International Journal of Electronics and Communication Engineering.
ISSN 0974-2166 Volume 4, Number 2 (2011), pp. 217-223
© International Research Publication House
http://www.irphouse.com

A Novel 2D Cat Map based Fast Data Encryption Scheme

Swapnil Shrivastava

M.Tech., S.R.I.T., Jabalpur, M.P., India
E-mail: swapnilmtech@yahoo.in

Abstract

The security is an essential part of any communication system. Presently there are many types of encryption methods are available in symmetric and asymmetric key schemes because of long time requirement asymmetric schemes are not preferred for the large data encryption. Symmetric scheme is much better when compared for decoding time, in symmetric key the same key is used for both coding and decoding also in this scheme a digital signal is encrypted by relatively simple operations like EX-OR, hence for its necessary that the encryption sequence generated by the must have noise-like autocorrelation, cross-correlation, uniformity, attractors, etc. according to chaotic theory, chaotic sequences are best suited and they have all these properties. In this paper; first, we design and simulate a 2D cat mat using Matlab then using it as 1D stream generator for encryption Second, we show the a comparative study of the dynamical statistical properties obtained under simulation.

Keywords: Chaotic sequences generators, encryption, Cat map, security.

Introduction

Chaos has been widely studied in secure communications for both analog and digital, but in this paper we will focus only in digital chaotic systems, the chaotic sequences are preferred choice for encryption because of its property of generating the long non-repetitive random like sequences and dependency on initial states, which makes it very difficult to decode. The idea of using digital chaotic systems to construct cryptosystems has been extensively studied since 1990s, and attracts more and more attention in the last years. Chaotic output signal of chaotic generator is used for both confusion and diffusion operations in a cryptosystem. A Digital chaotic generator must full fill the following properties before it can be used in good cryptographic systems, 1) Equal numbers of ones and zeros during each period. 2) Long repeating period. 3) Uniform distribution of ones and zeros. 4) Zero correlation with delayed sequence.

From the chaotic theory it is known that not all non linear system can produce a good chaotic sequence hence the proper operating point selection must be done before using a system as chaotic generator this is not only true for analog but also for digital systems. In this paper we will study some methods of generating the chaotic sequences and then, we will do a comparative analysis of these methods in order to conclude by choosing the best one. This paper is organized as follows. The second paragraph is presenting some chaotic maps. The third part describes the proposed encryption technique. The fourth part presents some simulation results. Finally, some conclusions are drawn.

Chaotic Generators

A non linear system with properly selected operating parameters can be used as chaotic sequence generators.

Logistic map

The logistic map is perhaps one of the simples mathematical system showing many characteristics of the development of chaotic behaviour.

$$x_{n+1} = 1 - a.x_n^2 + y_n$$
$$y_{n+1} = b.x_n$$

This simple map, which was extensively studied by Feigenbaum, shows very intriguing behaviour when the value of **a** is increased. For **a** smaller than 0.75 the x-value quickly converges to a single value (fixed point). As **a** is increased above 3 the value of x alternates between two values (2-cycle). As **a** is increased further the period is doubled: it goes into a 4-cycle. Such period doublings keep occurring when **a** is increased futher until the behaviour becomes completely chaotic. Feigenbaum found that this type of behavior, the development of chaos - occurs in many systems in a similar way.

2D Cat Map

A 2D Cat map is first presented by V.I. Arnold in the research of ergodic theory. Let the coordinates of positions of pixels in an image are P = {(x, y) | x, y = 1, 2, 3, . . ., N}, a 2D Cat map with two control parameters is as follows:

$$x' = (x + ay)\mathrm{mod}(N)$$
$$y' = (bx + (ab+1)y)\mathrm{mod}(N)$$

Where, a, b are control parameters which are positive integers and (x’, y’) is the new position of the original pixel position (x, y) of N x N plain-image when Cat map is applied once to the original. Cat map permutes/shuffles the organization of pixels of plain-image by replacing the position of the image pixel points with new coordinate. After several iterations, the correlation among the adjacent pixels is disturbed completely and the image appears distorted and meaningless. But after iterating many times it will return the original image i.e. the Cat map is periodic.

2D Standard Map

An invertible discretized 2D standard map with a random scan couple (r_k, r_y) given by

$$\begin{cases} x_{k+1} = (x_k + y_k + r_x + r_y) \bmod N, \\ y_{k+1} = \left(y_k + r_y + K_c \sin \frac{2\pi x_{k+1}}{N} \right) \bmod N, \end{cases}$$

where (x_k, y_k) and (x_{k+1}, y_{k+1}) is the original and the corresponding permuted bit position of an N × N matrix, respectively. The standard map parameter K_c is a positive integer.

2D Baker's Map

In dynamical systems theory, the baker's map is a chaotic map from the unit square into itself. It is named after a kneading operation that bakers apply to dough: the dough is cut in half, and the two halves are stacked on one-another, and compressed. (The word baker is used to denote the profession and not a name.) The baker's map can be understood as the bilateral shift operator of a bi-infinite two-state lattice model. The baker's map is topologically conjugate to the horseshoe map. In physics, a chain of coupled baker's maps can be used to model deterministic diffusion. The Poincare recurrence time of the baker's map is short compared to Hamiltonian maps. As with many deterministic dynamical systems, the baker's map is studied by its action on the space of functions defined on the unit square. The baker's map defines an operator on the space of functions, known as the transfer operator of the map. The baker's map is an exactly solvable model of deterministic chaos, in that the eigenfunctions and eigenvalues of the transfer operator can be explicitly determined.

The folded baker's map acts on the unit square as

$$S_{\text{baker-folded}}(x,y) = \begin{cases} (2x, y/2) & \text{for } 0 \le x < \frac{1}{2} \\ (2-2x, 1-y/2) & \text{for } \frac{1}{2} \le x < 1. \end{cases}$$

Proposed Algorithm

The proposed image encryption algorithm has two major steps. Firstly, the generations of chaotic sequence as by using 2D cats map and then EXOR-ing the generated sequence with data stream.

Step 1: Firstly a binary matrix I of size NXN is generated with equal probability of ones and zeros and with uniform distribution of ones and zeros.

Step 2: Decide the initial condition (p, q, n, rx, ry, etc.) for cats map as encryption key.

Step 3: After each iteration of Cat map take I(x, y) bit as output for encryption of data stream.

Step 4: Perform EXOR operation between data stream and chaotic stream.

Step 5: The original data stream can be recovered successfully by applying the proposed algorithm in reverse order.

Simulation Results

The proposed encryption algorithm is implemented in MATLAB for computer simulations. We take a random data stream of 10^4 bits in size for experimental purposes. The original data and its statistical properties are shown in figure 1,2 and 3. The initial conditions and system parameters are: p = 2, q = 3, rx = 3, ry = 7, n = 5. The result of proposed cat map based data encryption scheme for above mentioned conditions is shown in figure 4 and the corresponding chaotic sequence properties of the same scheme is shown in figure 7 and 8. However, the result of proposed encryption algorithm for n = 5 is shown in Figure 4. It is clear from the statistical analysis of data before and after encryption shown in figure 5 and 6 that the proposed scheme provides more distortion and more uncorrelated adjacent bits in resultant encrypted data stream. Moreover, as we can see in Figure 4 that the distribution of the bits encrypted data stream is fairly uniform and much different from the distribution of the original data shown in Figure 1 i.e. the occurrence of consecutives zeros and ones in the encrypted data has greatly reduces . Hence, the encrypted data doesn't provide any information regarding the distribution of original values to the attacker. As a result the proposed algorithm can resist any type of statistical attacks.

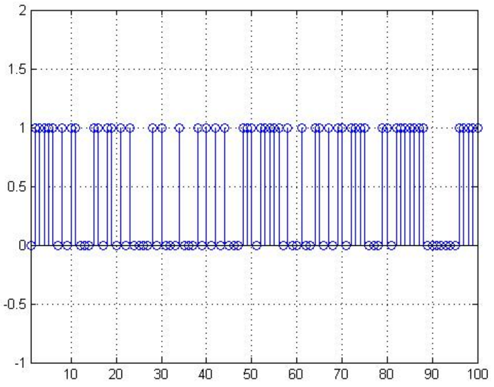

Figure 1: Original data stream.

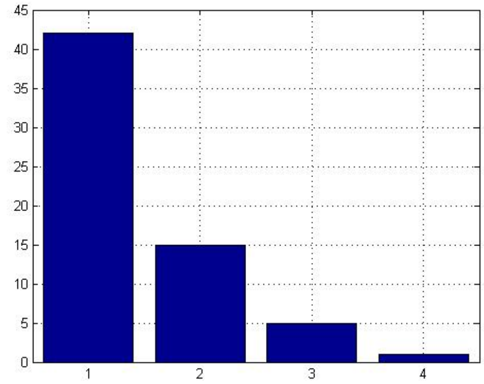

Figure 2: Occurrences of successive zeros.

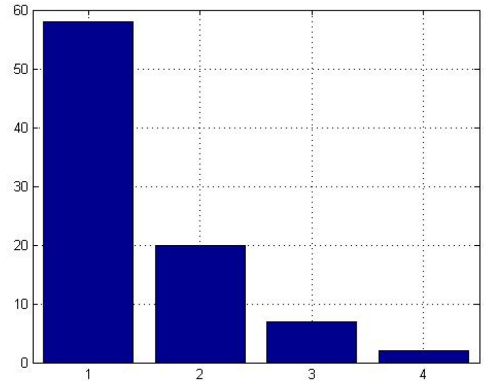

Figure 3: Occurrences of successive ones.

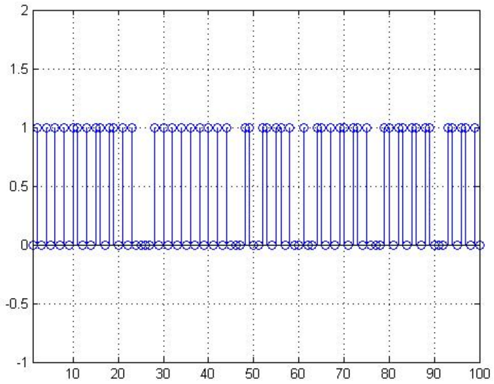

Figure 4: Encrypted data stream.

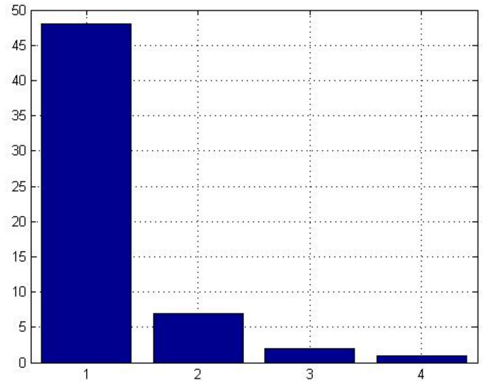

Figure 5: Occurrences of successive zeros after encryption.

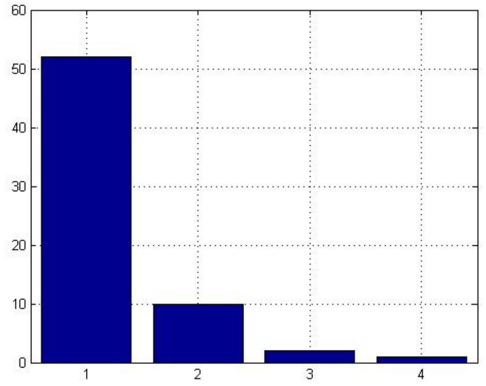

Figure 6: Occurrences of successive ones after encryption.

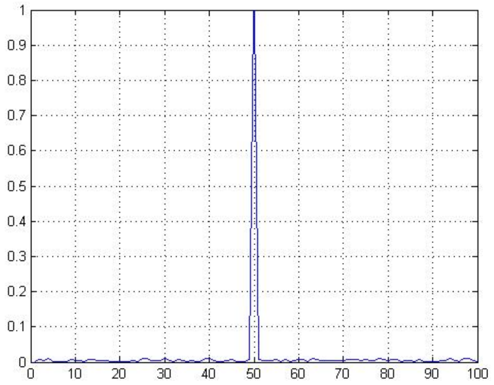

Figure 7: Correlation of Chaotic Sequence.

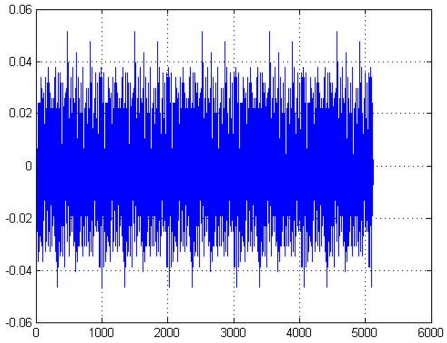

Figure 8: Cross-correlation of Chaotic Sequence.

Conclusion

In this paper, we presented a chaotic algorithm for encryption and decryption of data stream. The algorithm is based on the concept of randomness and long repetition time period of chaotic sequences can be used for changing the values of the data bits. To generate the encrypting stream a 2D Cat map based scheme is proposed, in which the 8x8 binary matrix is shuffled by 2D Cat map, and a stream of bits is generated by picking bits from certain location. Moreover, the control parameters of shuffling map can be selected separately as key for encryption and decryption. All the simulation and experimental analysis show that the proposed encryption system has (1) Large key space, (2) Sensitivity to secret keys, and (3) has low correlation coefficients close to the ideal value 0. Hence, we can say that all the analysis prove the security, effectiveness and robustness of the proposed encryption algorithm.

References

[1] S. Li, G. Chen, and X. Zheng, “Chaos-based encryption for digital images and videos,” in Furht B and Kirovski D (Eds.), Multimedia Security Handbook, Ch. 4, pp.133-167, CRC Press, 2005.

[2] T. Xiang, K. W. Wong, and X. Liao, “A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map,” Phys. Lett. A 364, pp.252-258, 2007

[3] Chengqing Li, Shujun Li, Gonzalo Alvarez, Guanrong Chen and Kwok_Tung Lo. “Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations”. Physics Letters A, 2007.

[4] Luiz P.L de Oliveira and M. Sobottka, “Cryptography with chaotic.

[5] Predrag Cvitanović, Roberto Artuso, Ronnie Mainieri, Gregor Tanner, Gabor Vattay, Niall Whelan and Andreas Wirzba, "Chaos: Classical and Quantum", ChaosBook.org version12.3, Sep 30 2008. mixing,” Chaos, Solitons & Fractals , vol. 35, pp. 408-419, 2008.