8-2010

Performance Measures in Acousto-optic Chaotic Signal Encryption System Subject to Parametric Variations and Additive Noise

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

Anjan K. Ghosh
University of Oklahoma

Mohammed A. Al-Saedi
University of Dayton

Performance measures in acousto-optic chaotic signal encryption system subject to parametric variations and additive noise

Monish R. Chatterjee [1], Anjan K. Ghosh [2] & Mohammed A. Al-Saedi [1]

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

[2]Telecom. Engr., School of ECE, University of Oklahoma, Tulsa, OK 74135

ABSTRACT

Signal encryption and recovery using chaotic optical waves has been a subject of active research in the past 10 years. 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 using a low-amplitude sinusoidal signal applied via the bias input of the sound cell driver [1, 2]. Subsequent recovery of the message signal was carried out via a heterodyne strategy employing a locally generated chaotic carrier, with threshold parameters matched to the transmitting Bragg cell. The simulation results, though encouraging, were limited to relatively low chaos frequencies and sinusoidal message signals only. In this paper, we extend the previous work by (i) increasing the chaos frequency using appropriate parameter control; (ii) carefully examining the system sensitivity to three system parameters, viz., feedback delay, feedback gain, and dc bias level; (iii) examine signal recoverability relative to shifts in the three parameters mentioned above relative to the transmitter; and (iv) determining the robustness of such a system relative to the primary transmitter parameters. Additionally, we consider also the effect of the additive bandpass noise (obtained from white Gaussian noise in the simulator) on signal recovery in such a system from a performance standpoint. It is also conjectured that signal recovery can be effected by passing the modulated light through a second sound cell in a matched chaotic regime. This aspect is also under investigation.

Keywords: Acousto-optics, chaos, feedback, modulation, encryption, heterodyne, recovery, nonlinear dynamics

1. INTRODUCTION AND BACKGROUND

In 1979, Ikeda predicted theoretically that bifurcation and chaos may appear in an optically bistable device using a ring cavity[3]. This effect was first observed in a so-called hybrid bistable device by Gibbs *et. al*[4] . Hybrid implies that part of the optical output is detected and delayed by an electronic circuit, or held for a while by a microprocessor and then fed back to the input (driver) signal. During the past 30 years, all optically bistable devices have also been designed to demonstrate optical chaos[5-9]. Since 1979, there has been sustained interest in nonlinear optical devices involving hybrid acousto-optic feedback that exhibit hysteresis, differential gain, and hard limits of optical output versus input power characteristics, as well as chaotic regimes. It is well-known that if the first- (or zeroth-) order light in an acousto-optic device operating in the Bragg domain is detected and amplified, and then fed back into the acoustic driver, the amplitudes of the diffracted fields, i.e., the resulting first- and the zeroth-orders exhibits optical bistability. The feedback makes the system inherently nonlinear and complex in terms of its space-time dynamics[6,7,10]. In ref. [11], optical bistability, possible multistability and chaos may be generated for three fundamental types of tuning effects, i.e., feedback gain, bias voltage and input amplitude. In 2008, early simulation work was undertaken to demonstrate the possibility of encrypting information signals within acousto-optic chaotic waves based on the hybrid device[1]. Subsequently, the idea was extended to examine the process of signal encryption and recovery using the equivalent of a heterodyne technique in which the *chaotic local oscillator* in the receiver is exactly matched parametrically to the chaotic wave in the transmitting Bragg cell prior to signal insertion[2]. In the present work, we study carefully the properties of the system in terms of its robustness. To this end, we first obtain a complete encryption and decryption operation using heterodyne simulation for a simple sinusoidal input. Thereafter, the effects of changes in the receiver

Free-Space Laser Communications X, edited by Arun K. Majumdar, Christopher C. Davis,
Proc. of SPIE Vol. 7814, 78140D · © 2010 SPIE · CCC code: 0277-786X/10/$18 · doi: 10.1117/12.862108

parameters (feedback gain, d.c. bias, and time delay), thereby causing mismatch from the transmitter *keys* are examined for distortions in the recovered signal. The expectation is that even small changes in the receiver *keys* distort the recovered signal beyond recognition. Some of these results are presented here. Finally, the problem of electronic noise incorporated via the system instrumentation is considered. For this purpose, we begin with a white, Gaussian noise model, which is thereafter converted in the simulator to band pass noise (of variable bandwidth), and propagate it through the acoustic input along with the feedback signal and the information signal. The basic strategy is to measure the characteristics of the recovered signal without noise (within a selected noise bandwidth), and thereafter, examine the signal past the output filter when band limited noise is present. The resulting mean-squared signal error is examined vis-à-vis changes in the noise bandwidth, the output low-pass cutoff, and the input SNR.

1.1 Acousto-optic feedback- hybrid devices:

Since 1979, there has been much interest in nonlinear optical devices that exhibit hysteresis, differential gain, and hard limits of optical output versus input power characteristics. Acousto-optic devices with positive feedback gain also exhibit bistability characteristics. In an acousto-optic device, the amplitude of the diffracted fields that the operate in the Bragg regime, .i.e., the first and zero order, which appear at the output of the Bragg cell, are related through a set of coupled differential equations as given by Eqs. (1) and (2)[11] . In a standard experiment, a Bragg cell is driven by an ultrasonic sound wave from an RF generator (typically at 40 MHz), with the laser beam incident at the Bragg angle. The diffracted first order is picked up by a photodetector, amplified and fed back to the RF generator bias input. Fig. 1 shows a schematic of the above. The resulting plot of the first order detected intensity versus the dc bias input ($\hat{\alpha}_0$) indicates bistable behavior for appropriate drive parameters. The width of the hysteresis loop increases with the feedback delay time, and also widens plus shifts to the left with increasing feedback gain. In this paper, we examine the first order diffraction characteristics under feedback *beyond the bistable regime*, by forcing the system to operate strictly in chaos. The diffraction (before feedback) is given by:

$$\frac{dE_1}{d\xi} = -j\frac{\hat{\alpha}_0}{2}E_0, \tag{1}$$

$$\frac{dE_0}{d\xi} = -j\frac{\hat{\alpha}_0}{2}E_1, \tag{2}$$

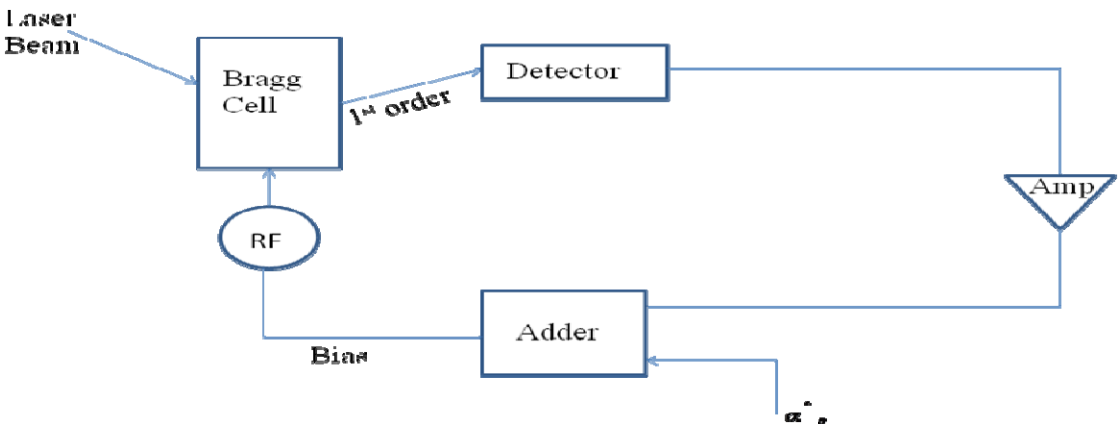

Fig. 1. The acousto-optic modulator with feedback.

where Bragg regime is assumed. In the above, $\hat{\alpha}_0$ is the peak phase delay through the medium (before feedback), and ξ is the normalized propagation distance (= z/L, where L is the effective interaction length).

$$E_1 = -jE_{inc}\sin\left(\frac{\hat{\alpha}_0 \xi}{2}\right), \tag{3}$$

$$E_0 = E_{inc}\cos\left(\frac{\hat{\alpha}_0 \xi}{2}\right), \tag{4}$$

With feedback plus time delay, the corresponding first-order detected intensity follows the nonlinear dynamical equation:

$$I_1(t) = I_{inc}\sin^2\left[\frac{\hat{\alpha}_0(t)}{2} + \frac{\tilde{\beta}}{2} I_1(t - TD)\right], \tag{5}$$

where $\tilde{\beta}$ is the effective feedback gain, I_{inc} is the incident intensity, and TD is the feedback delay time. It is the nonlinear dynamics of Eq.(5) that leads to mono-, bi- and multistable behavior, followed by chaos in its various manifestations[12]. The feasibility of operating 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 a *heterodyne* approach, has been explored with some success recently[1,2].

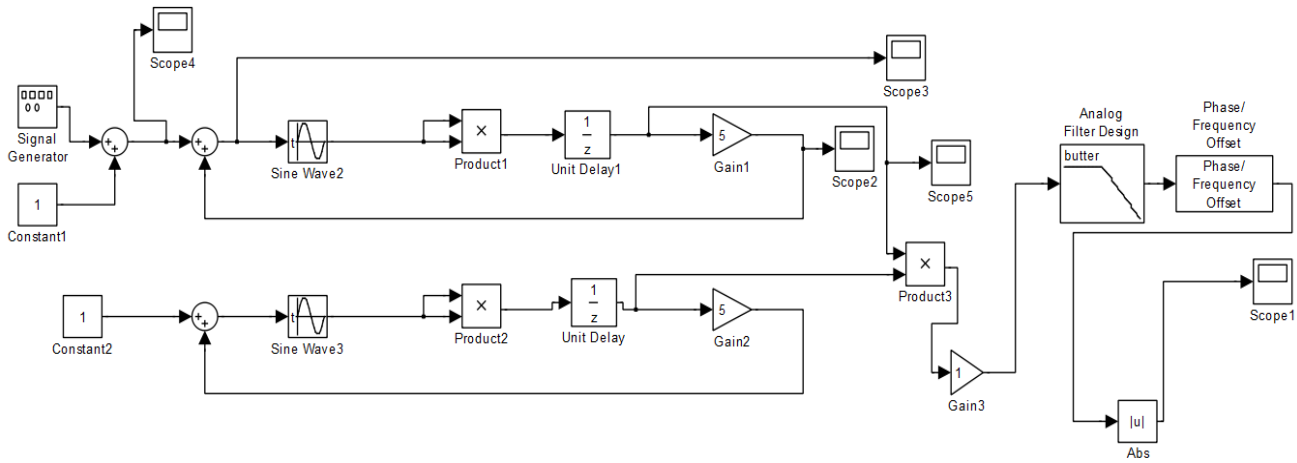

Fig. 2. Heterodyne scheme for encrypting and decrypting the input signal

In earlier work, it was shown that multiple oscillations beyond the bistable regime begin to occur for a time delay fraction of 0.02 and a feedback gain ($\tilde{\beta}$) of 2.41. By increasing the value of $\tilde{\beta}$ tot 4.2, and with normalized TD of 0.0125, the system becomes completely chaotic. The parameter thresholds corresponding to the onset of chaos (i.e., threshold values of $\hat{\alpha}_0$, $\tilde{\beta}$ and TD) are taken into consideration in order to examine the message encryption and recovery properties of the system. The proposed *heterodyne* encryption and recovery scheme is shown in Fig. 2. In this scheme, on the transmitter side, by setting up the system on Bragg regime and the input (message) signal used as a third component of the summer at the RF bias point (along with $\hat{\alpha}_0$ and the feedback) for the Bragg cell driver, and by choosing high enough value of $\tilde{\beta}$ (greater than the threshold value of 2.41) to ensure total chaos, the signal is encrypted. Note that $\hat{\alpha}_0$ in this setup serves as the appropriate dc level shift for the total $\hat{\alpha}_{tot}$ to remain above the necessary chaotic threshold when a signal (with negative excursions) is imposed. Further, we note that since the information is carried by the chaos wave, we need the (average) chaos frequency (f_{ch}) to be substantially higher than the frequency of the baseband message. To achieve a high average chaos frequency (shown in section 2), we simply reduce the time delay in the feedback loop. In our simulations, the highest average chaos frequency achieved was 100 KHz, even though in principle, it may be made arbitrarily higher. On the receiver end, a locally generated chaos (from a matched Bragg cell with system parameters identical to those of the transmitter) is used to multiply the incoming (encrypted) signal from the transmitter (following photodetection), and the resulting product is then fed to a low pass filter with a cutoff frequency in the neighborhood of the highest signal frequency. The output signal of the filter suffers a 180-degree phase shift; this justifies the use of a phase shifter to properly retrieve the signal at the receiver.

2. SIMULATION RESULTS

2.1 Onset of bistability in hybrid devices

At lower values of $\tilde{\beta}$ (less than 2.41) and time delay at 5.24 milliseconds, by plotting $\hat{\alpha}_0$ versus the intensity I_1, the hysteresis loop shown in Fig. 3(a) is obtained. When the value of $\tilde{\beta}$ is increased to a value near 2.41, we see from Fig. 3(b) that the system enters well-defined chaotic oscillations.

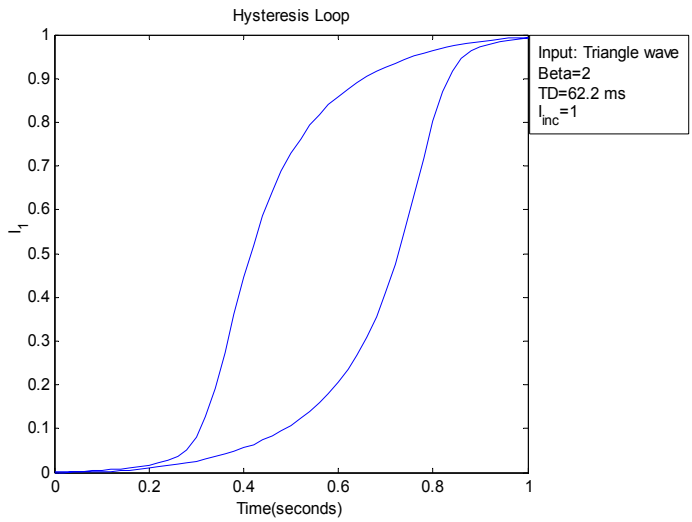

Fig. 3(a). Plot of bistable characteristics.

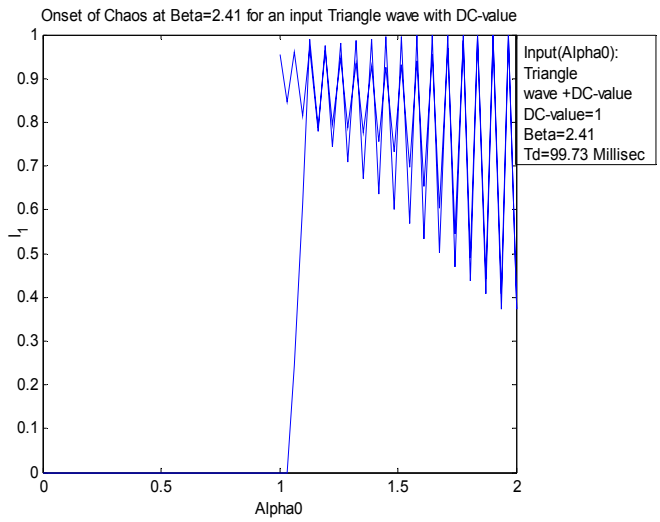

Fig. 3(b). Onset of chaos at $\tilde{\beta} = 2.41$.

2.2. Onset of chaos

Upon increasing $\tilde{\beta}$ to 3.0, and decreasing the time delay to 0.0001s, a chaotic signal appears with an (average) frequency of 10.714 KHz as shown in the time versus intensity plot of Fig. 4(a). Fig. 4(b) shows the corresponding chaos waveform for $\tilde{\beta}$ = 3.0, $\hat{\alpha}_0$ = 2.0and TD = 0.00001s respectively. The (average) chaos frequency for the latter case is about 102.912 KHz.

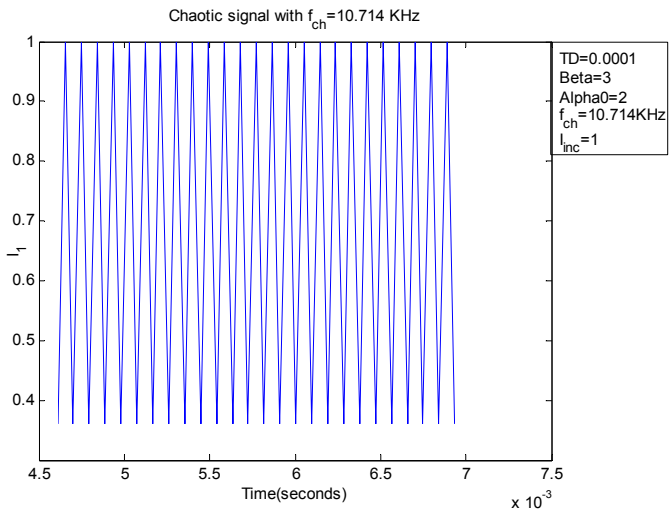

Fig. 4(a). Chaotic signal at frequency = 10.714 KHz**.**

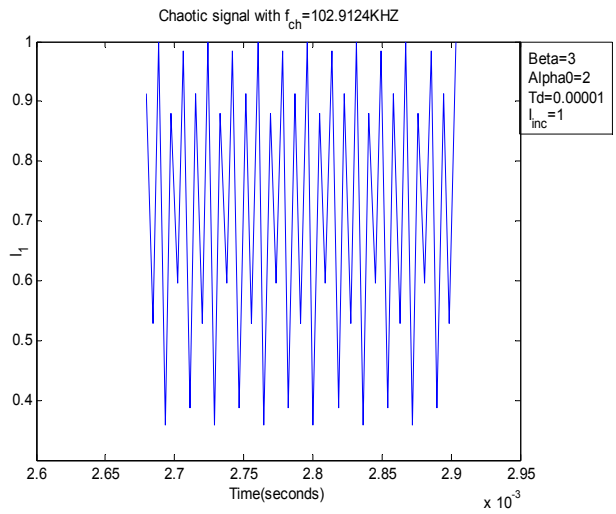

Fig. 4(b). Chaotic signal at frequency = 102.912 KHz.

The envelope of the chaotic signal is not constant as can be seen from Fig. 4(b). The total chaotic signal for a long period of time is shown in Fig. 5 for the av. chaos frequency of 10.714 KHz. Note that due to the time scale on the graph, the chaos envelope *appears* to be uniform.

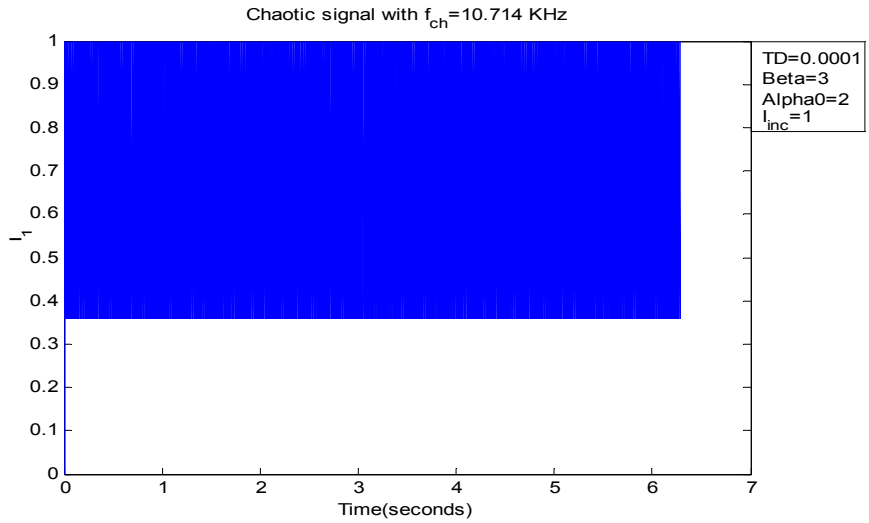

Fig. 5. Chaotic signal at av. frequency 10.714 KHz for a period of 6.28 seconds.

2.3. Effect of system parameters on chaos

The effects of time delay, $\hat{\alpha}_0$ and $\tilde{\beta}$ on the chaos frequency and amplitude are studied in this section.

2.3.1 Effect of time delay (TD)

To study the effect of time delay TD on chaos, the other system parameters ($\hat{\alpha}_0$ and $\tilde{\beta}$) were fixed at $\hat{\alpha}_0$ =2, and $\tilde{\beta}$ = 3. The time delay was varied and the chaos frequency was calculated using the zero crossing method for the average line. Also, the average amplitude is calculated by taking the difference between the maximum and minimum amplitudes and dividing by 2. The time delay is plotted versus the av. chaos frequency as shown in Fig. 6. It can be seen that upon decreasing the time delay, the av. chaos frequency increases. However, it is found that the average amplitude for different time delays (based on the max and min differential) is constant and the average value is 0.68.

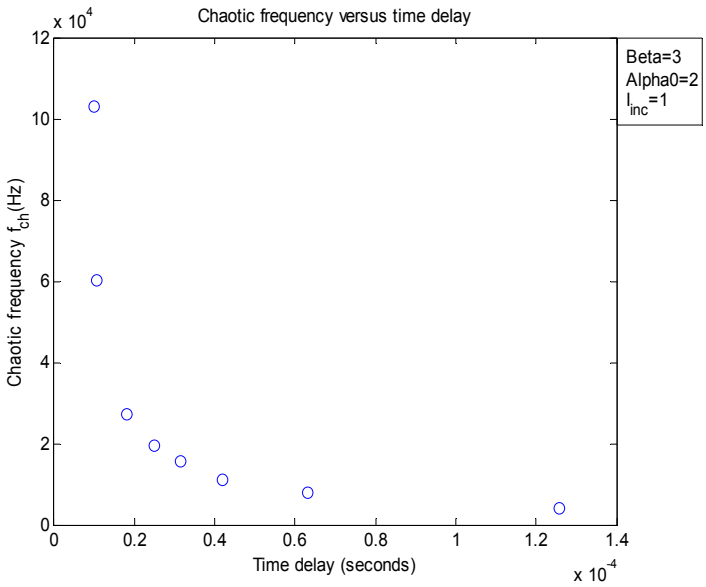

Fig. 6. Dependence of chaos frequency on time delay.

2.3.2 Effect of feedback gain ($\tilde{\beta}$)

To study the effect of feedback gain $\tilde{\beta}$ on chaos, the other system parameters ($\hat{\alpha}_0$ and TD) were fixed at $\hat{\alpha}_0$ =2, and TD = 0.1 ms. As seen in Fig. 7, the chaos frequency does not change with $\tilde{\beta}$. However, $\tilde{\beta}$ does impact the chaos amplitude, which approximately increases linearly, as shown in Fig. 8.

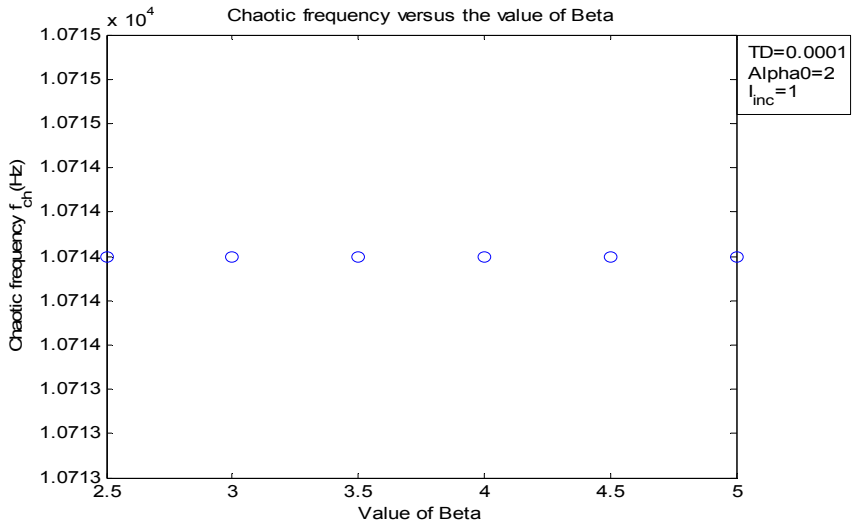

Fig. 7. Dependence of chaos frequency on $\tilde{\beta}$.

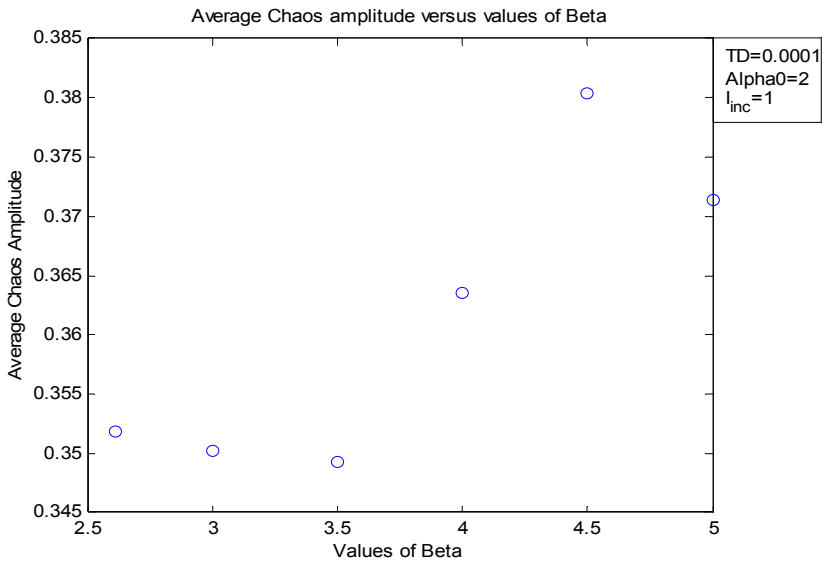

Fig. 8. Dependence of chaos amplitude on $\tilde{\beta}$.

2.3.3 Effect of increasing the bias ($\hat{\alpha}_0$)

The system parameters to study the effect of increasing the bias $\hat{\alpha}_0$ are studied using the value of 3 for the feedback gain and a value of 0.1 ms for the time delay. As seen in Fig. 9, $\hat{\alpha}_0$ 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. 10.

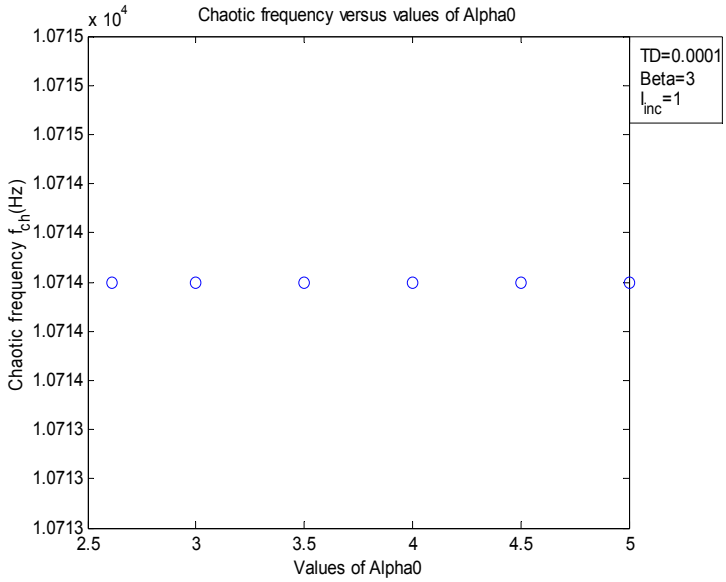

Fig. 9. Dependence of chaos frequency on $\hat{\alpha}_0$.

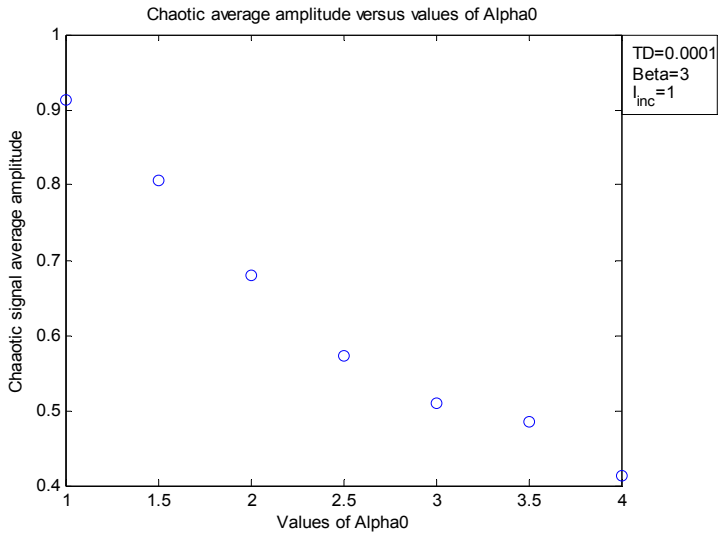

Fig. 10. Dependence of chaos amplitude on $\hat{\alpha}_0$.

3. SYSTEM ROBUSTNESS

The scheme in Fig.2 is used to encrypt and decrypt/recover message signals via simulation. Fig. 11(a) and (b) are examples of encrypting two signals, one sinusoidal and the other triangular. Both signals were encrypted at a chaos frequency of 10.714 KHz for same time delay with different feedback gains ($\tilde{\beta}$) of 4 and 3.5, respectively. When the parameters are matched between the transmitter and the receiver, the corresponding original and recovered signals (after appropriate low pass filtering) are shown in Fig. 12(a) and (b). Both chaos frequencies were at 10.714 KHz. However, to verify the system robustness, mismatching one of the parameters between transmitter and receiver was carried out in a

series of simulation experiments. Examples of the resulting impact on the quality of the recovered signal are presented below.

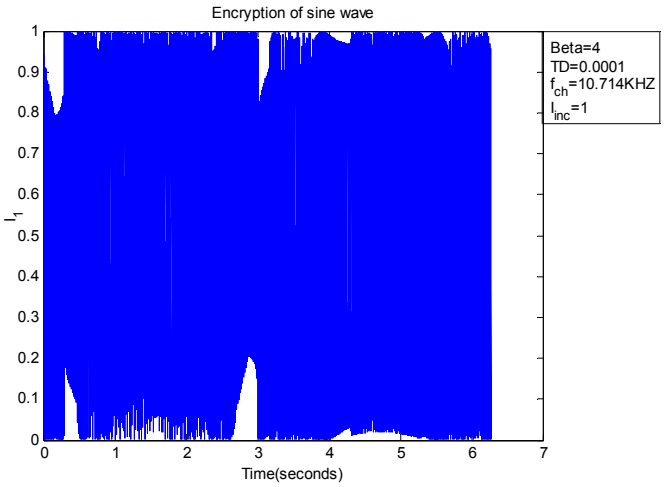

Fig. 11(a). Encryption of sine wave.

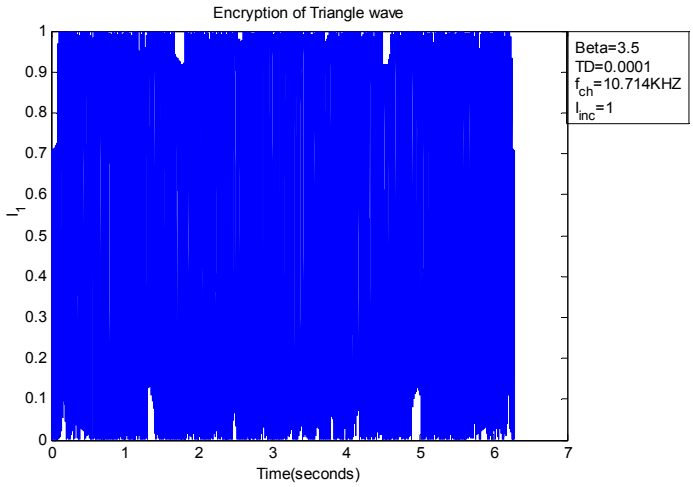

Fig. 11(b). Encryption of triangular wave.

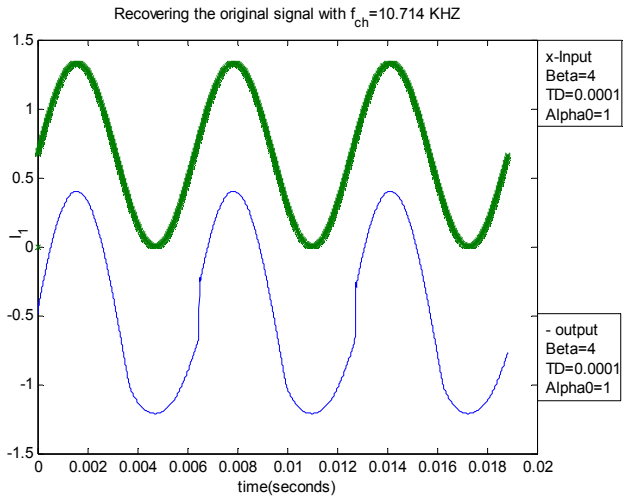

Fig. 12(a). Original and recovered sine wave.

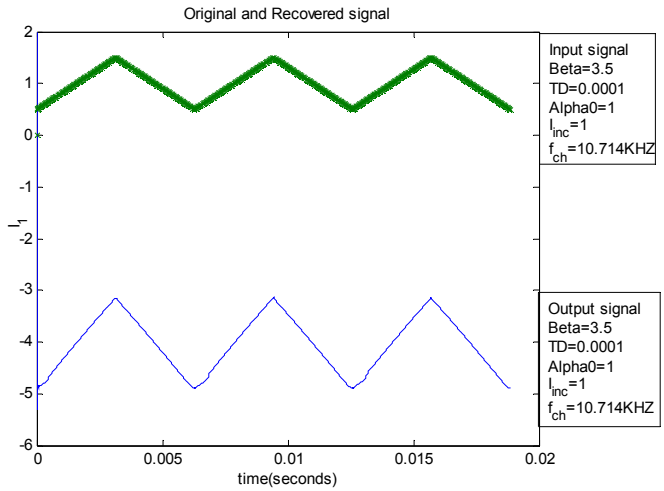

Fig. 12(b). Original and recovered triangular wave.

3.1 Beta mismatch

As shown in Fig. 13(a), when the $\tilde{\beta}$ in the receiver is changed from 4.0 to 4.1, the recovered signal is significantly distorted. We see similar distortion upon recovery for the triangular case with a mismatched $\tilde{\beta}$ of 3.6, as shown in Fig. 13(b).

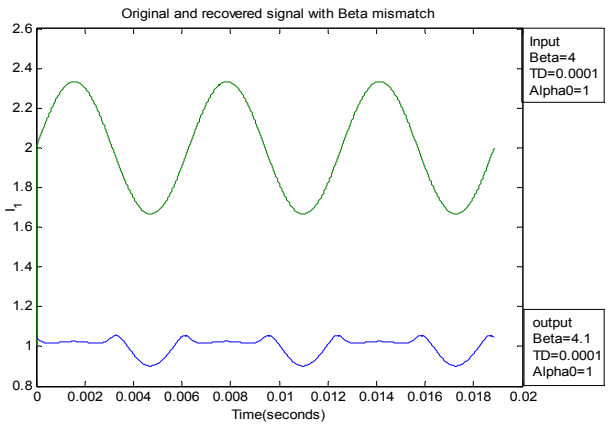

Fig. 13(a). Recovered sine wave with beta mismatch.

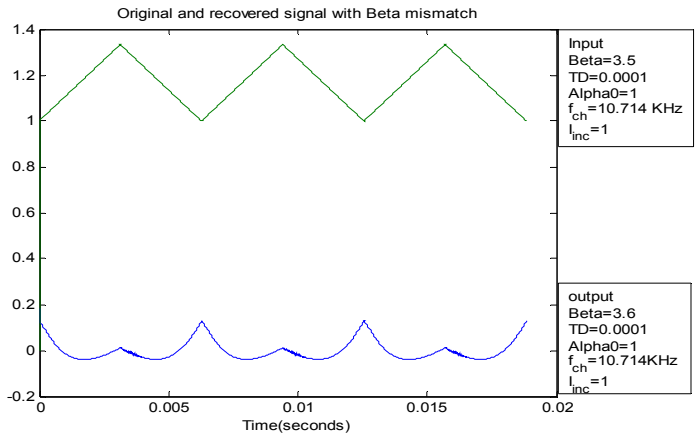

Fig**.13(b).** Recovered triangular wave with beta mismatch.

3.2 Time delay mismatch

Here, the time delay (TD) between transmitter and receiver is varied. The delay at the transmitter side was 0.1 ms, while at the receiver side it was 0.115 ms for both sinusoidal and triangular waves. However, the other parameters ($\hat{\alpha}_0$ and $\tilde{\beta}$) were kept the same in the transmitter and the receiver side. Fig. 14(a) and (b) show the results for the recovered signals for both sinusoidal and triangular waves.

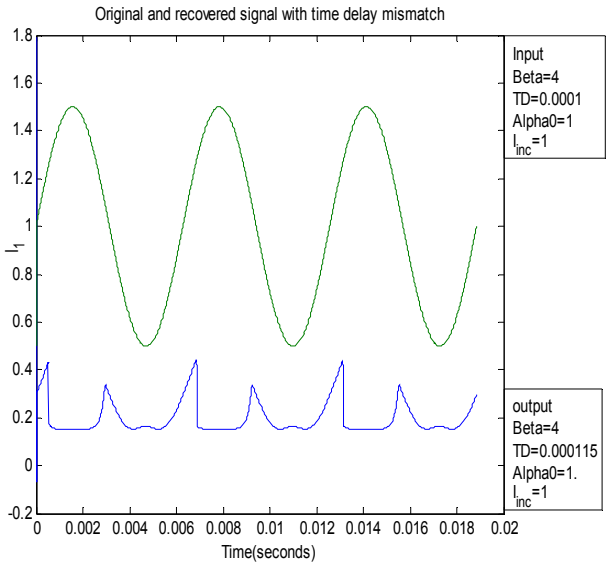

Fig.14(a). Recovered sine wave with TD mismatch.

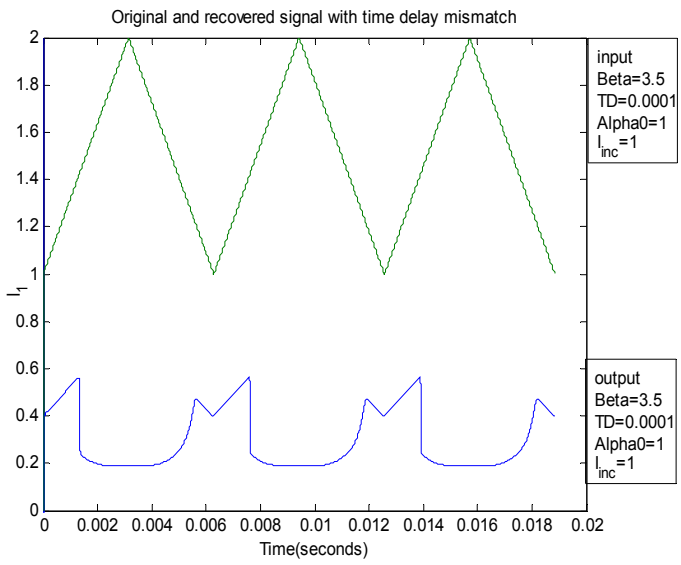

Fig. 14(b). Recovered triangle wave with TD mismatch.

3.3 DC bias mismatch

Here, the parameters $\tilde{\beta}$ and TD are kept the same in the transmitter and receiver, while $\hat{\alpha}_0$ is mismatched (1 and 1.17), with a chaos frequency of 10.714 KHz. The resulting signal distortion is shown in Fig. 15(a) and (b).

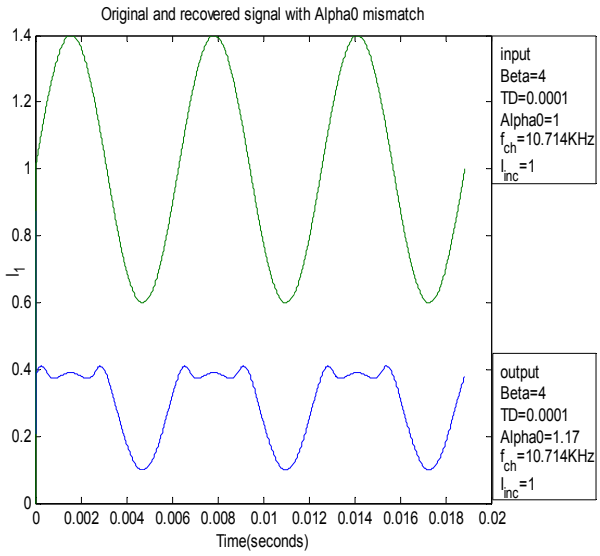

Fig. 15(a). Recovered sine wave with $\hat{\alpha}_0$ mismatch.

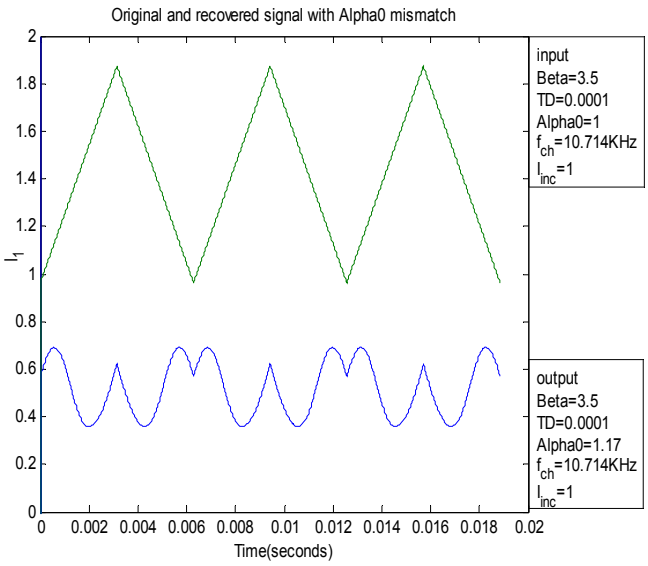

Fig. 15(b). Recovered triangle wave with $\hat{\alpha}_0$ mismatch.

4. EFFECT OF ELECTRONIC AND INSTRUMENTAL NOISE ON SYSTEM PERFORMANCE

In this section, we examine the effect of (band pass) electronic/instrumental noise on the propagation of the encrypted message and its final recovery. To achieve a band pass noise process, we begin with a standard, white Gaussian noise process which is then suitably filtered. The cutoff frequency of the filter is set up at the 1 KHz signal frequency or higher. This limits the input noise bandwidth to about 1 KHz. At the receiver end, we have a low pass filter (LPF) whose cutoff is typically set at approximately the signal frequency, in order to eliminate content at the chaos frequency or its harmonics. In all cases, the chaos frequency is much higher than the cutoff frequency of the noise filter or the signal frequency. However, when we increase the noise bandwidth above the signal frequency, we need to correspondingly reset the receiver LPF cutoff in the neighborhood of the noise bandwidth in order to be able to study the effect of the noise during transmission and recovery.

4.1 Encryption and decryption of signal in presence of band pass noise

In the following example, a band pass noise, obtained via passage of a white Gaussian noise through a LPF with cutoff frequency 1.5KHz, was added to a triangular wave, and fed to the Bragg cell driver bias input. The noise amplitude (or, equivalently, noise powe)r, is kept considerably lower than the signal amplitude. Also, the (matched)

parameters between transmitter and receiver are chosen to be: $\hat{\alpha}_0 = 2.0$, $\tilde{\beta} = 3.5$, and TD = 0.0001 s. The cutoff frequency at the receiver side is 1.5 KHz. In Fig. 16, we show the noisy input and recovered signals for this case.

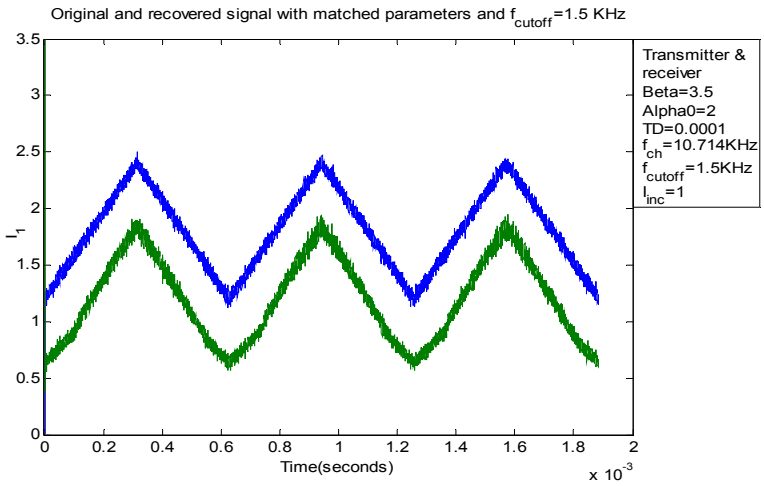

Fig.16. The input signal with additive white Gaussian noise and the recovered signal.

4.2 Comparison of mean-squared error for noise-free output and noisy outputs

For the problem with band pass noise, we evaluate the effect of the noise propagated through the chaotic system through a measure of the mean-squared error (MSE) between the noise-free output and the noisy output. The mean-squared error is defined simply as the square of the difference between the noise-free and the noisy outputs for the same output LPF, time-averaged over a cycle. The MSE of the proposed scheme is computed for different chosen values of the noise bandwidth for comparison purposes. The chosen noise bandwidth is used to select the cutoff of the output LPF (kept at the signal or noise bandwidth, whichever is higher)

4.3 Calculating the MSE of recovered signals with fixed cutoff frequency of LPF at the receiver end

In this case, the generated additive white Gaussian noise was passed through a low pass filter with variable cutoff frequency. The cutoff frequency varies from 100 Hz till 1.5 KHz.

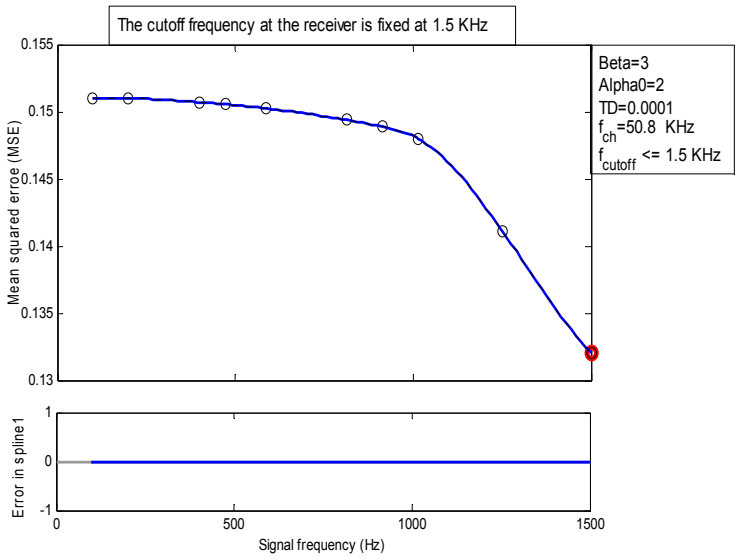

Fig.17. MSE versus input noise bandwidth with fixed output LPF cutoff.

The cutoff frequency of the low pass filter at the receiver is kept fixed at 1.5 KHz. (which is the signal frequency).

Fig. 17 shows that the MSE decreases with increasing the input noise bandwidth.

4.4 Effect of noise bandwidth higher than that of signal with adjusted out LPF cutoff

The cutoff frequency of the low pass filter for the white Gaussian noise was varied at the transmitter in the range 1.5 KHz up to 20 KHz, and the output LPF cutoff was adjusted to match the noise BW (kept lower than the chaos frequency). The parameters like $\hat{\alpha}_0$, $\widetilde{\beta}$ and TD were kept fixed and the average chaos frequency was selected to be 50.8 KHz.

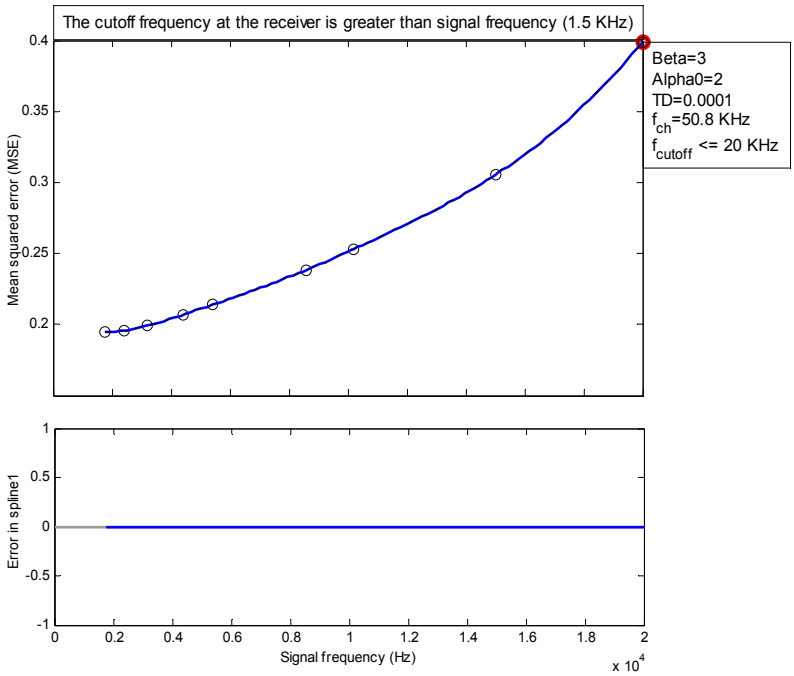

Fig.18. MSE versus noise bandwidth exceeding signal bandwidth.

The chaos frequency is chosen to be higher than the LPF cutoff frequency to avoid detecting the chaos. The simulation results show that MSE increases when the noise bandwidth increases.. This is shown in Fig. 18.

5. CONCLUDING REMARKS

A new heterodyning scheme for encrypting and decrypting/recovering message signals is proposed using acousto-optic Bragg diffraction in the chaotic regime. Appropriate values of the parameters $\hat{\alpha}_0$, $\tilde{\beta}$ or TD or a combination of the same may lead to chaos which is then encrypted using the message signal. At the receiver end, using

matched parameters in a second Bragg feedback setup that generates a matched chaotic waveform, the signal can be recovered using heterodyne demodulation. The robustness of the scheme is examined vis-a-vis system performance for variations in the feedback gain, time delay and DC bias. The system is found to be reasonably robust w.r.t. the feedback gain (significant output distortion for less than 2% mismatch). Robustness w.r.t. TD or $\hat{\alpha}_0$ shows greater mismatch tolerance, with distorted outputs occurring only for mismatch greater than about 10%. The noise analysis involved different amounts of band pass noise at the transmitter (electronic or instrumental) added to the bias input of the RF source. The cutoff of the output LPF is adjusted to allow passage of any waveform content up to the signal or noise bandwidth (whichever is higher). The results obtained are not definitive in terms of noise-induced distortions. The output waveforms recovered for most cases exhibit additive effects due to noise, but not any significant waveform distortion. Channel noise, including frequency or phase interference have not been considered.

REFERENCES

[1] M.R. Chatterjee and M. Al-Saedi, "Examination of chaos-based encryption and retrieval in a hybrid acousto-optic device," Frontiers in Optics Technical Digest (CD), paper # FWC3, Rochester, NY (2008).

[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," in Proc. SPIE **7464**, San Diego, CA, USA (2009).

[3] K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," Opt. Commun. **Vol. 30**, 257.

[4] H.M. Gibbs, F.A. Hopf, D.L. Kaplan, and R.L. Shoemaker, "Observation of chaos in optical bistability," Phys. Rev. Lett. **46**, 474 (1981).

[5] R.G. Harrison, W.J. Firth, C.A. Emshary, and I.A. Alsaidi, "Observation of period doubling in all-optical resonator containing NH_3 gas", Phys, Rev. Lett. **51**, 562 (1983).

[6] J. Chrostowski, C. Delisle and R. Tremblay, "Oscillations in acousto-optic bistable device," Can. J. Phys. **61**, 188 (1983).

[7] J. Chrostowski, "Noisy bifurcation in acousto-optic bistability," Phys. Rev. A **26**, 3023 (1982).

[8] T.-C. Poon and S.K. Cheung, "Performance of a hybrid bistable device using an acoustooptic modulator," Appl. Opt. **28**, 4787 (1989).

[9] M.R. Chatterjee and J.-J. Huang, "Demonstration of acousto–optic bistability and chaos by direct nonlinear circuit modeling," Appl. Opt. **31**, 2506 (1992).

[10] P.P. Banerjee, U. Banerjee and H. Kaplan, "Response of an acousto-optic device with feedback to time-varying inputs," Appl. Opt., **31**, 1842 (1992).

[11] A. Korpel**, "**Two-dimensional plane wave theory of strong acousto-optic interaction in isotropic media," J. Opt. Soc. Am. **69**, 678 (1979).

[12] S.-T. Chen and M.R. Chatterjee, "Dual-input hybrid acousto-optic set-reset flip-flop and its nonlinear dynamics," Appl. Opt. **36**, 3147 (1997).