An efficient chaos-based chaotic maps using block encryption ciphers method

D.Lakshmi Prabha
Dr.R.V. Arts and Science college
karamadai, Coimbatore

Abstract

A chaotic map is first generalized by introducing parameters and then discretized to affnite square lattice of points which represent pixels or some other data items. Conventional cryptographic methods are used to scramble the message signal. Simulation results based on a typical chaotic system; namely, Chua's oscillator, are provided. Chaotic maps have good potential for information encryption. In this paper, a block cipher based on the chaotic standard map is proposed, which is composed of three parts: a confusion process based on chaotic standard map, a diffusion function, and a key generator. The parameter sensitivity of the standard map is analyzed, and the confusion process based on it is proposed. A diffusion function with high diffusion speed is designed, and a key generator based on the chaotic skew tent map is derived. Some cryptanalysis on the security of the designed cipher is carried out, and its computational complexity is analyzed. We present several chaos based ciphers. Using the well-known principles in the cryptanalysis we show that these ciphers do not behave worse than the standard ones, opening in this way a novel approach to the design of block encryption ciphers. In this secure communication scheme, the transmitted signals are divided into small time frames. In each time frame, the synchronization impulses and the scrambled message signal are embedded.

Keyword: ***Continuous cryptographic function, impulsive control, Block encryption ciphers, chaos.***

Introduction

With the desirable properties of ergodicity and high sensitivity to initial conditions and parameters [1], chaotic maps are very suitable for various data encryption schemes. In particular, chaotic maps are easy to be implemented by microprocessors and personal computers. Therefore, chaotic cryptosystems generally have high speed with low cost, which makes them better candidates than many traditional ciphers for multimedia data encryption. Early chaos-based cryptosystems, developed in the last decade, modulate messages with chaotic signals generated from continuous-time chaotic dynamic systems. This kind of cryptosystems depends heavily on the synchronization of two chaotic systems [2]. Although this approach can be directly used for analog devices such as walkie-talkies, it suffers from its poor noise performance and weak synchronizability: if the synchronization of the cryptosystem is robust, then it is vulnerable to controlled-synchronization type of attacks; but if not, then even the receiver may easily lose synchronization thereby leading to the failure of message recovery. There are some other types of chaotic cryptosystems, most of which transform plaintext directly. And they are often classified into two types: chaotic stream cryptosystems and chaotic block cryptosystems. In chaotic stream cryptosystems, a key stream is produced by a chaotic map, which is used to encrypt a plaintext bit by bit.

A chaotic block cryptosystem, on the other hand, transforms a plaintext block by block with some chaotic maps. For example, a cryptosystem based on the chaotic gradient tent map was constructed in [7], and the one based on the modified baker map was suggested in [8]. These cryptosystems apply chaotic maps repeatedly, which guarantees the randomness of the encrypted data. Their security is determined by the properties of the chaotic maps and the realization of the encryption scheme. Notably, these cryptosystems often include digital data and analog data at the same time, which make the m rely heavily on the machine_s precision. Thus, the machine_s precision has to be considered in order to keep the decryption process symmetric to the encryption one, which decreases the speed of the encryption or decryption process. In order to avoid the shortcomings of floating-point computing, some new cryptosystems based on discretized chaotic maps have been proposed. The core problem is how to obtain good discretized chaotic maps. Generally, chaotic maps are discretized by rounding the floating data according to the computer_s resolution. As a result, these chaotic cryptosystems depend on the mathematical properties of the corresponding continuous chaotic systems [9,10]. For example, a cryptosystem was proposed in by directly discretizing the 2-D baker map, and the relationship between the original map and the discretized map was then discussed in. A cryptosystem based on the discretized tent map was proposed in, in which, the discretization process avoids floating-point computing, increases the encryption speed significantly and is therefore suitable for large-volume data encryption in real-time. For cryptosystems, Shannon defined the ideal security, perfect security and computational security, respectively. A cryptosystem is regarded as having ideal security if the difficulty of ciphertext-only attack equals to the difficulty of brute-force attack. In cryptosystems with ideal security, a ciphertext is uniformly and randomly distributed, which prevents any attack. However, this kind of ideal cryptosystem does not exist in practice, so it is not useful for real design.

A cryptosystem is regarded as having perfect security if the ciphertext is independent of the plaintext, which means that the ciphertext provides no help to attackers. Compared with the ideal security, perfect security is easier to be realized theoretically, but it is still difficult to be applied in practice. Shannon believed that, in practice, the security of a cryptosystem depends on its computational complexity. If a cryptosystem is not ideally secure, but there is only one solution to it, and any other solutions require very high computational complexity, then the cryptosystem is regarded as computationally secure. Many cryptosystems are constructed based on high computational security, such as DES, IDEA, NSSU, etc., which are all implemented through confusion and diffusion processes, and are strengthened by increasing the loop time.

2. Background Works

Bianco et al. [1991, 1994] use the logistic map to generate a sequence of floating point numbers, which is then converted to a binary sequence which is XOR-ed with the plain-text. The parameter of the logistic map together with the initial condition form part of the ciphering key. The conversion from floating point numbers to binary values is done by choosing two disjoint interval ranges (not necessarily covering the whole unit interval) representing 0 and 1. The authors claim that this irreversible process makes it impossible to recover the original values. However, it is a well-known fact from symbolic dynamics that when a chaotic orbit is converted to a sequence of symbols | sets from some partition | it may be possible to calculate the initial condition with a much better accuracy than the size of the partition sets [Fridrich, 1995a, 1995b, 1997a].

The fact that this method is based on floating point arithmetic constitutes a possible disadvantage because this makes it machine dependent, and care needs to be exercised when implementing the schemes in software. Also, while for most common chaotic maps there are numerous exact results guaranteeing aperiodic, chaotic sequences for parameters from a set of nonzero Lebesgue measure, we cannot directly transfer the results to computer approximations. It has been pointed out by Jackson [1991] andWheeler [1989] that computer implementations

of chaotic maps can exhibit surprisingly different behavior, e.g. very short cycles, depending on the particular numerical representation.

As discussed above, virtually all today's chaos based software encryption techniques use the one time pad. However, one time pad is not suitable for encryption of large amounts of data, such as digital imagery, electronic databases and archives. The scheme presented in this paper, is a symmetric block encryption technique based on two-dimensional chaotic maps. Possible advantages of the proposed scheme over other available encryption schemes are discussed below. A good introductory text on encryption is [Schneier, 1996].

It is a better idea to encrypt large data _les with private-key symmetric block encryption schemes. Although advances in crypt-analytic techniques and quantum computing threaten symmetric encryption schemes as well [Brassard, 1997], those schemes can provide a more stable framework with a higher degree of security and are certainly much faster than public-key schemes. Today's most common block encryption scheme, the Data Encryption Standard, DES, was designed for hardware implementation and software implementation is relatively slow.

3. Computational And Complexity Analysis

Compared with traditional block ciphers such as DES, IDEA and NSSU, the proposed chaos-based cryptosystem has some distinct properties. Firstly, the plaintext size of the chaos-based cryptosystem is not fixed. The bigger the size of the plaintext matrix, the more difficult the brute-force attack, and the more secure the cryptosystem. This advantage makes it suitable for large-volume data encryption such as image, audio and perhaps also video data. Secondly, the confusion process and diffusion process are controlled completely by the users (via the user keys), so they act more securely as compared to the fixed confusion and fixed diffusion processes used in traditional ciphers. Thirdly, the confusion and diffusion processes are known to all users, so the encryption process is clear to them without any possibility of being trapped like the S-boxes in DES. What’s more, the encryption process and decryption process are symmetric, and easy to be realized, which makes it suitable for multimedia encryption.

$$P_{i+1} = C_i(P_0 = P; i = 0, 1, \ldots, m-1), \text{-}(1)$$

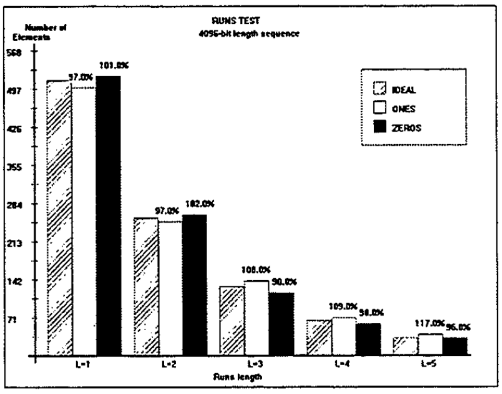
$C_i = D_e(M_i,K_{di}) = D_e(C^n{}_e\ (P_i,K_{ci}),K_{di})$ -(2)

$C_{i+1} = P_i(C_0 = C;\ i = 0, 1, . . . ,m-1)$, -(3)

$P_i = C^n{}_d(M_i,K_{ci}) = C^n{}_d(D_d(C_i,K_{di}),K_{ci})$ -(4)

The close relationship between chaos and cryptography makes chaos based cryptographic algorithms as a natural candidate for secure communication and cryptography chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power etc.

4. Result Analysis



We further perform a comparison of the randomness of the signal using the NIST-STS and tabulate the results for the various tests in Table 8. We see that in most cases the quasigroup block cipher with CBC randomizes the input waveform much more than AES256 does, especially in the case of Fast Fourier Transform (FFT) tests.

5. Conclusion

In this paper, the basic properties of the discretized chaotic standard map have been carefully analyzed, including the parameter sensitivity and computational complexity. Some means to enhance the chaotic maps performance in data permutation have been suggested. The map is first generalized by introducing parameters and then discretized to affinite rectangular lattice of points. Then the map is extended to three dimensions to obtain a more complicated substitution cipher. This cipher alone can turn an arbitrary plain-text into random looking cipher-text. This is utilized for constructing a nontraditional random number generator. 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 the Baker map are shown to correspond to a typical random permutation. In particular, computer experiments done for the Baker map 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. Based on the improved standard map, a block cipher has been designed and presented for encrypting large-volume data sets. It is composed of improved chaotic confusion, diffusion, and key generation. Both theoretical analysis and experimental results show that the proposed cryptosystem has satisfactory security and can be implemented efficiently, thus may provide a choice for multimedia encryption applications.

Reference

[1] Kotulski Z, Szczepariski J. Discrete chaotic cryptography (DCC). In: Proc NEEDS97.

[2] Kapitaniak T. Controlling chaos, theoretical and practical methods in non-linear dynamics. London: Academic Press; 1996.

[3] Alvarez G, Montoya F, Romera M, Pastor G. Breaking parameter modulated chaotic securecommunication system. Chaos, Solitons & Fractals 2004;21:783–7.

[4] Yang T. A survey of chaotic secure communication systems. Int J Comput Cognit 2004;2:SI-130.

[5] Kohda T, Tsuneda A. Stream cipher systems based on chaotic binary sequences. SCIS96-11C, January 1996.

[6] Lu HP, Wang SH, Hu G. Pseudo-random number generator based on coupled map lattices. Int J Modern Phys B 2004;18(17–19): 2409–14.

[7] Habutsu T, Nishio Y, Sasase I, Mori S. A secret key cryptosystem by iterating chaotic map. Lect Notes Comput Sci 1991;547:127–40.

[8] Tsueike M, Ueta T, Nishio Y. An application of two-dimensional chaos cryptosystem. Technical Report of IEICE, NLP96-19, May 1996 [in Japanese].

[9] Percival I, Vivaldi F. Arithmetical properties of strongly chaotic motions. Physica D 1987;25(1–3):105–30.

[10] Scharinger J. Kolmogorov systems: internal time, irreversibity and cryptographic applications. In: Dubois D, editor. Proc AIP Conference on Computing Anticipatory Systems, vol. 437. Woodbury, NY: American Institute of Physics; 1998.

D.Lakshmi Prabha: She has completed her B.Sc(ComputerScience)at Pionner college of arts and science coimbatore, Bharathiar University. and M.Sc(Information Technology) at S.N.R & Sons College Coimbatore Bharathiar University. She has 8 months of experience working in Dr.R.V. Arts and Science college,karamadai. Area of interest is networking.