Image Cryptography with Chaos: Testing the k-epsilon Turbulence Model as a Chaos Generator

Gary Hammock, MSME, PE

MIDDLE TENNESSEE STATE UNIVERSITY

Computer Science @ Middle Tennessee

Abstract

Cryptography has uses in everyday applications ranging from e-commerce transactions to military communications. Traditional approaches for encrypting images has been performed by processing an input image as a one-dimensional stream of bits before applying the encryption algorithms. There is current research in manipulating images in their native two-dimensional form rather than as a one-dimensional stream. To do this, deterministic chaos maps have been explored for their use in providing the operations required to transform a plaintext image into a ciphertext encrypted image and vice versa. Different approaches for generating chaos maps have been explored ranging from cellular automata to bio-inspired algorithms. This research aims to borrow a deterministic chaos technique from the field of Computational Fluid Dynamics that is used to simulate turbulence in fluid systems. The feasibility of using this technique as a chaos generator will be quantitatively determined using cryptanalysis techniques including measuring the luminance histograms, various image spectra, and pixel covariant dependence.

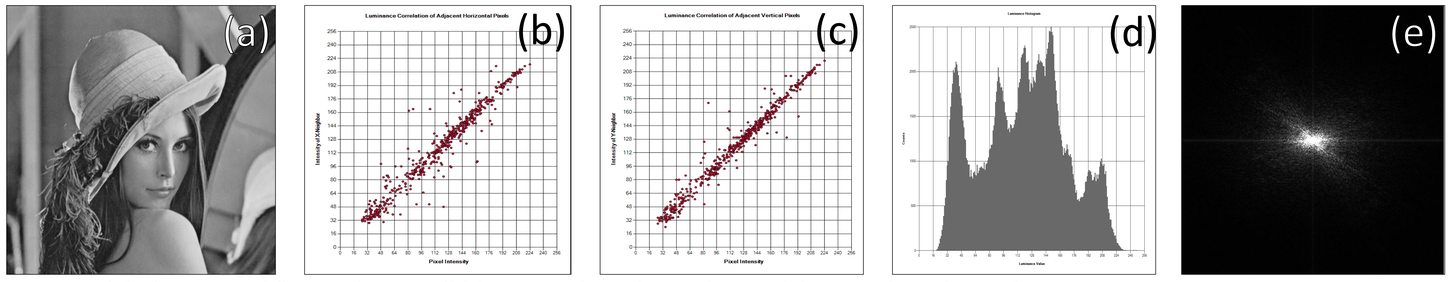

Figure 2. (a) The original "Lenna" image (b) horizontal pixel correlation (c) vertical pixel correlation (d) luminance histogram (e) Fourier spectra

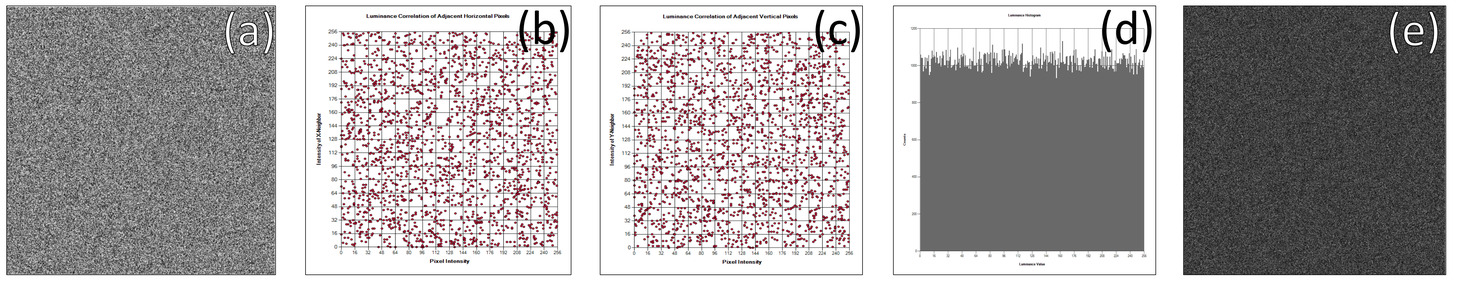

Figure 3. (a) "Lenna" encrypted with the proposed scheme (b) horizontal pixel correlation (c) vertical pixel correlation (d) luminance histogram (e) Fourier spectra

Conclusions / Future Work

As may be observed from Figures 3(b) through 3(e), the proposed technique of image encryption adequately diffuses the original image data. These protections help to ensure that the ciphertext image is robust enough to prevent unauthorized disclosure of the plaintext contents.

A full cryptanalysis has not yet been performed on the technique and additional metrics such as Shannon entropy have not yet been performed, but these results show that the technique of using fluid dynamics inspired approaches can ultimately be used for image encryption.

During this research effort, it was reinforced that discrete chaos maps must be used as an input to maximize the diffusion and information entropy. The conservation equations that govern many natural processes do not adequately maximize the system entropy. This may be an interesting topic for future research.

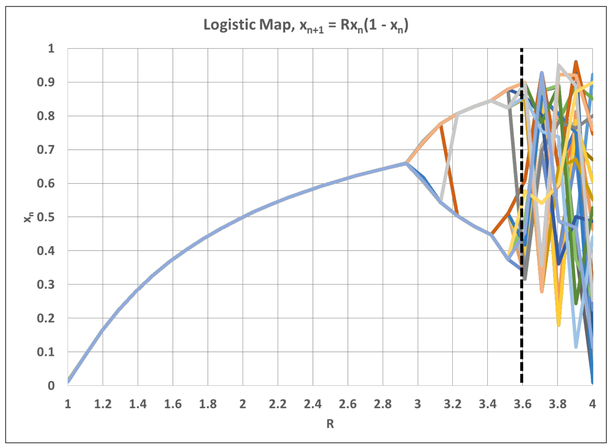

Figure 1. The Logistic map plot showing chaos for R > 3.57

Background

There is current interest in exploring so-called chaos-based cryptographic algorithms for secure image encryption. These image encryption techniques may be envisioned as two-dimensional symmetric key cryptosystems. In these systems, a plaintext image (this could represent a true image that is decoded visually or a matrix of binary data that is parsed algorithmically) is transformed into a ciphertext image where the hidden data should be otherwise unrecoverable without knowledge of the secret key. As mentioned previously, it is ideal for the cryptosystem algorithms to ensure a high degree of confusion between the key and a ciphertext produced using this key. To this end, research is ongoing to explore how to produce higher degrees of confusion without compromising the system to forms of cryptanalysis attacks. This field of research is currently exploring the use of chaos-based approaches to key generation.

Methods

This study assumes a grayscale plaintext image to be analogous to a two-dimensional flow field where the pixel intensities represent energy gradients. Arrays of "mass flow rates" and "heat fluxes" are generated using user input parameters (i.e. the secret key) which seed the logistic map (Figure 1). As may be seen in Figure 1, the logistic map is chaotic for input multipliers $\approx 3.57 < R \leq 4.0$.

The "mass flow rate" array is used to translate the scanlines (rows of pixels) of plaintext image in the same way that increasing the mass flow rate in a pipe inlet increases the amount of shift for each discrete volume in a pipe.

The "heat flux" array is applied on the image rows as an exclusive-or (XOR) operation analogous to a Fourier conduction system. This helps to normalize the pixel data while providing key confusion.

Lastly, a user input "secret image" (analogous to a password in a traditional system) is XOR-ed with the intermediate image and a scalar value in the domain [0, 255] that is calculated from additional user inputs that are analogous to turbulence energy dissipation.

Results

Figure 2(a) shows the original "Lenna" plaintext image. This image has the horizontal and vertical correlations shown in Figures 2(b) and 2(c), respectively. Figure 2(d) shows the image histogram, the total number of pixel counts for each luminance value from 0-255, inclusive. A Fourier spectra is given by Figure 2(e). By observation of Figures 2(b) through 2(e), it is readily apparent that detectable visual information is present in the source image (Figure 2(a)).

Figure 3(a) is the "Lenna" image encrypted using the proposed technique. It is apparent by observing Figures 3(b) and 3(c) that no correlations may be observed in the encrypted image. That is, the original image pixel data has been adequately diffused throughout the entire image uniformly. From Figure 3(d) one may infer that image luminance data has been uniformly distributed over the domain—hiding any correlation that may be detected from the histogram alone. Figure 3(e) shows the Fourier spectra of the encrypted image. It is apparent that any "fingerprints" of the unencrypted image have been dispersed throughout the encrypted image.

References

[1] K. A. Al-Utaibi and E.-S. M. El-Alfy, "A bio-inspired image encryption algorithm based on chaotic maps," in *IEEE Congress on Evolutionary Computation*. IEEE, Jul 2010, pp. 1-6. [Online].

[2] M. Baptista, "Cryptography with chaos," *Physics Letters A*, vol. 240, no. 1-2, pp. 50-54, Mar 1998. [Online].

[3] B. Launder and D. Spalding, "The numerical computation of turbulent flows," *Computer Methods in Applied Mechanics and Engineering*, vol. 3, no. 2, pp. 269-289, mar 1974. [Online].

[4] T.-Y. Li and J. A. Yorke, "Period Three Implies Chaos," *The American Mathematical Monthly*, vol. 82, no. 10, pp. 985-992, Dec 1975. [Online].

[5] S. Liu, J. Sun, Z. Xu, and J. Liu, "Analysis on an Image Encryption Algorithm," *2008 International Workshop on Education Technology and Training and 2008 International Workshop on Geoscience and Remote Sensing*, Vol 1, Proceedings, pp. 803-806, 2009.

[6] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Physical Review Letters, vol. 64, no. 8, pp. 821-824, Feb 1990. [Online].

[7] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Systems Technical Journal*, vol. 28, pp. 656-715, 1949.