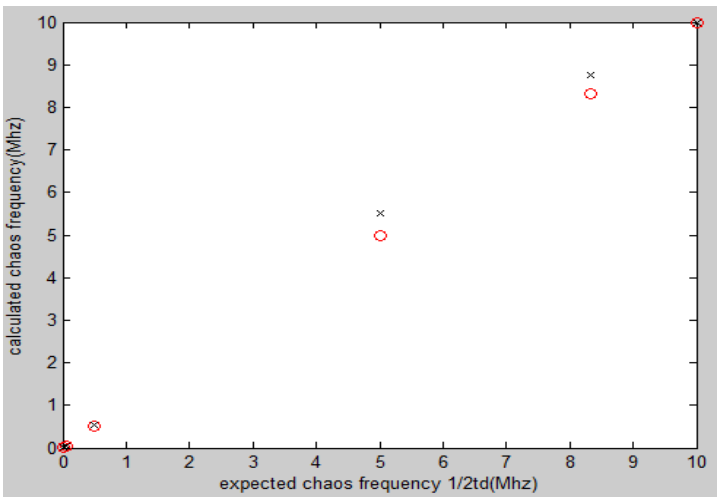


Fig.5. Plot of average chaos frequency versus 1/2TD.

2.2 RF signal modulation and recovery

In Fig.6, we show a (positive) rectangular pulse train with fundamental frequency 0.5 MHz, and amplitude 0.25 V. This waveform was added to the feedback signal and a DC bias voltage in the summer unit of the RF driver. The closed loop parameters were: TD = 50 ns, $\tilde{\beta}$ = 4.0, I_{inc} = 1, $I_1(0)$ = 0, and $\hat{\alpha}_0$ = 3.5. The waveform modulates the resulting 10 MHz chaos wave, and the modulated chaos waveform is shown in Fig.7. We observe that the waveform has the nature of a modulated AM wave.

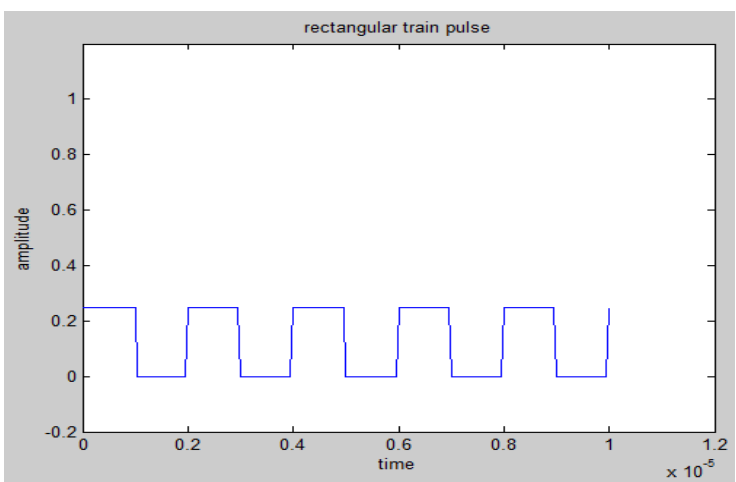


Fig.6. Rectangular pulse train applied to the HAOF chaos modulator.

Previously, attempts were made to tweak parameters until the signal profile disappeared from the waveform envelope. In this instance, however, it was decided that the appearance of the profile did not matter since the signal may only be recovered upon application of the appropriate, *matched* keys at the receiver.

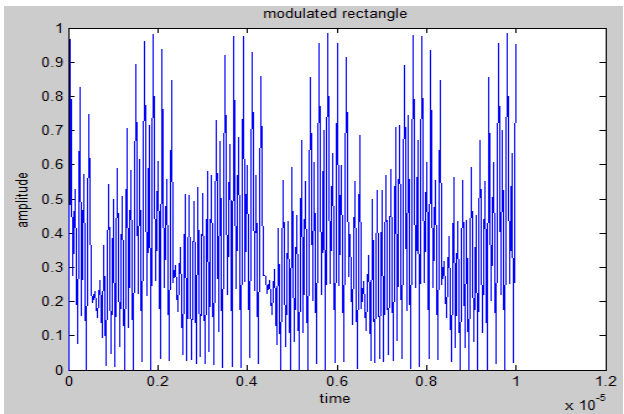


Fig.7. Modulated chaos waveform for a rectangular pulse train.

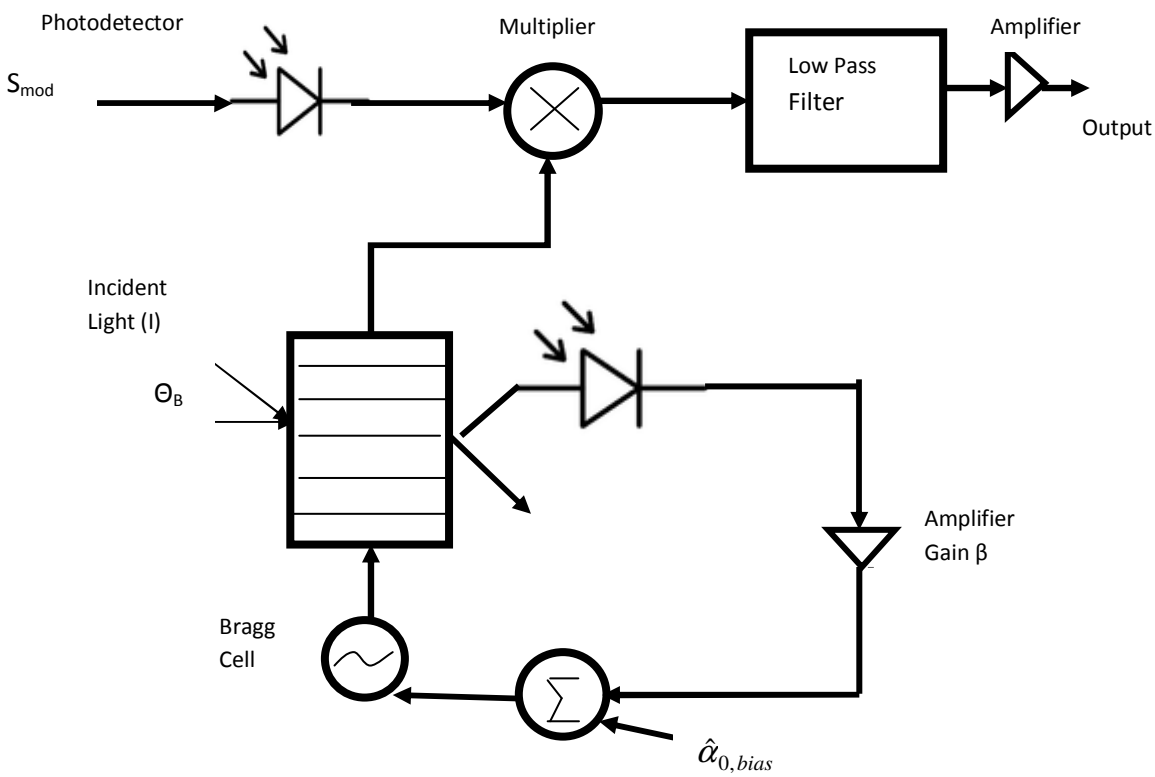


Fig.8. Schematic of the receiver demodulator/decryptor using heterodyne detection.

Shown in Fig.7 is a modulated chaos waveform corresponding to the rectangular pulse train of Fig.6. We observe the periodicity (equivalent to the fundamental signal period) in the waveform envelope, reminiscent of DSB-type modulation, except for a 180^0 phase shift. This would normally be counter-intuitive from the standpoint of signal encryption and security. However, it turns out that proper signal recovery for the above waveform involves having a receiver chaos unit (a *matched* Bragg cell) that matches the *keys* at the transmitter (these are the five parameters, TD, $\tilde{\beta}$, I_{inc}, $I_1(0)$ and $\hat{\alpha}_0$. As such, the signal envelope riding on the chaos wave does not guarantee downloading or demodulation by any unauthorized interceptor. Fig.8 shows a schematic of the receiver system that recovers the encrypted message. The received modulated chaos wave is multiplied by the chaotic output of a *matched* HAOF device. The product is then passed through a low-pass filter, whose output recovers a scaled (and possibly phase-shifted) version of the transmitted message. Typically, an output amplifier restores the recovered amplitude to a level comparable to that transmitted.

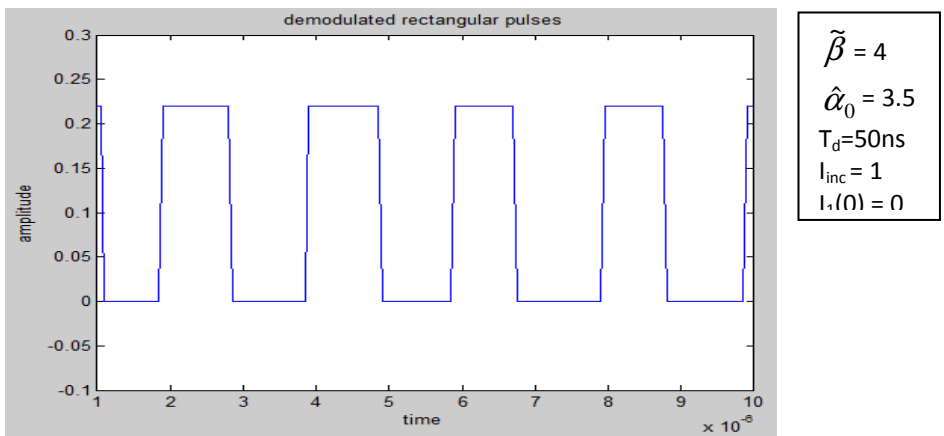


Fig.9. Recovered pulse train upon heterodyne demodulation with matched keys.

Upon application of the receiver heterodyne scheme of Fig.8 using the Matlab simulation, the recovered signal of Fig.9 was obtained. We observe that a rectangular pulse train of period 2 μs has indeed been recovered in this case.

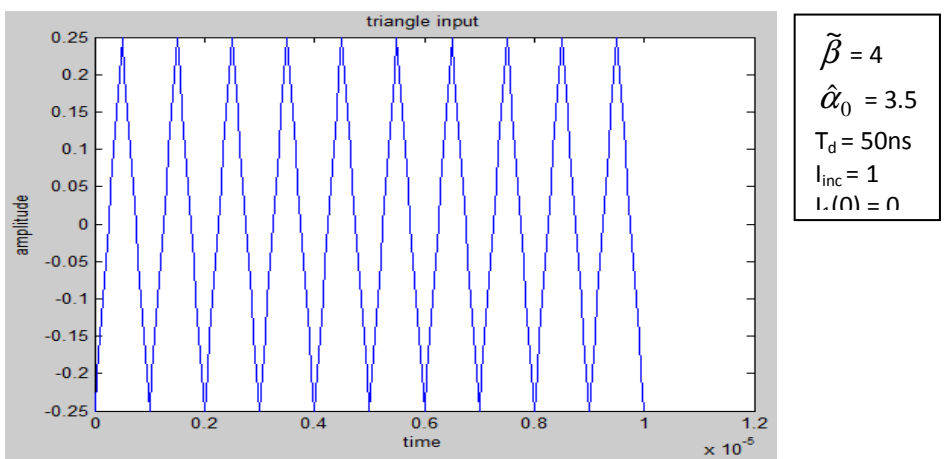


Fig.10. Periodic triangular wave input.

For the case of the periodic triangular input with fundamental period 1 μs, shown in Fig.10, the modulated chaos waveform of Fig.11 was obtained.

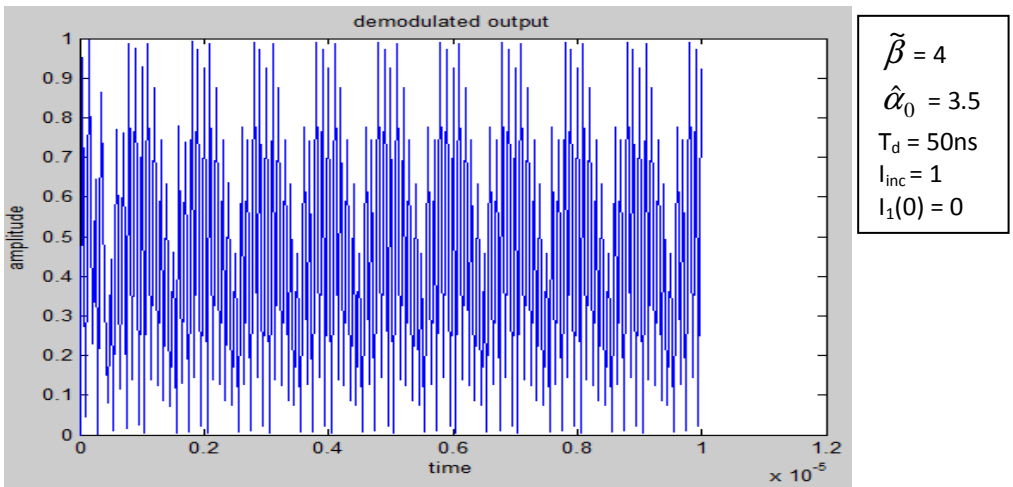


Fig.11. Modulated chaos waveform corresponding to periodic triangular wave.

Finally, the recovered signal output obtained after heterodyne demodulation, is shown in Fig.12. We observe a certain amount of rounding-off of the peaks of the triangle, even though the periodicity is reasonably reproduced. The rounding-off may likely the ascribed to the fact that portions of the AC signal (combined with the DC bias) may fall outside the nominal passband of the chaos, as identified by the Lyapunov exponent or the bifurcation maps [3]. Also, the slight unevenness of the recovered amplitude is attributable to the "self-modulation" of the chaos amplitude.

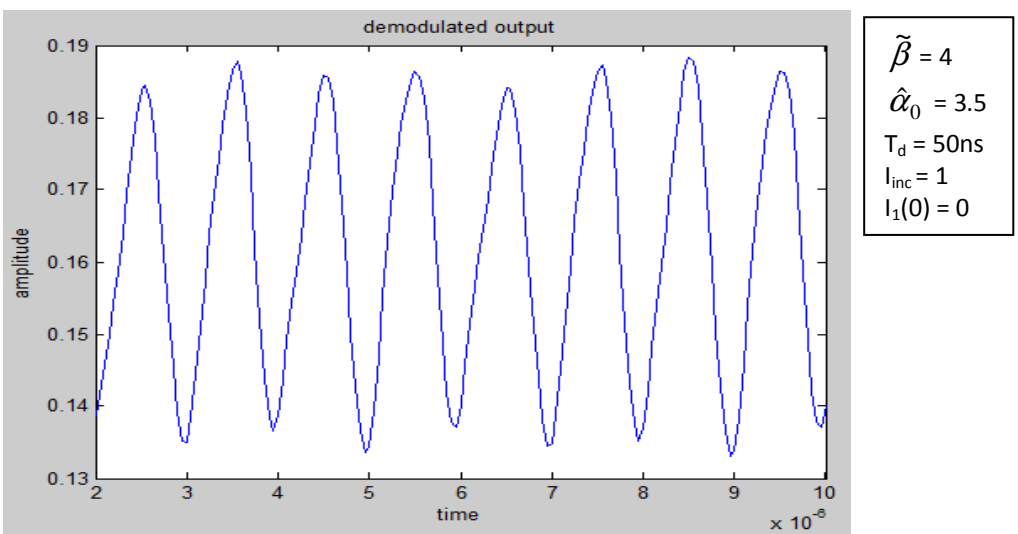


Fig.12. Recovered triangular waveform obtained after heterodyne demodulation.

The plot in Fig.13 shows the Fourier spectrum of the modulated chaos wave obtained by running a fixed length of the time signal over an FFT routine. This may sometimes be useful when trying to read a modulated chaos wave, because the time waveform by itself may not reveal whether any modulation has taken place. From the spectrum, we observe that there are spectral mainlobes at about 10 MHz (corresponding to the average chaos frequency, i.e., the chaotic carrier), and other sidelobes peaking at intervals of 1 MHz, which is the fundamental frequency of the triangular

wave. There is also a large spectral component around DC; this is obviously because of the DC bias voltage applied to the RF bias input. Thus, the chaos spectrum generally agrees with expected DSB modulation results.

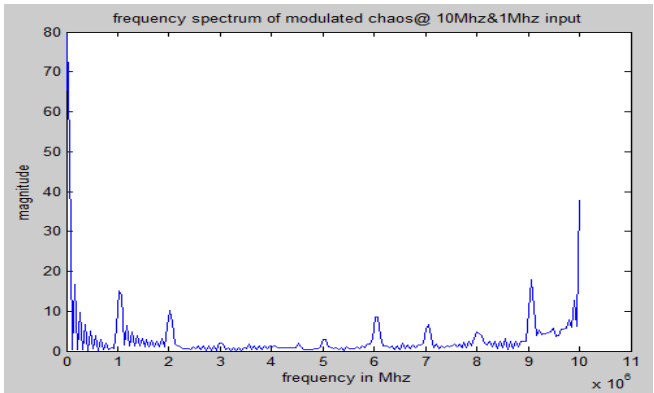


Fig.13. Fourier spectrum of the chaos wave with triangular modulation.

3. PARAMETER TOLERANCE AND ROBUSTNESS OF THE ENCRYPTION SCHEME

In the series of figures that follow, we examine the integrity of signal recovery at the chaotic receiver subject to small deviations or mismatches of three principal *key* parameters, viz., $\Delta\tilde{\beta}$, $\Delta\hat{\alpha}_0$, and ΔT_d. In our earlier work in the low-frequency domain, the parameter tolerances were found to vary in the ±5% - ±10% range. The actual parameter tolerance, or the degree of robustness of the encryption system was likely much more tight, since mismatch of more than one key may occur simultaneously. In the current mid-RF application, we find that severe signal distortion happens when $\tilde{\beta}$ changes from 4.0 to 4.3, i.e., the system exhibits about 7.5% tolerance relative to $\tilde{\beta}$. This is shown in Fig.14.

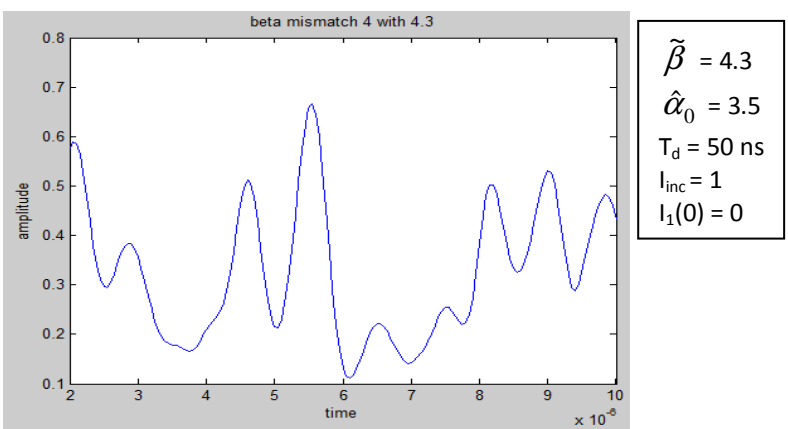


Fig.14. Signal distortion for 7.5% mismatch of $\tilde{\beta}$.

Likewise, when the DC phase shift parameter ($\hat{\alpha}_0$) is changed from 3.5 to 3.6, the output waveform begins to distort noticeably, as shown in Fig.15. Thus, the onset of distortion for the phase shift parameter is around 2.5%.

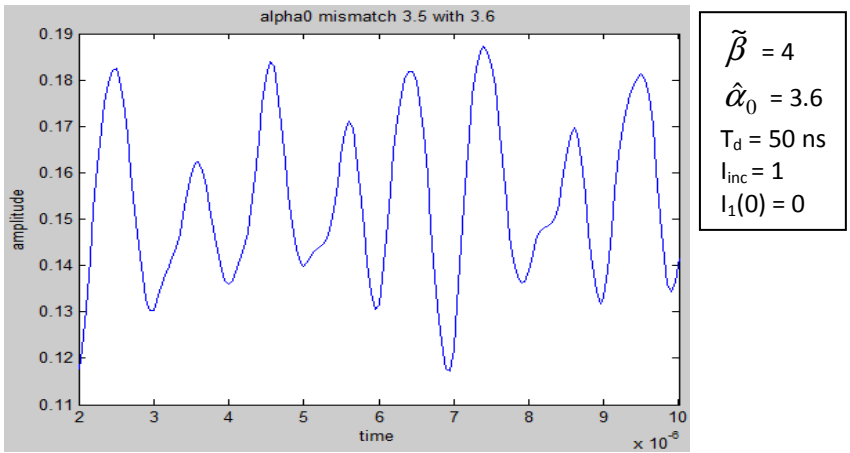


Fig.15. Signal distortion under phase parameter ($\hat{\alpha}_0$) mismatch.

Finally, in Fig.16 we show the signal distortion resulting from mismatch of the feedback time delay, TD. As seen from the figure, a change of TD from 50 ns to 45 ns brings about some primarily amplitude distortions in the output. This would nominally indicate a parameter tunability of 10%, which is higher than that for the other two keys; however, this result in compatible with the results found in the low-bandwidth simulations reported earlier [2].

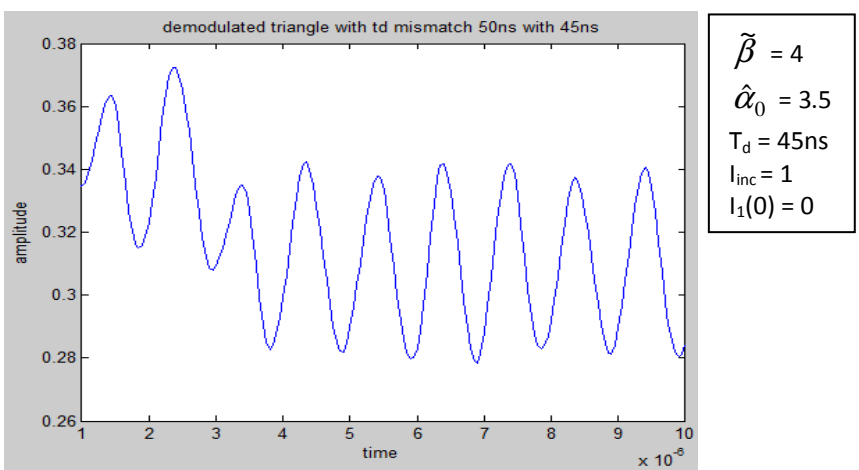


Fig.16. Signal distortion under feedback time delay (TD) mismatch.

4. CONCLUDING REMARKS AND FUTURE WORK

In this paper, information signal encryption, transmission and retrieval in the mid-RF range (1-50 MHz or so) operation of an A-O Bragg cell with feedback have been investigated via Matlab-based simulations. In general, the results are in reasonable agreement with previous, low-frequency work. This is true also of the receiver key parameter tolerance vis-a-vis signal distortion (with distortion occurring for single-parameter variations of ±2.5% - ±10%). In future work, we expect to report results from implementing encryption and transmission of digitized images, where, as

our preliminary work indicates, additional transmitter-end random scrambling of the image pixels may be needed in order to ensure secure transmission.

REFERENCES

1. M.R. Chatterjee, and M. A. Alsaedi, "Examination of chaotic signal encryption and recovery for secure communication using hybrid Acousto-optic feedback," Opt. Eng. 50, 55002-1 – 055002-14 (2011).

2. 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).

3. M.A. Al-Saedi, and M.R. Chatterjee, "Examination of the nonlinear dynamics of a chaotic acousto-optic Bragg modulator with feedback under signal encryption and decryption," Opt. Eng. 51, 018003-1 – 018003-10 (2012).

4. J.-W. Ryu, W.-H. Kye, S.-Y. Lee, M.-W. Kim, M. Choi, S. Rim, Y.-J. Park and C.-M. Kim, "Effects of time-delayed feedback on chaotic oscillators," Phys. Rev. E 70, 036220 (2004).