8-2009

Design of Acousto-optic Chaos Based Secure Free-space Optical Communication Links

Anjan K. Ghosh
University of Oklahoma

Pramode K. Verma
University of Oklahoma

Samuel Cheng
University of Oklahoma

Robert C. Huck
University of Oklahoma

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

See next page for additional authors

Design of Acousto-optic Chaos based Secure Free-space Optical Communication Links

A. K. Ghosh[a], P. Verma[a], S. Cheng[a], R. C. Huck[a], M. R. Chatterjee[b], M. Al-Saedi[b]

[a]Telecommunication Engineering, School of Electrical and Computer Engineering, University of Oklahoma, Tulsa, OK 74135.
[b]Department of Electrical and Computer Engineering, University of Dayton, Dayton, OH 45469.

ABSTRACT

We discuss the design of an acousto-optic cell based free space optical communication link where the data beam is made secure through chaos encryption. Using external signal modulation of the diffracted light from a hybrid acousto-optic cell chaos (or directly via incorporation in the sound-cell driver's bias voltage) encryption of data is possible. We have shown numerically that decryption of the encoded data is possible by using an identical acousto-optic system in the receiver.

Keywords: Chaos, Acousto-Optics, Laser Communications, Free-space optical communications, Chaos encryption, Secure communications.

INTRODUCTION

Security is a most desirable aspect of present-day communication systems. The application of chaos and nonlinear dynamical systems to communications provides many promising new directions in areas of coding, security, and ultra-wideband communications [1]. Nonlinear techniques and chaotic systems can be applied in a straightforward manner to the encryption/decryption blocks of a digital communication system. Data can be embedded in a chaotic sequence, which is only known to the desired receiver – significantly enhancing security. Nonlinear and chaotic techniques can also be applied to channel encoding/decoding functions providing a greater immunity to channel fading problems.

Chaotic modulation and spreading techniques may allow for improved multiple channel access approaches and improved immunity to potential jamming and fading conditions [1]. Chaotic modulation of data may be less sensitive to electronic nonlinearities in the transceivers. The spectra of chaotic signals make them very attractive for use as carriers in spread spectrum communications. Because chaotic signals are generated by deterministic dynamical systems, two coupled chaotic systems can be synchronized to produce nearly identical chaotic oscillations. This fact provides the key to the recovery of information that is modulated onto a chaotic carrier. Deployment of communication systems where signals are encrypted with chaos started with the demonstration of the synchronization of two coupled chaotic systems [1]. In addition, a chaos-based communications system could also improve privacy and security, and reduce probability of intercept, because chaotic sequences, unlike pseudorandom sequences, can be made completely nonperiodic.

A number of papers have been written on the chaotic encryption of optical signals in both fiber optic and free-space optical communication links and networks [2-14]. Most of these papers reported the chaotic encryption and decryption performed using nonlinear dynamics of external cavity feedback in semiconductor lasers. In a few papers the researchers generated the chaos using the nonlinearities in Er doped fiber lasers. Analysis of such optical chaos cryptosystems has been so far more difficult to implement than that of the electronic set-ups. Only Er fiber laser chaotic dynamics was shown to be analyzed with enough detail, with the disadvantage that the chaos thus generated can be broken and the message easily retrieved. The lack of complexity inherent to the weak nonlinearity attached to the fiber laser dynamics is responsible for this weakness [14]. Cryptanalysis of the other optical chaos encryption systems is still under progress.

Free-Space Laser Communications IX, edited by Arun K. Majumdar, Christopher C. Davis,
Proc. of SPIE Vol. 7464, 74640L · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.826813

In recent papers [15, 16], authors numerically demonstrated secure data transmission, using synchronized "twin" semiconductor lasers working in the chaotic regime, which represent the transmitter and receiver of a cryptographic scheme, compatible with free-space optics technology. Chaotic dynamics and synchronization are obtained by current injection into the laser pair of a common, chaotic driving-signal. Results of simulations were reported in [15] for the configuration in which the chaotic driving-current is obtained by photodetection of the emission of a third laser (driver), chaotic by delayed optical feedback in a short cavity scheme. The emissions of the synchronized, matched lasers were highly correlated, whereas their correlation with the driver was low [15]. The digital message modulates the pumping current of the transmitter. Message recovery is performed by subtracting the chaos, locally generated by the synchronized receiver laser, from the signal obtained by photodetection (at the receiver side) of the chaos-masked message transmitted in free space. Attenuation of the signal in atmospheric propagation and noise were included in the simulations. Security has been investigated and demonstrated by considering the effect, on synchronization and message recovery, of the parameter mismatch between transmitter and receiver.

BASIC DESIGN

Refs. [17-20] have shown that (a) encryption of optical signals using external modulation of the diffracted light in acousto-optic modulators and (b) retrieval and de-encryption of encoded signal using parametrically synchronized chaotic demodulation with another acousto-optic cell are both possible. A typical configuration of an acousto-optic (AO) Bragg call based chaos encryption system is shown in Fig. 1 [19]. In Fig. 1 we show that a laser beam diffracted by an acousto-optic Bragg cell is detected by a photodiode (PD) whose output is fed back electronically to the Bragg cell.

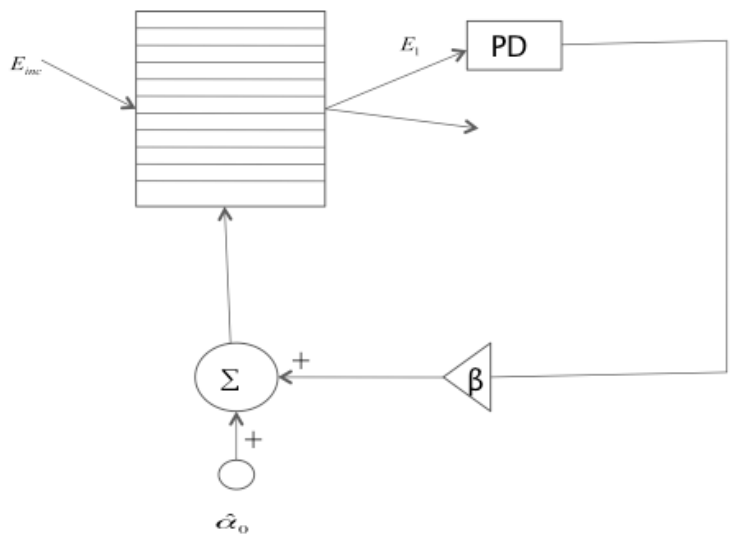

Fig. 1 An Acousto-optic feedback system for generating chaos.

Using this idea we design AO cell based free space optical communication links where the data beam is made secure through chaos encryption. It is well known that the with the electronic feedback the intensity of the diffracted beam detected by the PD is given by

$$I_1(t) = I_{inc} \sin^2\left[\frac{\hat{\alpha}_0}{2} + \frac{\hat{\beta}_0}{2} I_1(t-\tau)\right] \qquad (1)$$

where $\hat{\beta}_0 = \eta\beta$ is the effective feedback gain and τ is the time delay [19].

Chaotic modulation of the diffracted and the undiffracted beams of the light at the output of the AO cell are achieved with suitable values of the feedback and gain parameters of the opto-electronic system shown in Fig. 1 [17-20]. The modulation may be achieved by adjusting the bias voltage $\hat{\alpha}_0$ via adding a modulation signal to the DC bias level. Alternatively, it may also be achieved by external modulation of the chaotic laser beam. This enables modulation of the chaotic signal. In Fig. 2b we show an example of signal modulation/encryption of the output intensity of the waveform in Fig. 2a.

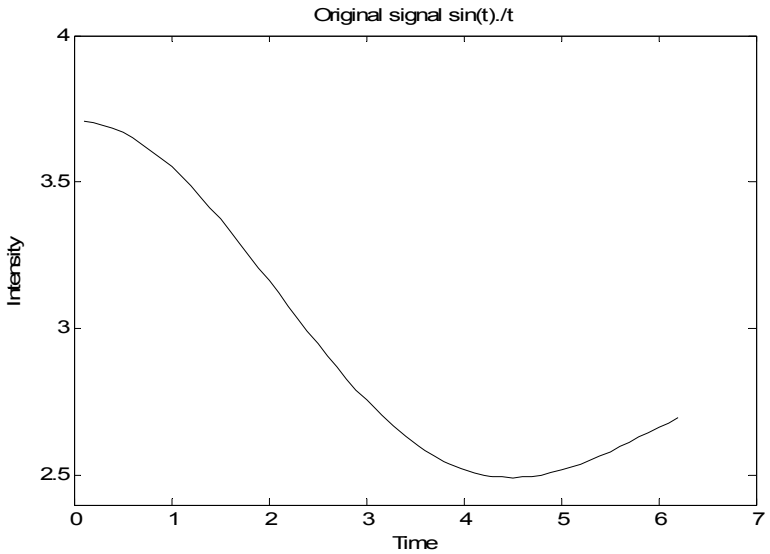

Fig. 2a: Intensity profile of incident beam [20].

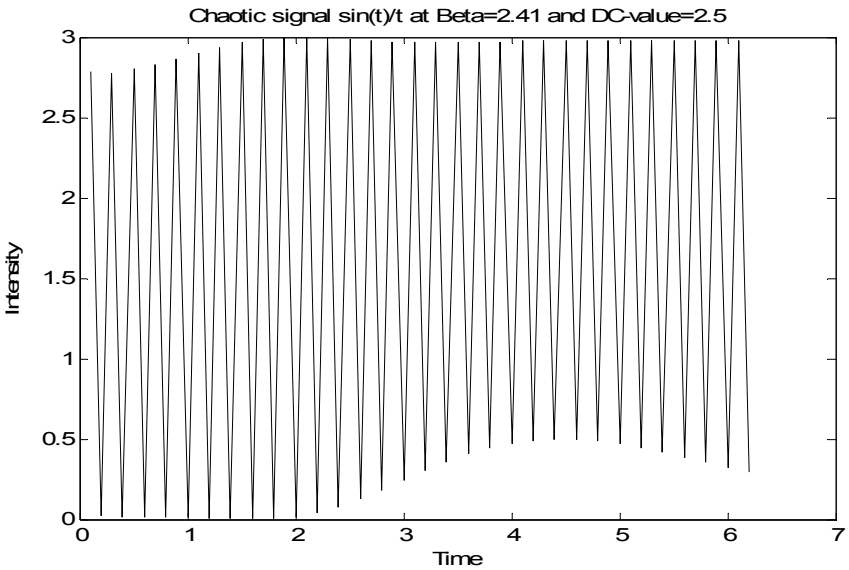

Fig. 2b: Intensity of Diffracted Beam with feedback on [20].

In the receiver a PD detects the chaos-encrypted beam. The current from the PD is then mixed with a chaotic

signal generated by an AO system identical to the one in the transmitter. A schematic block diagram of the chaos encryption and decryption with AO systems is shown in Fig. 3. In the top part of the block diagram we show the transmitter and in the bottom part the receiver unit is depicted.

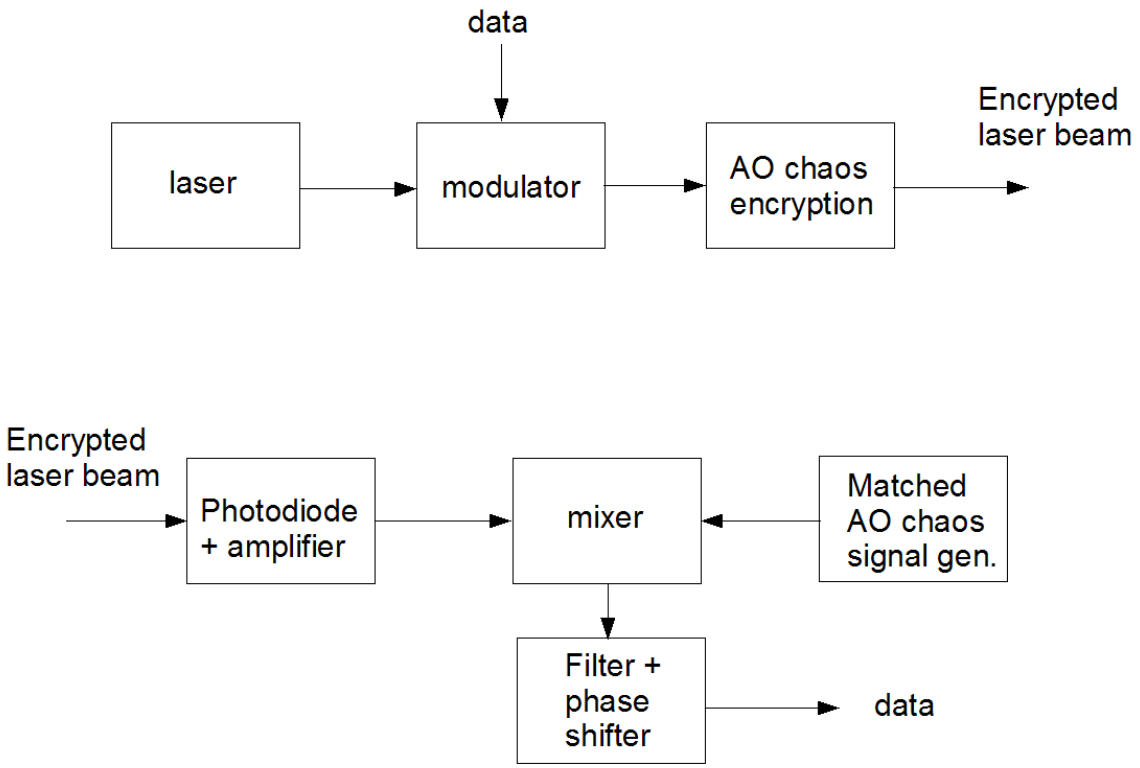

Fig. 3: A block diagram of a free-space optical communication system with AO chaos encryption and decryption.

In Fig. 4 we show the intensity profile of the waveform recovered from the chaos-encrypted waveform in Fig. 2b. Note that even though the displayed waveforms are shown at very low frequency (a few Hz) for illustration purposes only, it is possible to scale the chaos and the modulation bandwidth up to the MHz range or higher by adjusting such parameters as the delay time in the A-O feedback loop. We also note that while modulation of the chaos waveform will likely lead to spatial deflections of the first-order A-O beam, thereby potentially causing tracking problems at the receiver, this drawback may be averted by switching to the zeroth-order beam that remains spatially undeviated.

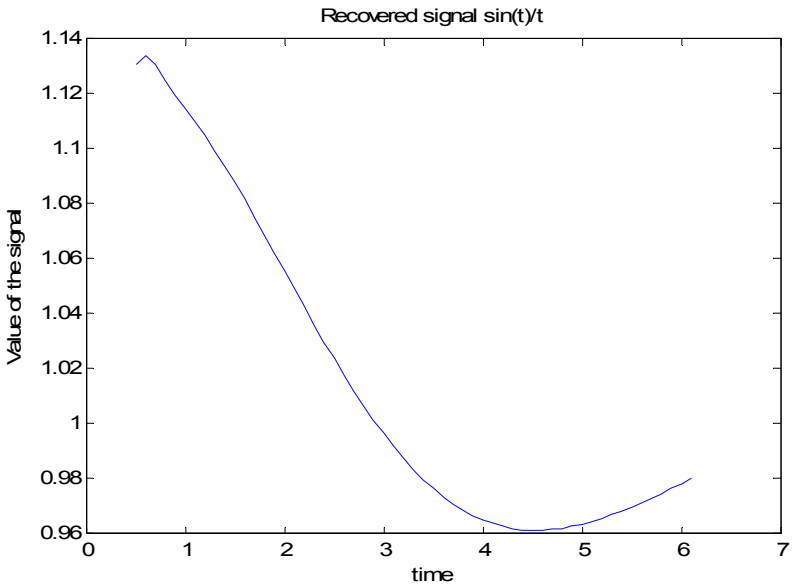

Fig. 4: Intensity of the recovered signal corresponding to the input in Fig. 2a [20].

CONCLUSIONS

It is possible to use chaos generated by an AO system with feedback to encrypt a laser beam carrying data. In this paper, we discussed preliminary results on using such an encryption and decryption technology in building a free space optical communication system.

REFERENCES

[1] Larson, L.E., Liu, J. and Tsimring, L. S., Editors, [Digital Communications Using Chaos and Nonlinear Dynamics], Springer-Verlag, New York 2006.

[2] Rulkov, N. F., Vorontsov, M. A., and Illing, L., "Chaotic Free-Space Laser Communication over a Turbulent Channel," Physical Rev. Letters, 89(27), 277905-1(2002).

[3] Dingjan, J., Altewischer, van Exter, E. M. P., and Woerdman, J. P., "Experimental Observation of Wave Chaos in a Conventional Optical Resonator," Physical Rev. Letters, 88(6), 064101-1(2002).

[4] Liu, Y. and Davis, P., "Optical Sequence Generation Based on Collision Avoidance Using Chaotic Mode Transitions", IEEE J of Quantum Electronics, 34(9), 1517(1998).

[5] Gastaud, N., Poinsot, S., Larger, L., Merolla, J.-M., Hanna, M., Goedgebuer, J.-P. and Malassenet, F., "Electro-optical chaos for multi-10 Gbit/s optical transmissions", Electronics Letters, 40 (14), (2004).

[6] García-Ojalvo, J. and Roy, R., "Parallel Communication With Optical Spatiotemporal Chaos", IEEE Trans. on Circuits and Systems—I, 48(12), 1491-1497(2001).

[7] Langley, L.N., Turovets, S.I. and Shore, K.A., "Targeting in nonlinear dynamics of laser diodes", IEE Proc.-Optoelectron., 142(3), 157-161(1995).

[8] Larger, L. and Goedgebuer, J.-P., "Encryption using chaotic dynamics for optical telecommunications," Comptes Rendus Physique, 5, 609–611(2004).

[9] Mirasso, C. R., Vicente, R., Colet, P., Mulet, J. and Pérez, T., “Synchronization properties of chaotic semiconductor lasers and applications to encryption,” Comptes Rendus Physique, 5, 613-622(2004).

[10] Annovazzi-Lodi, V., Benedetti, M., Merlo, S., and Norgia, M., “Fiberoptics setup for chaotic cryptographic communications”, Comptes Rendus Physique, 5, 623-631(2004).

[11] Peil, M., Fischer, I. and Elsäßer, W. , “A short external cavity semiconductor laser cryptosystem” , Comptes Rendus Physique, 5, 633-642(2004).

[12] Uchida, A. and Yoshimoria, S.,, “Synchronization of chaos in microchip lasers and its communication applications,” Comptes Rendus Physique, 5, 643-656(2004).

[13] Liu, J.-M. and Tang, S., “Chaotic communications using synchronized semiconductor lasers with optoelectronic feedback” , Comptes Rendus Physique, 5, 657-668(2004).

[14] Geddes, J. B., Short, K. M. and Black, K., “Extraction of Signals from Chaotic Laser Data “ Physical Rev. Letters, 83(25), 5389-5392(1999).

[15] Annovazzi-Lodi, V., Aromataris, G., Benedetti, M. and Merlo,, S., “Secure Chaotic Transmission on a Free-Space Optics Data Link”, IEEE J. of Quantum Electronics, 44(11), 1089-1095(2008).

[16] Ursini, L., Santagiustina, M., and Annovazzi-Lodi, V., “Enhancing the Performances of Digital Chaos-Based Optical Communication by Manchester Coding”, Proc. of OFC/NFOEC 2008, paper no. JWA50 (2008).

[17] Vallee, R. and Delisle, C., “Noise versus chaos in acousto-optic bistability”, Physical Review A, 30(1), 336-342(1984).

[18] Vallee, R. and Delisle, C., “Mode Description of the Dynamical Evolution of an Acousto-Optic Bistable Device”, IEEE J. of Quantum Electronics, 21(9), 1423-1428(1985).

[19] Chatterjee, M. R. and Huang, J.-J., “Demonstration of acousto-optic bistability and chaos by direct nonlinear circuit modeling”, Applied Optics, 31(14), 2506-2517(1992).

[20] Chatterjee, M. R. and Al-Saedi, M., “Examination of Chaotic Signal Encryption, Synchronization and Retrieval Using Hybrid Acousto-Optic Feedback”, Proc. of OSA FiO/LS/META/OF&T 2008, paper no. FWC3 (2008).