7-2015

Secure Transmission and Retrieval of Images in Conjunction with Steganography using Chaos in Nonlinear Acousto-optic Feedback

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

Fares S. Almehmadi
University of Dayton

eCommons Citation

Chatterjee, Monish Ranjan and Almehmadi, Fares S., "Secure Transmission and Retrieval of Images in Conjunction with Steganography using Chaos in Nonlinear Acousto-optic Feedback" (2015). *Electrical and Computer Engineering Faculty Publications.* Paper 325.
http://ecommons.udayton.edu/ece_fac_pub/325

Secure Transmission and Retrieval of Images in Conjunction with Steganography Using Chaos in Nonlinear Acousto-Optic Feedback

Monish R. Chatterjee[1] **and Fares S. Almehmadi**[1]
[1]*Department of Electrical & Computer Engineering*
University of Dayton, Dayton, Ohio 45469
E-mail: mchatterjee1@udayton.edu

Abstract: Digital images are encrypted onto a chaotic carrier in a Bragg cell under hybrid nonlinear feedback and secure data is embedded into the system via steganography. System robustness (with and without channel noise) is analyzed vis-a-vis information security.

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

1. Background

An acousto-optic (AO) device consists of a crystal driven by a piezoelectric oscillator, allowing for controllable diffraction of a laser beam. The sound waves effectively create a grating, and the deflection is a function of the light and sound frequencies and crystal properties, all of which are summarized by the Klein-Cook parameter (Q). A single diffracted order is created in the Bragg regime, in which Q is larger than 8π. This arrangement is utilized for many signal-processing applications, and if it is incorporated into a feedback loop, an AO cell can chaotically modulate an input signal for encryption applications. When used within a nonlinear feedback loop, the diffracted beam in the chaotic regime may be used as a carrier for secure information transmission. This arrangement produces controllable nonlinear dynamics, leading to secure static and dynamic transmission and retrieval of analog and digital signals, including applications in the medical and steganography areas.

2. Chaotic encryption and decryption with profiled optical beams

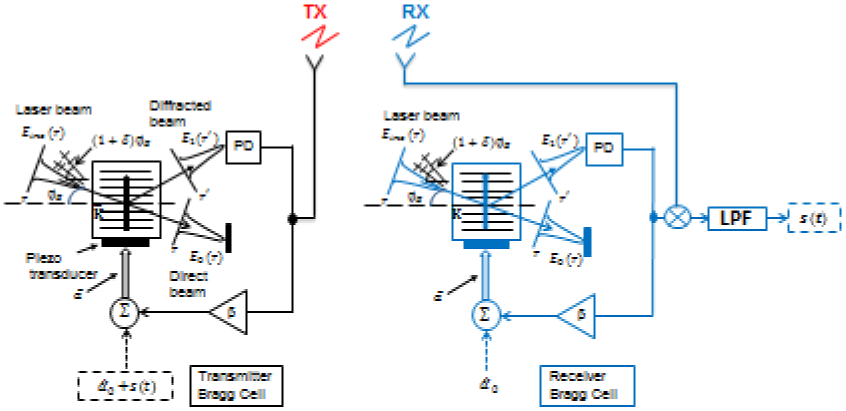

Fig.1. Heterodyne scheme for encrypting and decrypting using A-O chaos.

Figure 1 illustrates the AO feedback loops for chaotic encryption/decryption. An understanding of the full hybrid closed-loop AO system (HAOF) is achieved by exploring the nonlinear dynamics of the photodetector current $I(t)$. The feedback is nonlinear because of the intensity-dependent ($\propto$ (amp)^2) feedback current. Uniform plane waves lead to a $\sin^2$ variation in intensity. Here, to understand the effect of profiled beams, a modified version of this expression was developed and used to simulate the system for arbitrary profiles [1]. Equation 1 contains this expression, where the function f represents the observed output along the optical phase shift dimension for a non-uniform input profile, $\hat{\alpha}_0$ is the peak phase delay, $\tilde{\beta}$ is the feedback gain, and TD is the feedback time delay [1].

$$I_{ph}(t) = \left| f\left[0.5\left(\tilde{\alpha}_0(t) + \tilde{\beta}\left(I_{ph}(t-T_D)\right)\right)\right]\right|^2. \qquad (1)$$

To apply chaos as a means of encrypting a signal waveform $s(t)$, the signal is applied to the bias driver such thatthe peak phase delay has the form of $\hat{\alpha} = \hat{\alpha}_0 + s(t)$. The resulting chaotic photodetector current is then viewed as a modulated version of the input signal. After transmission through a channel, $s(t)$ is recovered in the manner of standard heterodyne detection where a local chaos wave is generated using a second Bragg cell parameters matched to the transmitter cell. The local chaos is multiplied with the modulated signal, and the product is low-pass filtered to recover $s(t)$.

With the proper choice of parameters, $s(t)$ is completely encrypted, and a simulation of this case is shown in Fig. 2 using a digital signal. The chaos contains no apparent hint of the original signal, but by using matched parameters in the receiver, it is recovered with no bit errors [1]. To illustrate the sensitivity to mismatch achieved using non-uniform input beams, Fig. 3 shows digital images recovered with different levels of mismatch in a single parameter. The original image is a color version of the standard Lena test image, and mismatches of 0.1%, 0.2%, and 0.4% are used in the gain parameter.

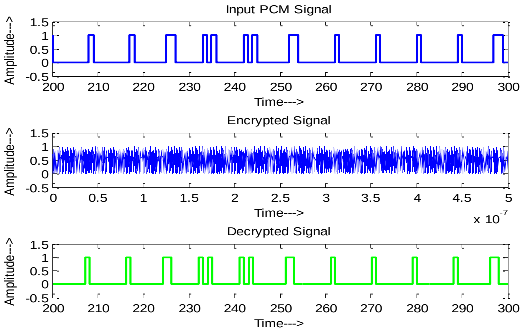

Fig.2. Encryption and recovery; matched transmitter and receiver keys; $\widetilde{\boldsymbol{\beta}}$ =3, $\boldsymbol{TD}$= 0.05 μs, $\widehat{\boldsymbol{\alpha}}_{\boldsymbol{0}}$= 2.

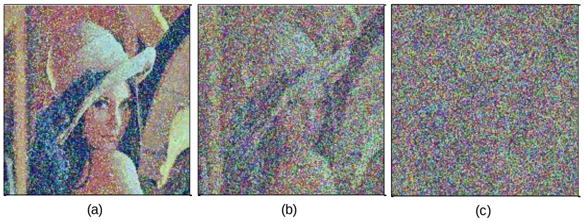

Fig.3. Recovered Lena images with three levels of mismatch (a) 0.1% mismatch, (b) 0.2% mismatch, and (c) 0.4% mismatch.

3. Applications of the AO modulation scheme

The potential strength of encryption for the AO scheme is appropriate for especially sensitive medical applications, and the scheme is tested on the encryption of electrocardiography (ECG) signals, which require higher security due to their biometric properties as well as legal protections. This work includes combining AO encryption with steganography as an additional layer of security [2,3]. Fig. 4 illustrates this concept for a medical image in which patient information is hidden using steganography encoding. The resulting stego image is then encrypted, transmitted, and recovered with AO modulation, and the hidden text is recovered with steganography decoding.

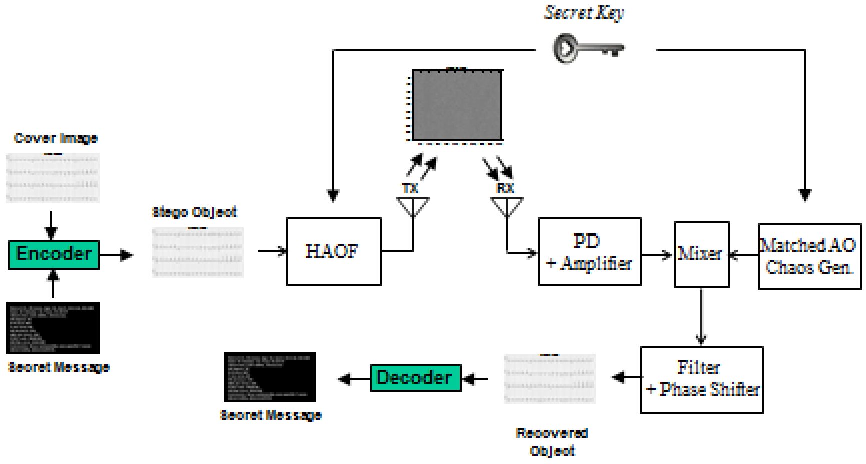

Fig.4. Block diagram of multilayer security technique combining steganography with chaotic image encryption to transmit ECG combined with patient identification.

4. Conclusion

The feasibility of chaotic encryption of low or high bandwidth signals with HAOF-based nonlinear modulation is clearly demonstrated. The strength of the encryption is shown to significantly increase due to the use of physically realistic *profiled* beams in the simulation, relative to earlier analyses that assume uniform input beams.

5. References

[1] 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).
[2] F.S. Almehmadi and M.R. Chatterjee, "Secure chaotic transmission of ECG signals with acousto-optic modulation under profiled beam propagation," Appl. Opt. 54, 195-203 (2015).
[3] G. Kenfack and A. Tiedeu, “Chaos-based encryption of ECG signals: experimental results,” J. Biomed. Sci. Eng. 7, 368–379 (2014).