# IMAGE ENCRYPTION BASED ON CHAOTIC MAPS

**Jiri Fridrich**
**Department of Systems Science and Industrial Engineering &**
**Center for Intelligent Systems**
**SUNY Binghamton**
**Binghamton, NY 13902-6000, USA**

## ABSTRACT

In this paper, it is shown how to adapt certain invertible chaotic two-dimensional maps on a torus or on a square to create new symmetric block encryption schemes. The schemes are especially useful for encryption of large amounts of data, such as digital images or electronic databases. A chaotic map is first generalized by introducing parameters and then discretized to a finite square lattice of points which represent pixels or some other data items. Although the discretized map is a permutation and thus cannot be chaotic, it shares certain sensitivity and mixing properties with its continuous counterpart as long as the number of iterations remains small. It is shown that for the two-dimensional baker map the permutations behave as typical random permutations. The discretized map is further extended to three dimensions and composed with a simple diffusion mechanism. As a result, a block product encryption scheme is obtained. To encrypt an $N \times N$ image, the ciphering map is iteratively applied to the image. This paper is an extension of the work of Pichler and Scharinger [1, 2] who first introduced encryption schemes based on two-dimensional baker map.

## 1. INTRODUCTION

The idea of using chaos for data encryption is certainly not new and can be traced to the classical Shannon's paper [3]. Sloane [4] also points out the importance of chaos for generating random permutations in groups.
Chaotic maps have been utilized in several different ways in cryptography. Probably the most obvious application [5–11] of chaotic maps is to use one or more one-dimensional maps as pseudorandom number generators producing a binary stream which is then XOR-ed with the plain-text to produce the cipher-text. However, these schemes have been shown to produce weak ciphers [6, 8]. A different application of chaotic circuits to cryptography and communication is based on synchronized chaotic circuits [12–20]. However, these systems, too, have questionable security [21] and are more appropriate for covert communication.

The scheme presented in this paper, is a symmetric block encryption technique based on two-dimensional chaotic maps. Several unique properties distinguish it from other symmetric block encryption algorithms. The main features are: a variable key length, a relatively large block size (several kB or more), and a high encryption rate (1Mb unoptimized C code on a 60MHz Pentium). The cipher is based on two-dimensional chaotic maps, which are used for creating complex, key-dependent permutations. Unlike most today's symmetric encryption schemes, which rely on complex substitution rules while somewhat neglecting the role of permutations, the new cipher is based on complex permutations composed with a relatively simple diffusion mechanism. A good introductory text on encryption is [22].

Section 2 describes a five-step process of building a block cipher based on a two-dimensional chaotic map. The process of building a cipher is explained with the generalized baker map in Section 3. Since the security of the cipher lies in its permutation step, which is key-dependent, it is important to study the permutations as functions of the key. This is analyzed in Section 4 by comparing the number of cycles forming the permutations and their length with random permutations. It is shown that after several iterations, the map behaves as a typical random permutation. In Section 5, we discuss the relationship between discrete chaos and cryptosystems. The basic features of the chaos-based encryption scheme, its advantages and disadvantages, and future research directions are summarized in Section 6.

## 2. CREATING A CHAOS-BASED CIPHER

The process of developing a chaos-based cipher can be summarized as follows. First, a chaotic map is generalized by introducing parameters into the map. Geometrical arguments are often used at this stage. Then, the map is modified so that its domain and range are both the same square lattices of points (pixels, or some other general data items). The map is extended to three dimensions so that the values of the pixels (the gray levels) can be changed. A diffusion step is introduced by composing the generalized discretized map with a simple diffusion mechanism. Let us consider square images consisting of

**0-7803-4053-1/97/$10.00 © 1997 IEEE**

$N \times N$ pixels with $L$ levels of gray. The method for developing a cipher consists of the following five steps.

**1. Designing the basic map.** In this step, the mathematical form of a chaotic two-dimensional map $f$ which maps the unit square $I \times I$, where $I = [0, 1]$, onto itself in a one-to-one manner is chosen. There are a number of different chaotic maps which seem to be suitable for ciphering purposes. However, the only maps of interest are those which are simple so that the ciphering / deciphering phases can be performed quickly. The map should allow natural parametrization to create a short ciphering key with a large number of possible keys. Such maps are often described geometrically (e.g., the baker map, the cat map, the standard map, etc.).

**2. Generalized map.** In the second step, a set of parameters is introduced into the map to create a part of the ciphering key. If the basic map is described in geometric terms, the parametrization is usually straightforward. If it can be done in several different ways, the one which best suits the purpose of secure ciphering needs to be chosen. Two-dimensional chaotic maps will be characterized by a sequence of integers. Another parameter is the number of applications of the chaotic map.

**3. Discretizing.** This step consists of modifying the generalized map to account for the fact that an image is a finite lattice of points. The domain and range of the map is changed from the unit square $I \times I$ to the lattice $\{0, \ldots, N-1\} \times \{0, \ldots, N-1\}$ with $N$ equal to the number of pixels in one row. The discretized map $F$ takes each pixel and assigns it to some other pixel in a bijective manner (e.g., the discretized version is a permutation of pixels). The discretization must satisfy the following asymptotic property:

$$\lim_{N\to\infty} \max_{0\leq i,j<N} |f(i/N, j/N) - F(i,j)| = 0, \qquad (1)$$

where $f$ is the continuous basic map and $F$ is the discretized version.

**4. Extension to three dimensions.** After step 3, the cipher is just a permutation cipher. By extending the map to three dimensions, the pixel values are also modified and a good substitution cipher is obtained. This can be easily achieved with a very little increase in cipher complexity. A general procedure which can be applied to any two-dimensional map is designed. The cipher is so effective that only two applications of the three-dimensional map to an image consisting of a black square create a uniform histogram.

**5. Composing with a diffusion mechanism.** Since the chaotic map extended to three dimensions is a complicated substitution cipher with no diffusion properties, it is necessary to compose the map with some simple diffusion mechanism. Linear feedback registers with carry over [1, 2] or other simple nonlinear mechanisms can be used to achieve this goal. The resulting cipher is a product cipher with good diffusion and confusion properties.

## 3. CIPHERING USING BAKER MAP

The **baker map**, $B$, is described with the following formulas

$$B(x, y) = (2x, y/2) \qquad \text{when } 0 \leq x < ½$$

$$B(x, y) = (2x-1, y/2 + 1/2) \qquad \text{when } ½ \leq x \leq 1.$$

The map acts on the unit square as depicted in Figure 1. The left vertical column $[0, ½) \times [0, 1)$ is stretched horizontally and contracted vertically into the rectangle $[0, 1) \times [0, ½)$, and the right vertical column $[½, 1) \times [0, 1)$ is similarly mapped onto $[0, 1) \times [½, 1)$. The baker map is a chaotic bijection of the unit square $I \times I$ onto itself.

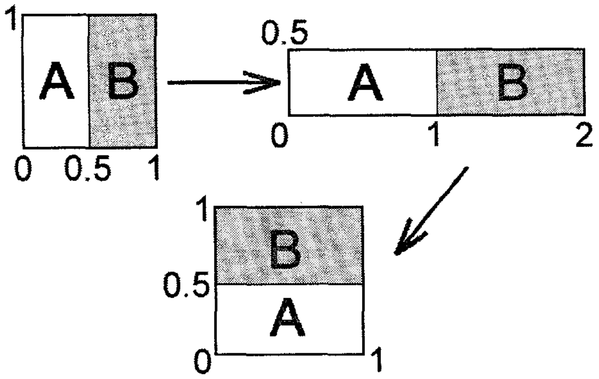

**Figure 1 The baker map**

The map can be generalized in the following way [1, 2]. Instead of dividing the square into two rectangles of the same size, the square is divided into $k$ vertical rectangles $[F_{i-1}, F_i) \times [0, 1)$, $i = 1, \ldots, k$, $F_i = p_1 + \ldots + p_i$, $F_0 = 0$ such that $p_1 + \ldots + p_k = 1$. The lower right corner of the $i$-th rectangle is located at $F_i$. The generalized baker map stretches each rectangle horizontally by the factor of $1/p_i$. At the same time, the rectangle is contracted vertically by the factor of $p_i$. Finally, all rectangles are stacked on top of each other. Formally,

$$B(x, y) = (\,(x - F_i)/p_i\,, p_i\,y + F_i\,)$$
$$\text{for } (x, y) \in [F_i, F_i + p_i) \times [0,1).$$

The generalized map inherits all important properties of the baker map such as sensitivity to initial conditions and parameters, mixing, and bijectiveness.

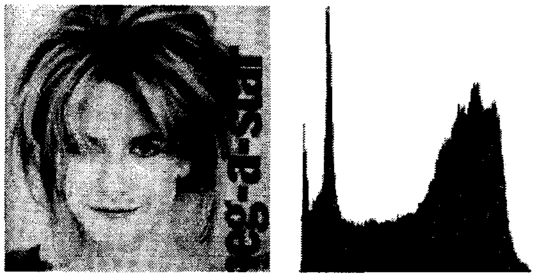

**Figure 2 Test image and its histogram**

Since an image is defined on a lattice of finitely many points (pixels), a correspondingly discretized form of the generalized baker map needs to be derived. In particular, the discretized map is required to assign a pixel to another pixel in a bijective manner. Since the discretized map is desired to inherit the properties of the continuous basic map, the discretized map should become increasingly close to the basic map as the number of pixels tends to infinity. This requirement is expressed mathematically with formula (1). Following the approach suggested by Pichler and Scharinger [1, 2] we define a sequence of $k$ integers, $n_1, \ldots, n_k$ such that each integer $n_i$ divides $N$, and $n_1 + \ldots + n_k = N$. Denoting $N_i = n_1 + \ldots + n_i$, $N_0 = 0$, the pixel $(r, s)$, with $N_{i-1} \leq r < N_i$ and $0 \leq s < N$ is mapped to

$$(q_i(r - N_i) + s \bmod q_i,\ (s - s \bmod q_i)/q_i + N_i),$$

where $q_i = N / n_i$. It is possible to justify this expression via symbolic dynamic using Bernoulli shifts in finite abelian groups [1, 2]. A geometric interpretation of this formula enables us to use an arbitrary combination of integers (e.g., not only divisors of $N$ are considered) which add up to $N$. For details, see [23].

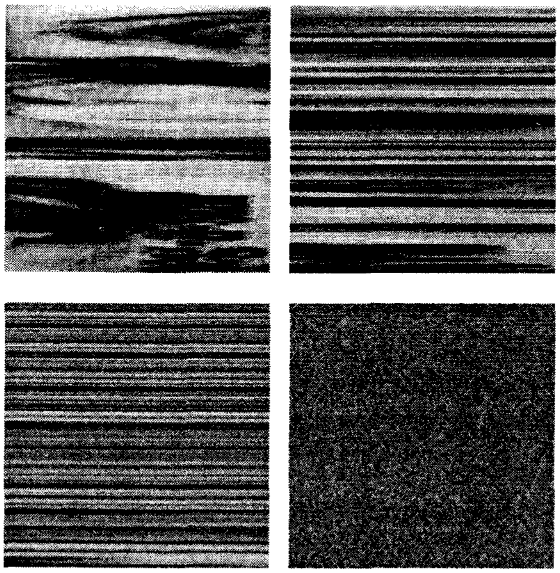

**Figure 3 Test image after applying the discretized baker map once, twice, three times, and eight times.**

The results of applying the discretized baker map to the test image shown in Figure 2 after 1, 2, 3, and 8 iterations are shown in Figure 3.

The discretized baker map is further extended to three dimensions in order to mix the gray levels. The following general procedure can be applied to any 2d map. We will map pixel $(i, j)$ with gray level $g_{ij}$ to $B(i, j)$ with gray level $h(i, j, g_{ij})$, which depends on both the old gray level and the position of the pixel. For this map to be invertible, $h$ needs to be one-to-one in the third variable. One possible form of $h$ satisfying this is $h(i, j, g_{ij}) = g_{ij} + h'(i, j) \bmod L$, where $L$ is the number of gray levels and $h'$ is an arbitrary function of $i$ and $j$. Since $B$ is invertible, it is easy to see that this 3d map will also be invertible. The resulting substitution cipher can create a random looking image with uniform histogram in only a few iterations. Starting with an image consisting of a black square, the histograms after one and two iterations are shown in Figure 4. Even though the histogram of a monochrome image is highly nonuniform, as few as two iterations of the 3d chaotic map create an almost uniform histogram.

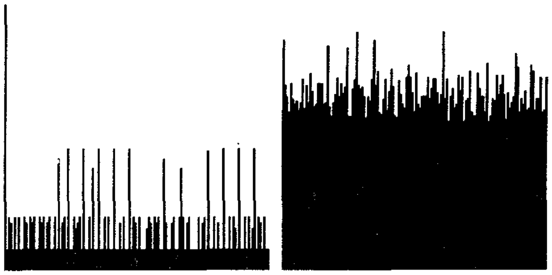

**Figure 4 Histogram of a black square after one and two applications of the 3d baker map with $h'(i,j) = i \cdot j$**

In order to achieve a complete diffusion with respect to changes to the key and the plain-text, we compose the 3d chaotic map with some simple diffusion mechanism. There are many ways one can implement a diffusion step into the scheme. Pichler and Scharinger [1, 2] take a product of the Bernoulli cipher with a maximal length linear feedback shift register with carry over. Their method also generates uniform histograms and, at the same time, achieves complete diffusion with respect to plain-text. We propose to apply a simple nonlinear feedback shift register. The diffusion is obtained by scanning the image by rows (starting, for example, in the upper left corner), and changing the gray levels according to the formula $g^*_{ij} = g_{ij} + G(g^*_{ij-1}) \bmod L$, $g_{0-1}$ = initial value. This procedure achieves complete mixing very quickly and also produces excellent results for complete diffusion – small changes to the key or the plain-text produce statistically independent cipher-texts. For details, see [23].

The ciphering key is formed by the parameters of the chaotic map, the number of applications of the map, the parameters of the gray level transformation $h$, and parameters of the diffusion part. The number of possible keys grows very rapidly with the number of pixels in the image. The parameters $n_1, \ldots, n_k$ of the baker map contribute to the total number of ciphering key by the factor of $2^{N-1}$.

## 4. STRUCTURE OF THE PERMUTATIONS

Each permutation can be uniquely represented as a collection of cycles. Permutations induced by the generalized discretized baker map have cryptographically strong properties. To see that, we calculated the average length of a cycle, and the average number of cycles and compared the values with those for a typical random permutation. The average length, $C(N)$, of a cycle in an $N \times N$ image is defined as the expected value of the number of iterations of the map necessary to bring a randomly chosen pixel back to its original position. It can be shown [24] that for a random permutation, $C(N) = (N^2 +1)/2$ and $cyc(N) = 2\ln(N) \pm 2\ln(N)$, where $cyc(N)$ denotes the number of different cycles. Computer experiments with 1000 randomly chosen keys of length between 10 and 15 for a square image 472 × 472 pixels give $C(N)$ = 111,115.7, $cyc(N)$ = 33.5. These values should be compared to random permutations with $C(N)$ = 111,392.5, $cyc(N)$ = 24.6. Since the standard deviation for $cyc(N)$ is 24.6, we can conclude that the permutations induced by the baker map behave as typical random permutations.

## 5. RELATIONSHIP BETWEEN CHAOS AND CRYPTOSYSTEMS

There appears to be a relationship between chaotic systems and symmetric block cryptosystems. Among other things, any good cryptosystem should:

1. Map plain-text to a random cipher-text. There should not be any patterns in the cipher-text, if the cryptosystem is good.

2. Be sensitive with respect to plain-text. This means that flipping one bit in the plain-text creates completely different cipher-text.

3. Be sensitive with respect to keys. This means that f via symbolic dynamic using Bernoulli shifts in finite abelian groups [1, 2]. A geometric interpretation of this lipping one bit in a key creates completely different cipher-text when applied to the same plain-text.

In addition to these requirements, it is a well known fact that virtually all symmetric block encryption methods are *iterative schemes* and work by iterating some basic encryption function several times. DES has 16 rounds, IDEA 8 rounds, LOKI 16 rounds, Blowfish 16 rounds, GOST 32, Khufu and Khafre 24. Almost all symmetric ciphers are based on an iterative scheme called Feistel network. Feistel network transforms a block $(L, R)$ according to the following invertible formula

$$L_{i-1} = R_i$$
$$R_{i-1} = L_i \oplus f(R_i, K_i),$$

where $f(.\ ,\ .)$ is an arbitrary function of two bit strings, and $K_i$ is the subkey derived from a passphrase for the $i$-th iterative step. The operation $\oplus$ is usually the bitwise XOR but could be some other operation. It is worth mentioning that many chaotic maps expressed in the form of a discrete mapping have the same structure as the Feistel network! For example, the standard map and the Hénon map [25] can be put into this form.

Now, let us list the basic properties of chaotic systems. A chaotic system is formed by some basic function $f$ which is iterated (repeatedly applied) on some set $X$. Any chaotic system should:

a) Be mixing. This means that the phase space $X$ should be randomly mixed by repeated action of $f$. A precise mathematical concept of mixing can be found, for example, in [25].

b) Be sensitive to initial conditions. This means that starting with a slightly modified initial state, one quickly obtains completely different states.

c) Most chaotic systems depend on some control parameters and exhibit sensitivity with respect to those parameters. This means that a slight change in the parameters will generally cause a drastic change in the properties of the chaotic map.

By comparing 1. with a), 2. with b), and 3. with c) it becomes very obvious that encryption and chaos exhibit remarkably similar features if we consider that plain-text corresponds to an initial condition, key corresponds to parameters, and the encryption function corresponds to $f$. However, there is one important difference between these two concepts. Cryptosystems work on finite sets, while chaotic systems only have meaning on a continuum, an infinite set. This is probably the main reason why the relationship between chaos and encryption went unnoticed for such a long time. One of the goals of our future research is to establish a formal relationship between chaos and cryptosystems, and use this connection to enrich both fields. Encryption would readily benefit because one could use a large number of powerful mathematical tools previously developed for nonlinear dynamic systems. For example, we could use the concept of Lyapunov number to quantify diffusion in cryptosystems. The minimal number of iterations for any given cryptosystem is usually estimated by the designers and there is no general method which would guide us as to how many iterations are actually needed to guarantee a secure cipher. For example, IDEA has 8 rounds, but it is generally accepted that as few as 6 or even 4 produce a safe cipher as well. Why the designers have chosen 8 and not 6? How can we justify the number of iterations in an encryption scheme? How many iterations are necessary for our chaos-based encryption method? The concept of Kolmogoroff entropy from the theory of dynamic systems might help us answer these questions. Kolmogoroff entropy measures the rate with which information about initial conditions is lost in the course of iterations. In addition to the applications stated above, we expect that a successful connection between encryption and discretized chaos would lead to new attacks for breaking symmetric ciphers and to new cryptanalytic techniques.

On the other hand, the impact of cryptanalytic theoretical tools in chaos theory can only be guessed right now. It seems that symbolic dynamics [26] would be the candidate number one for this type of application.

The main problem that needs to be solved is a correct generalization of chaos from a continuum to finite sets. Although the size of the sets will usually be of the order of $2^{64}$ or $2^{128}$ (the typical size of all possible encryption blocks), the sets are nevertheless finite. Any definition of chaos on finite sets should merge with the classical definition as the number of elements tends to infinity. This correspondence principle will be the guide of our research. One possible approach towards the definition of chaos on finite sets is using symbolic dynamics and the concept of randomness on finite sets. The latter topic has been extensively and successfully studied in the past [27].

## 6. CONCLUSION AND FUTURE DIRECTIONS

In this paper, it is shown how to adapt certain invertible chaotic two-dimensional maps on a torus or on a rectangle for the purpose of encryption. The map is first generalized by introducing parameters and then discretized to a finite rectangular lattice of points. Then the map is extended to three dimensions to obtain a more complicated substitution cipher. This cipher alone can turn plain-texts into random looking cipher-texts. Since the substitution cipher has no diffusion properties with respect to plain-text, it is finally composed with a simple diffusion mechanism. The resulting cipher appears to have good diffusion properties with respect to both the key and the plain-text. The properties of the permutations induced by chaotic maps are shown to correspond to typical random permutations. In particular, computer experiments with many different ciphering keys demonstrate that the average length of cycles and the average number of different cycles have values similar to those for random permutation.

The main features of the encryption scheme studied in this paper are: a variable key length, a relatively large block size (several kB or more), and a high encryption rate (1Mb unoptimized C code on a 60MHz Pentium). The cipher is based on two dimensional chaotic maps, which are used for creating complex, key-dependent permutations. Unlike most today's symmetric encryption schemes, which rely on complex substitution rules while somewhat neglecting the role of permutations, the new cipher is based on complex permutations composed with a relatively simple diffusion mechanism.

Future research directions will be directed to a more detailed study of security analysis of the proposed cipher. We plan to use standard crypt-analytic tools, such as differential and linear cryptography to further assure the safety and robustness of the cipher. Also, we intend to study other maps and their discretized forms. The generalized standard map, for example, provides a general framework for a whole new class of encryption schemes resembling in structure Feistel networks [22]. One of the major goals of our future effort is establishing a connection between discretized chaotic systems and encryption schemes. This would enable us to quantify diffusion and sensitivity with respect to key and the plain-text using concepts, such as entropy or Lyapunov exponents. In order to do that, an appropriate framework and definition of chaos on finite metric spaces needs to be established.

## 7. ACKNOWLEDGMENTS

The work on this paper was supported by Rome Laboratory, Air Force Material Command, USAF, under grant number F30602–96–1–0047. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation there on. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of Rome Laboratory, or the U. S. Government.

## 8. REFERENCES

[1] F. Pichler and J. Scharinger, "Efficient Image Encryption Based on Chaotic Maps." Johannes Kepler University, Linz, Austria, preprint, 1996.

[2] F. Pichler and J. Scharinger, "Ciphering by Bernoulli Shifts in Finite Abelian Groups." In: *Contributions to*

*General Algebra*, *Proc. of the Linz-Conference*, June 2–5, 1994.

[3] C. Shannon, "Communication Theory of Secrecy Systems." *Bell System Technical Journal*, **28**, pp. 656–715.

[4] N. J. Sloane, "Encrypting by Random Rotations," In: *Proceedings of the Workshop on Cryptography*, LNCS edited by G. Goos and J. Hartmanis, Burg Feuerstein, Germany, March 29–April 2, 1982, pp. 71–128.

[5] R. Matthews, "On the Derivation of a 'Chaotic' Encryption Algorithm," *Cryptologia*, **XIII**(1), Jan. 1989, pp. 29–42.

[6] D.D. Wheeler, "Problems with Chaotic Cryptosystems," *Cryptologia*, **XII**(3), 1989, pp. 243–250.

[7] T.Y. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A Secret Cryptosystem by Iterating a Chaotic Map," In: *Advances in Cryptology* - EUROCRYPT' 91, edited by D. W. Davies, LNCS 547, Springer–Verlag, 1991.

[8] E. Biham, "Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT' 91," In: *Advances in Cryptology* - EUROCRYPT' 91, edited by D. W. Davies, LNCS 547, Springer–Verlag, 1991.

[9] M.E. Bianco and D. A. Reed, *Encryption System Based on Chaos Theory*. US Patent No. 5,048,086, Sep. 10, 1991.

[10] V.A. Protopopescu, R. T. Santoro, and J. S. Tolliver, *Fast and Secure Encryption-Decryption Method Based on Chaotic Dynamics*. US Patent No. 5,479,513, Dec. 26, 1995.

[11] K.S. Deffeyes, *Encryption System and Method*. US Patent No. 5,001,754, Mar. 19, 1991.

[12] L.M. Pecora and T. Carol, "Synchronized Chaotic Signals and Systems", *Proceedings of ICASSP Conference*, San Francisco, Calif., Mar. 1992.

[13] T. Carol and L. M. Pecora, "Cascading Synchronized Chaotic Systems," *Physica D*, **67**, 1993, pp. 126–140.

[14] T. Carol and L. M. Pecora, *System for Producing Synchronized Signals*. US Patent No. 5,245,660, Sep. 14, 1993.

[15] K.M. Cuomo and A.V. Oppenheim, *Communication Using Synchronized Chaotic Systems*. US Patent No. 5,291,555, Mar. 1, 1994.

[16] K. Murali and M. Lakshmanan, "Transmission of Signals by Synchronization in a Chaotic Van der Pol-Duffing Oscillator," *Phys. Rev. E*, **48**(3), Sep. 1993, pp. R1624–R1626.

[17] L.J. Kocarev et al., "Experimental Demonstration of Secure Communications via Chaotic Synchronization," *International Journal of Bifurcation and Chaos*, **2**(3), Dec. 4 1992, pp. 709–713.

[18] Parlitz et al., "Transmission of Digital Signals by Chaotic Synchronization," *International Journal of Bifurcation and Chaos*, **2**(3), Dec. 4 1992, pp. 973–977.

[19] S. Papadimitriou, A. Bezerianos, and T. Bountis, "Secure Communication with Chaotic Systems of Difference Equations", *IEEE Trans. Comp.*, **46**(1), 1997, pp. 27–38.

[20] G.M. Bernstein and M.A. Lieberman, "Secure Random Number Generator Using Chaotic Circuits," *IEEE*, May 1989, pp. 0640–0644.

[21] K.M. Short, "Detecting and Extracting Messages from Chaotic Communications using Nonlinear Dynamic Forecasting", talk at The Fourth SIAM Conference on Applications of Dynamical Systems, Snowbird, May 18–22, 1997

[22] B. Schneier, *Applied Cryptography*. Wiley, New York, 1996.

[23] J. Fridrich, *Secure Image Ciphering Based on Chaos*. Final Technical Report, Rome Laboratory, New York, February 1997.

[24] W. Feller, *An Introduction to Probability Theory and Its Applications*. John Wiley&Sons, New York, 1957.

[25] E.A. Jackson, *Perspectives in Nonlinear Dynamics*. Cambridge University Press, Cambridge, 1991.

[26] Hao Bai-Lin, *Chaos II*. World Scientific, Singapore, 1990, pp. 27.

[27] D.E. Knuth, *The Art of Computer Programming*, Volume 2 (Seminumerical Algorithms), pp. 142. Addison–Wesley, Reading, Massachusetts, 1991