University of Dayton
eCommons

Electrical and Computer Engineering Faculty Publications

Department of Electrical and Computer Engineering

2-2015

Secure Transmission of Static and Dynamic Images via Chaotic Encryption in Acousto-optic Hybrid Feedback with Profiled Light Beams

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 of Static and Dynamic Images via Chaotic Encryption in Acousto-optic Hybrid Feedback with Profiled Light Beams" (2015). *Electrical and Computer Engineering Faculty Publications*. 356.
https://ecommons.udayton.edu/ece_fac_pub/356

Secure transmission of static and dynamic images via chaotic encryption in acousto-optic hybrid feedback with profiled light beams

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

Secure information encryption via acousto-optic (AO) chaos with profiled optical beams indicates substantially better performance in terms of system robustness. This paper examines encryption of static and time-varying (video) images onto AO chaotic carriers using Gaussian-profile beams with diffracted data numerically generated using transfer functions. The use of profiled beams leads to considerable improvement in the encrypted signal. While static image encryption exhibits parameter tolerances within about ±10% for uniform optical beams, profiled beams reduce the tolerance to less than 1%, thereby vastly improving both the overall security of the transmitted information as well as the quality of the image retrieval.

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

1. INTRODUCTION

As handheld electronic devices become increasingly popular and more powerful, with capabilities of collecting, storing, and transmitting images and video, demand for protecting sensitive or personal imagery is increasing. There has been a recent uptick of hacked and stolen images, either private or classified government imagery, which are distributed illegally online. The ability to easily collect, store, and transmit images and video has great utility, but it also has a corresponding potential for harm. There is a growing need for strong protection, in the form of encryption, to prevent unauthorized distribution of imagery and data. Encryption for images typically reduces an image to a bit stream and applies generic encryption algorithms that work for any binary data. Examples of such algorithms include the Digital Encryption Standard (DES), the Advanced Encryption Standard (AES), the TwoFish cipher, and the BlowFish cipher [1-3]. The literature on image-specific encryption can be divided into techniques that use optics, and techniques that use software or electronic circuits [4,5]. Within these categories, there are approaches that utilize chaos for encryption. This is advantageous due to the fact that a chaotic system is sensitive to a set of parameters and initial conditions, which serves to create a strong encryption key [6]. In this work, a method for chaotic image/video encryption implemented with acousto-optic (AO) devices is studied.

AO devices controllably diffract light beams using the interaction of light and sound waves. An input light beam passes through a crystal in which a piezoelectric device creates acoustic vibrations. These vibrations behave as a diffraction grating, causing the deflection of the light beam. AO cells are commonly used in signal processing applications, including laser beam deflection, modulation, filtering, and, when used with feedback, encryption/decryption [7]. The light and sound frequencies along with various crystal properties determine the characteristics of the deflection. A unitless quantity called the Klein-Cook parameter (Q) summarizes these parameters into a single value that determines

Broadband Access Communication Technologies IX, edited by Benjamin B. Dingel, Katsutoshi Tsukamoto,
Proc. of SPIE Vol. 9387, 938711 · © 2015 SPIE · CCC code: 0277-786X/15/$18 · doi: 10.1117/12.2076217

the operating mode of the device. In the Bragg mode of operation, Q is larger than 8π, and the cell produces only one diffracted order [8].

To use an AO cell in a feedback loop, the diffracted beam is converted into an electrical signal by a photodetector, whose output is amplified, added to an offset, and applied to the acoustic driver for the piezoelectric device. If an input signal is applied to the offset and the output is taken from the photodetector, a signal processing device is made. These devices exhibit nonlinear dynamics, including mono-, bi-, multistable and chaotic behavior [9-11]. These dynamic properties, especially chaotic behavior, are useful for signal processing applications such as encryption and decryption [12].

In order to understand the chaotic behavior and the conditions under which it occurs, two techniques are applied to the AO feedback loop: the Lyapunov exponent and bifurcation maps. The Lyapunov exponent is a function of Q, the offset value, feedback gain, and input beam intensity, and it quantities when the system is chaotic. Bifurcation maps plot the photodetector output versus the optical phase shift or feedback gain, visually showing the threshold between bistability and chaos [13]. Both techniques indicate that chaotic bands appear unpredictably on intervals within the parameter space. In order to use such passbands of chaos for encryption, it is critical to know what combination of parameters produces chaos and the extent of the chaos as the parameters vary [14].

When the parameters are controlled to produce chaos, the output signal is interpreted as a chaotically encrypted version of the input signal applied to the bias driver. The chaotic signal, which is transmitted over a channel, has an amplitude that is related to the input signal amplitude via the RF oscillator. At the receiver, to demodulate the encrypted signal, a second AO feedback loop with parameters identical to the transmitter loop is used in the manner of a standard heterodyne detector. The locally generated chaos is multiplied with the incoming modulated chaotic signal. The product waveform is then passed through a low pass filter (LPF) with cutoff frequency adjusted to accommodate the information signal bandwidth, and corrected for a 180° phase shift [12]. For strong encryption, parameter mismatch beyond a small threshold will ideally cause demodulation to fail.

Previous analysis of closed-loop nonlinear properties utilizes the assumption of a uniform plane wave input light beam, leading to tractable mathematics for describing the light and sound interaction. This analysis produces commonly used expressions for Bragg diffraction, which can be used to model chaos and thereafter the encryption and decryption of signals [12]. Such modeling does not capture the effect of realistic, profiled laser beams, and the chaotic behavior for a feedback loops using non-uniform profiled beam was shown to be significantly different [14]. For example, the location and width of the passbands of chaos are sensitive to input beam profiles [14]. The present work uses simulation of feedback loops with profiled, non-uniform input beams for image and video encryption.

An overview of chaotic encryption with profiled beams is presented in section 2, describing the encryption performance for digital data. In section 3, performance results specific to image encryption are described, including performance in the presence of parameter mismatch and channel noise. Encryption results for a test video are presented in section 4, along with an analysis of the robustness of the encryption to the key parameters. The final section summarizes the main results and discusses future work.

2. CHAOTIC ENCRYPTION AND DECRYPTION WITH PROFILED OPTICAL BEAMS

Two AO feedback modulators, for transmission and reception, are shown in Fig.1. In the transmitter feedback loop, two scattered orders are created from an arbitrary input beam profile. 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 [15]. 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+ δ)ϕ_B where δ is a dimensionless measure of angular deviation. A set of coupled differential equations leads to expressions for the two scattered output at near-Bragg diffraction [11]. Using these expressions, a transfer function formalism is developed by Chatterjee *et*. al [15]. 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 [15].

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

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.

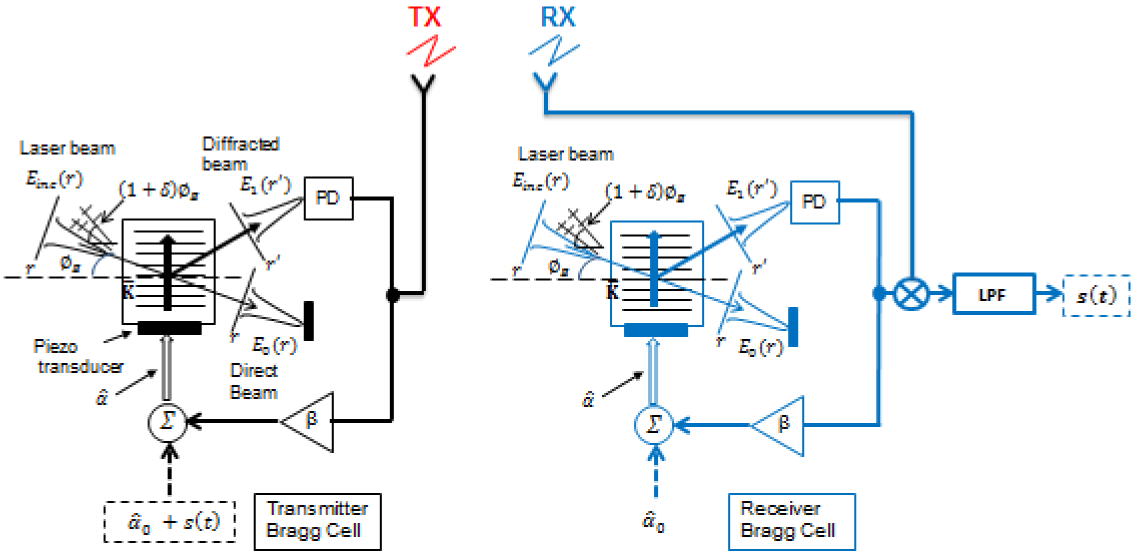


Fig.1. Heterodyne scheme for encrypting and decrypting using A-O chaos.

Previous work presented results using eq.1 with various incident profiles $E_{inc}(r)$, and it was found that the diffracted profile deviated in shape from the well-known results obtained with the uniform beam assumption, especially for high Q values. These deviations lead to significant changes in the behavior of the closed-loop system, as is discussed in [14], which strongly effects encryption performance. Since real laser beams are profiled, it is critical to understand and model these behaviors [16].

The full hybrid closed-loop AO system (HAOF) 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, first observed in 1978 [11]. If a uniform plane wave input is assumed, then well-known analysis leads to an expression for $I(t)$ [11]. To understand the effect of profiled beams, a modified version of this equation was developed and used to simulate the system for arbitrary profiles [14]. 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 [14].

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

The function f in general has no closed-form expression, unlike in the uniform plane wave case, where f becomes a sine-profile. For the simulations 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 AO cell [11].

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 $\hat{\alpha} = \hat{\alpha}_0 + s(t)$, as shown in Fig. 1. 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 then transmitted through a channel. At the receiver, the signal is recovered in the manner of standard heterodyne detection as shown in Fig. 1. 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 is then multiplied with the incoming photo-detected modulated chaotic signal, and the product is low-pass filtered, using a cutoff frequency adjusted to accommodate the bandwidth of $s(t)$.

Under certain conditions, the signal $s(t)$ modulates the chaos similar to standard AM, such that the shape of $s(t)$ appears in the envelope [12]. However, with the proper choice of parameters, the signal waveform may be completely hidden within the chaos. Similar to standard AM, the bandwidth of $s(t)$ it should be less than half the center frequency of the chaotic carrier to avoid aliasing, although in reality, the bandwidth should be substantially smaller than the chaos frequency. The chaos frequency depends on the TD through the equation $f = 1/(2 * TD)$, and in this work, frequencies in the range of 10 MHz are used.

The results of a simulation of the encryption system, using profiled beams and implemented in Matlab, are shown in Fig.2. The input signal $s(t)$ in this example is a periodic square wave with a frequency of a few MHz, and Fig. 2 illustrates the original square wave, the encrypted signal, and the recovered signal. The encrypted signal clearly has the original in its envelope, which is because the system is expected to be an amplitude modulation in some limit [12]. 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.

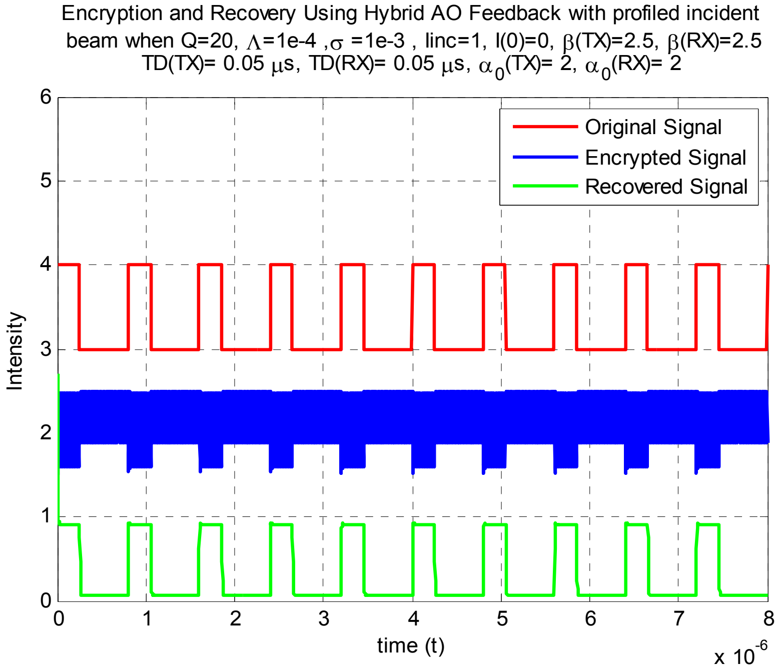


Fig.2. Encryption and recovery of a square waveform using chaos.

The second example considered here is a binary signal, shown in Fig.3 along with its encrypted and recovered versions. In this case, the parameters are chosen such that the original binary signal is not apparent in the encrypted chaos signal. Using matched parameters in the receiver, no bit errors occur in this simulation [17].

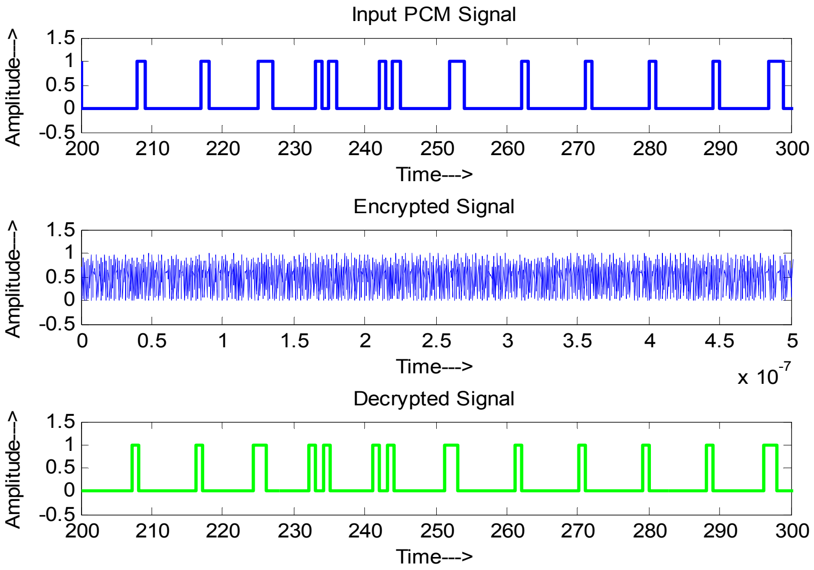


Fig.3. Encryption and recovery using hybrid AO feedback with profiled incident beam
when Q=20, Λ=1e-4; matched transmitter and receiver keys; $\tilde{\boldsymbol{\beta}}$ =3, $\boldsymbol{TD}$**=** 0.05 μs, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$= 2 (after [17])**.**

To quantify the effect of random channel noise on bit errors, a random binary signal is transmitted through the system for varying levels of fixed-variance channel noise, and the percentage of recovered bits in error is used to measure bit error rate (BER). The BER is measured as a function of the ratio of energy per bit to noise power (E_b/N_0) (with assumed white noise PSD $N_0/2$), and the BER curve is plotted on a logarithmic scale [17]. Fig.4 shows this BER curve for the AO chaotic system. This curve shows marginally higher bit error rates relative to systems that provide no encryption, as previously described [17].

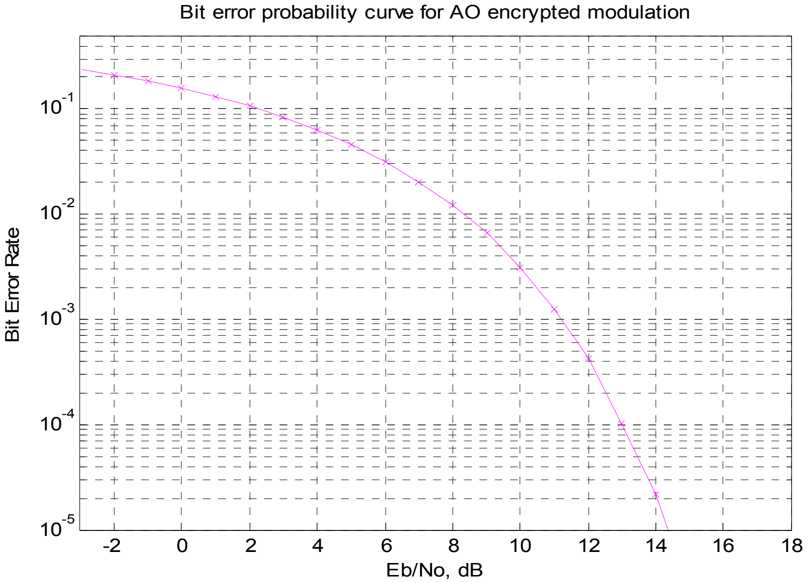


Fig.4. BER versus the ratio of energy per bit to noise power.

3. SIMULATION RESULTS FOR ENCRYPTION AND DECRYPTION OF IMAGES

Since a digital image can be reduced to a bit stream, it is straightforward to extend these results to test the performance of the closed-loop system with imagery. The results with profiled beams show significantly improved quality of signal retrieval as well as much lower parameter tolerance (around ±0.1% per key) relative to the uniform beam case, which has high parameter tolerance and has been shown to be far less satisfactory for image recovery. This motivates testing the profiled beam encryption system with digital images to measure the performance improvement. Fig. 5 illustrates a block diagram of the image encryption and recovery, using a pair of matched HAOFs in a heterodyne modulation scheme. A color version of the standard Lena test image, with 512x512 pixels and 24 bits per pixel, is applied under three conditions: matched parameter keys and no channel noise, mismatched parameter keys with no channel noise, and matched parameter keys with channel noise. In each case, the quality of the recovered signal is measured in terms of bit errors, similar to the previous characterization with binary data. Given a bit rate of 10 Mbits/sec, which is determined by the HAOF time delay parameter, an image of this dimension would require about 0.6 sec to encrypt and recover.

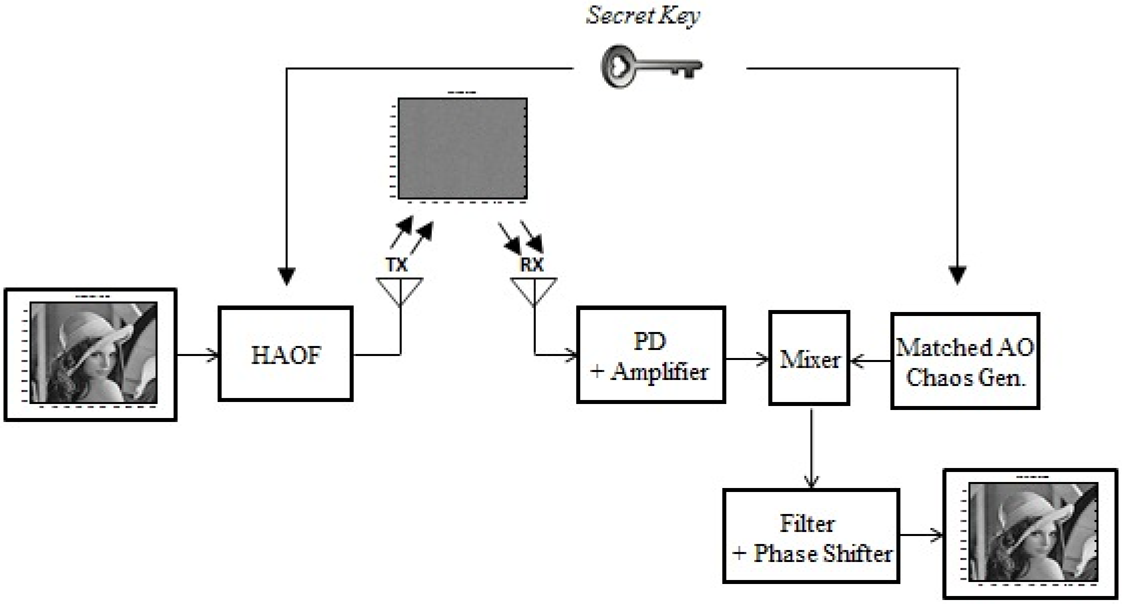


Fig.5. Block diagram for encryption and decryption of images using HAOF modulators.

The first test case applies the digital Lena image to the encryption scheme, using the same matched parameters for both the transmitter and receiver HAOFs. In this case, as was previously shown for PCM signals, the bit error rate is effectively zero, and the recovered image is identical to the original. Figure 6 illustrates this result, along with the encrypted version of the image, which has no visible remnant of the original. The encrypted image is formed by attempting to directly low-pass filter the chaotically modulated signal in order to recover the bit sequence. As was seen in the previous section with the square wave signal, if the gain parameter is too low, then the modulated signal will contain the original bit sequence in the envelope, and a low-pass filter will recover it. In Fig. 6, the gain parameter was set to $\tilde{\beta}$ =3.4, which is sufficient to fully obscure the original bit sequence in the chaos, and a low-pass filter is ineffective to recover the original image. The encrypted image appears as noise in this case.

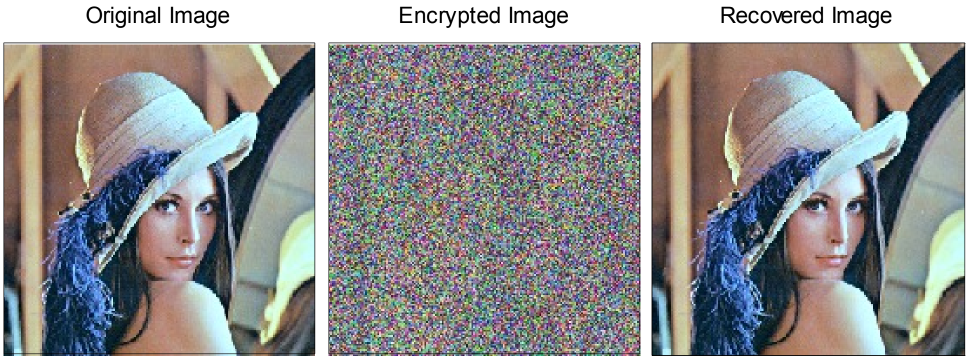


Fig.6. Original Lena standard (left), encrypted version (center) and recovered (right), with matched parameters: $\mathbf{Q}$=20, $\mathbf{\Lambda}$=1e-4 , $\tilde{\boldsymbol{\beta}}$ =3.4, $\mathbf{TD}$= 0.05 μs, $\hat{\boldsymbol{\alpha}}_{\mathbf{0}}$ = 2.

In the second test, the same Lena image is transmitted and recovered with three different levels of mismatch in the gain parameter: 0.1%, 0.2%, and 0.4%. No channel noise is simulated in this case. Figure 7 shows the recovered images for these mismatch values. The 0.1% mismatch causes a significant number of bit errors, but enough pixels remain in the recovered image that the original can visually be recognized. For 0.2% mismatch, the original image is barely recognizable, and fine details are lost. For 0.4%, the image appears as noise, and there is no hint of the original. The threshold level of mismatch, necessary to recover any aspect of the original image, is safely taken to be 0.3%. This threshold level is similar for the other three key parameters [17], creating a very robust key because it is extremely unlikely that all four parameters could be successfully guessed with thresholds this small. This encryption key strength is due to the fact that profiled beams are used in the simulation. Previous results with image encryption using uniform beams in the HAOF simulations indicated threshold values for recovery that were two orders of magnitude greater, in the range of 10-20%. In this case, the image data are not secure, because it is much more likely that the key could be guessed.

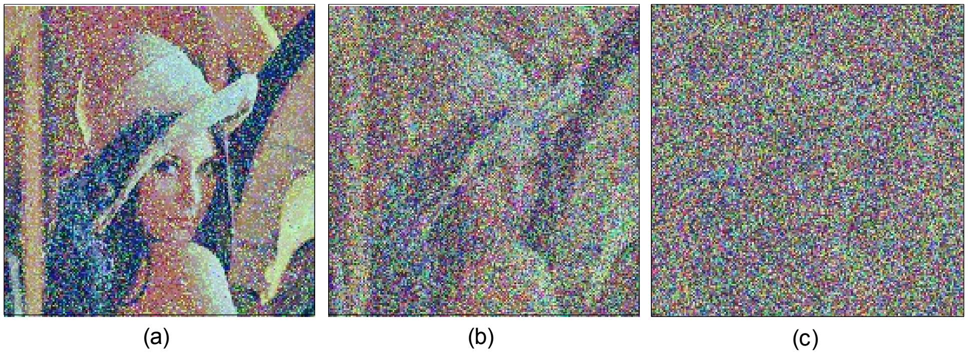
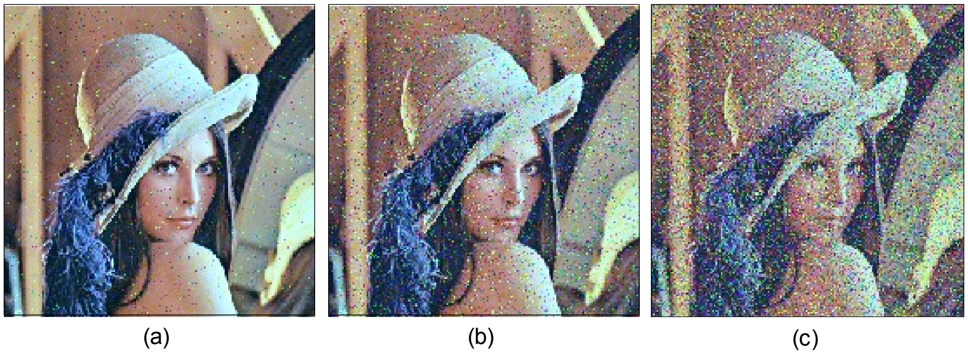


Fig.7. Recovered Lena images with three levels of mismatch in the $\tilde{\boldsymbol{\beta}}$ parameter: (a) 0.1% mismatch, (b) 0.2% mismatch, and (c) 0.4% mismatch.

To measure the effect of random channel noise (with fixed variance, i.e., a non-uniform power spectral density) on the system, the simulation as illustrated in Fig.5 is modified by adding a random signal to the encrypted bit stream. There is no parameter mismatch in this case, and values of energy per bit to noise power (E_b/N_0) are set to be 8 dB, 5 dB, and 1 dB, with corresponding bit error rates of 0.0073, 0.0338, and 0.1079, respectively. Figure 8 shows the effect of such channel noise on the recovered Lena image. These recovered images indicate that channel noise passes through the decryption process and creates pixel errors in the recovered image, without causing any other unpredictable distortion.

These findings indicate that under matched recovery, the chaotic encryption method allows reasonable signal recovery even with strong channel noise (at $E_b/N_0 \approx 1$ dB) being transmitted along with the encrypted signal.



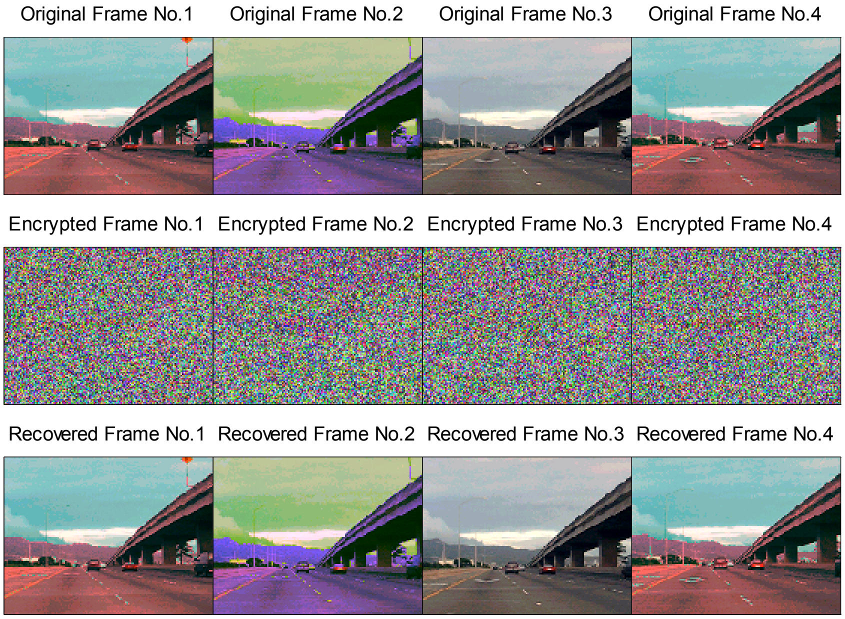
(a) (b) (c)

Fig.8. Recovered Lena images with three levels of channel noise power: (a) BER = 0.0073, E_b/N_0= 8 dB, (b) BER =0.0338, E_b/N_0=5 dB, (c) BER =0.1079, E_b/N_0=1 dB.

Digital image encryption and decryption naturally leads to video encryption, explored in the next section.

4. SIMULATION RESULTS FOR ENCRYPTION AND DECRYPTION OF VIDEO

Video encryption and decryption may be achieved by transmitting and recovering one video frame at a time, in sequence. Here, however, an entire video data cube is transmitted and recovered at one time. The video consists of 95 color frames with 240x320 pixels per frame and 24 bits per pixel. While the actual recovery involves a dynamic video, Fig.9 illustrates four (still) frames from the video clip, showing the original, encrypted, and recovered images assuming matched parameters were used in the transmitter and receiver HAOFs. With the chosen parameters, the original frames are completely hidden within the corresponding encrypted frames, which appear as noise. The results are consistent with what would be expected if the images were encrypted and recovered one at a time, in sequence.



Original Frame No.1 Original Frame No.2 Original Frame No.3 Original Frame No.4

Encrypted Frame No.1 Encrypted Frame No.2 Encrypted Frame No.3 Encrypted Frame No.4

Recovered Frame No.1 Recovered Frame No.2 Recovered Frame No.3 Recovered Frame No.4

Fig.9. Encryption and recovery for four frames from a video, with the original frames in the top row, the encrypted frames in the middle row, and the recovered frames in the bottom row.

The effect of parameter mismatch on the video recovery, shown in Fig.10, is similar to the effect previously observed for single images. Figure 10 shows the recovery for the same four frames as in Fig.9, but with increasing levels of mismatch in the gain parameter. With a mismatch of 0.1% (top row), the original frames are clearly evident, with few pixel errors. A mismatch of 0.15% introduces a significant number of pixel errors (second row), although the original frame can still be seen. At a level of mismatch of 0.2% (third row), the original frames are barely discernable, and they are reduced to noise at a level of 0.3% (bottom row), where the original frame will be unrecoverable. We note that these tolerance thresholds are comparable to those obtained for the single image case discussed earlier. This indicates that the level of robustness of the encryption scheme is not impacted negatively by introducing dynamic images into the transmission system.

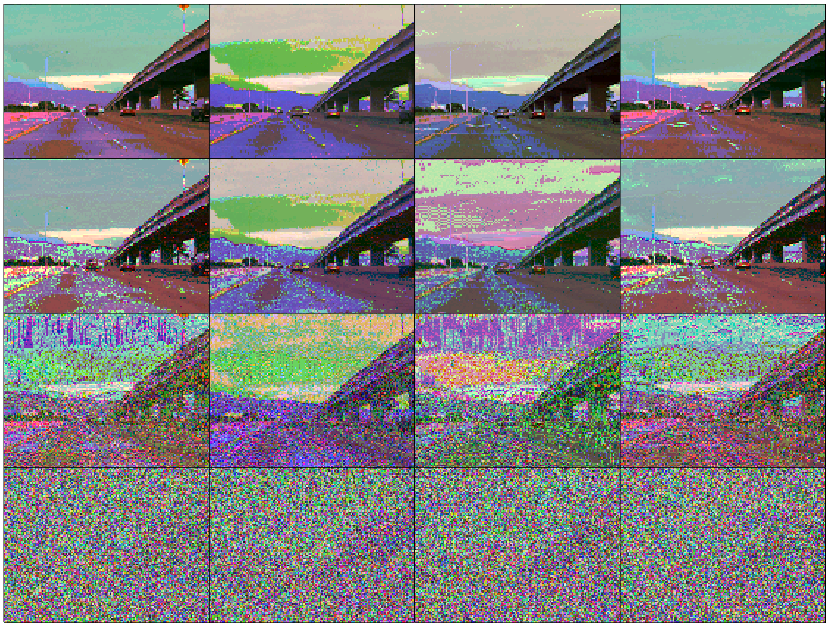


Fig.10. Four recovered frames with different levels of mismatch in the gain parameter: 0.1% (top row), 0.15% (second row), 0.2% (third row), and 0.3% (bottom row).

5. CONCLUSION

The feasibility of chaotic encryption of images and video, using HAOF-based modulation, is clearly demonstrated here. The encrypted signal is shown to be not easily recoverable without precise knowledge of the key system parameters; however, the digital information can be recovered with high accuracy if the key is known. It is shown, for both image and video data, that parameter mismatch beyond a very small threshold destroys the recovery. This sensitivity, which leads to secure encryption, is due to the use of *profiled* beams in the simulation, which create stronger encryption than simulations assuming uniform input beams achieve. This result, although somewhat intuitive, is not analytically tractable; hence, this finding leads to the possibilities of much more robust and versatile encryptions, some of which are reported here. Of special note is the fact that the use of profiled beams introduces a fourth key parameter, viz., the Q of the Bragg cell. This is because Q must be known for the decryption if profiled beams are used. Simulations of image encryption in the presence of channel noise indicate that recovery is possible with negligible bit errors when the ratio of energy per bit to noise power is about 10 dB or above; moreover, even for fairly high levels of noise power, with the energy per bit to noise reaching 1 dB or less, the recovery is not entirely destroyed. The current work will be extended to examine the application of the encryption system to medical imagery, and to combine the encryption with steganography in order to create a multi-layered system that securely embeds personal information within encrypted medical imagery.

REFERENCES

1. FIPS PUB 46, Data Encryption Standard (1977).

2. FIPS PUB 197, Avdanced Encryption Standard, New York, NY (2001).

3. R. Anderson and B. Schneier, “Description of a new variable-length key, 64 bit block cipher (Blowfish),” in Lecture Notes in Computer Science, Springer, Berlin Heidelberg, 191 –204 (1994).

4. B. Hennelly and J.T. Sheridan, “Optical image encryption by random shifting in fractional Fourier domains,” Opt. Lett. 28, 269 –271 (2003).

5. W. Chen and X. Chen, “Space-based optical image encryption,” Opt. Exp. 18, 27095 –27104 (2010).

6. C. Huang and H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” Opt. Commun. 282(11), 2123–2127 (2009).

7. A. Korpel, “Acousto-Optics,” 2nd edition, Marcel Dekker, New York, (1997).

8. 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).

9. J. Chrostowski and C. Delisle, “Bistable piezoelectric Fabry–Perot interferometer,” Can. J. Phys., 57, 1376-1379 (1979).

10. J. Chrostowski and C. Delisle, “Bistable optical switching based on Bragg diffraction,” Opt. Commun. 41, 71–74 (1982).

11. 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).

12. 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).

13. A.K. Ghosh, and P. Verma, “Lyapunov exponent of chaos generated by acousto-optic modulators with feedback,” Opt. Eng. 50, 017005 (2011).

14. 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).

15. 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).

16. 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).

17. F.S. Almehmadi and M.R. Chatterjee, “Improved performance of analog and digital acousto-optic modulation with feedback under profiled beam propagation for secure communication using chaos,” to be published in Opt. Eng. in November, 2014.