International Journal of Electronics Engineering, 3 (2), 2011, pp. 189–194

Review on Chaotic Sequences Based Cryptography and Cryptanalysis

Mina Mishra[1] & V. H. Mankar[2]

[1]*Ph.D Scholar (Electronics & Telecommunication), Nagpur University, Maharashtra, India*
E-mail: minamishraetc@gmail.com

Senior Faculty, Department of Electronics Engineering, Government Polytechnic Nagpur, Maharashtra, India,
E-mail: mvhmankar@gmail.com

Abstract: This literature review glances at the research that has been published in the area of chaos cryptography along with cryptanalysis of chaotic cryptosystem. It compares and contrasts the work done in different research papers towards the designing and cryptanalysis of chaotic cryptosystem for the validity of cryptosystems and improvement in encryption techniques. This review analyzes the role that chaotic cryptosystem has played and will play in the future relative to the security. By reviewing the papers, it is the objective to design a number of secured cryptosystem based on different families of chaotic sequences using various encryption techniques. The work can arrive with more efficient and robust chaotic cryptosystem so as to provide data security, privacy and to preserve the future of network security and prevail secured communication networking.

Keywords: Chaotic cryptosystem, Cryptanalysis, Chaotic Sequences, Chaotic maps, Network Security.

1. INTRODUCTION

Cryptography is the science of protecting the privacy of information during communication under private conditions. In the new era of information technology and rapid growing of computer network communications, cryptography assumes special importance. Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos [1] is another paradigm, which seems promising and challenging. Chaos originated from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. The chaotic behavior is an unpredictable behavior of a nonlinear system, which apparently looks random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes.

In reviewing the papers which has already been published with regard to the designing and security analysis of chaotic cryptosystem, it is found that chaotic communication systems have been updated to different generation [2]. The first generation developed in 1993 known as additive chaos masking and chaotic shift keying. The second generation proposed during 1993 to 1995 known as chaotic modulation. This generation used two different ways to modulate message signals into chaotic carriers. The first method called chaotic parameter modulation used message signals to change parameters of the chaotic transmitter. The second method called chaotic non-autonomous modulation used the message signal to change the phase space of the chaotic transmitter. The second generation improved the degree of security to some degree but was still found unsatisfactory. The third generation, with the purpose of improving the degree of security to a much higher level than the first two generations, is called as generation of chaotic cryptosystem.

2. MODERN APPROACHES TO CHAOS CRYPTOLOGY

2.1. Chaotic Cryptography

Principles of Chaos theory have been used in Cryptography which led to the development of number of new techniques of encryption method of text, Image, Watermarking, etc. Chaotic Cryptography is a field which provides unlimited opportunities of developing algorithms of Ciphers using 1-D, 2-D and Multidimensional Chaotic Maps. New methods of generating Binary number Sequence, Pseudo random Generators have been developed. The possibility of using Chaos in any field have been studied and invented by many Scholars.

Eng. Bogdan Cristea, *et.al* [3] have analyzed the possibility of using chaos theory in cryptography and presented two examples of cryptographic algorithms that utilize nonlinear dynamical systems with chaotic behavior. Cristian-Iulian, *et.al* [4] have presented some aspects regarding the chaos based cryptography stage. The essence of the theoretical and practical efforts which are done in

this new field have been represented by the idea that chaos-based cryptosystem is capable to have similar performances regarding the classic methods based on computational techniques. Muhammed Razel, *et.al* [5] has described chaos from historical point of view, in order to understand motivation behind this science. The earliest form of cryptography has been discussed and then they switched over to current modern forms of cryptography. David Arroyo, *et.al* [6] have analyzed the use of the logistic map for cryptographic applications. The most important characteristics of the logistic map have been shown in order to prove the inconvenience of considering this map in the design of new chaotic cryptosystems. Elena Dubrova, *et.al* [7] have proposed a Non-Linear Feedback Shift Registers (NLFSRs) that was as an alternative to Linear Feedback Shift Registers (LFSRs) for generating pseudo-random sequences for stream ciphers. Vinod Patidar, *et.al* [8] have proposed a novel pseudo random bit generator (PRBG) based on two chaotic standard maps running side-by side and starting from random independent initial conditions. The pseudo random bit sequences generated by comparing the outputs of both the chaotic standard maps. They have also presented the detailed results of the statistical testing on generated bit sequences. Dongmei Wu, *et.al* [9] has realized a Non-feedback chaos control of logistic map by means of periodic parameter perturbations. The feasibility of this scheme has been proved by bifurcation diagram and Lyapunov exponent method, and the control parameters were obtained. Numerical simulations have shown that as long as the proper intensity and periods of periodic perturbation is being chosen, the system can be controlled from chaos to the steady periodic orbit rapidly.

2.2. Message-embedding Scheme

Different Schemes of using chaotic systems in designing Chaotic ciphers have been developed since the origin of Chaos in Cryptography. Message-embedded is the scheme of third generation also known as generation of chaotic ciphers.

Floriane Anstet *et.al* [10] has compared two encryption schemes, the standard Stream cipher and a so-called message embedded cryptosystem. The comparison has been based on two main aspects. The first aspect deals with the synchronization of the time-varying keys at the transmission and reception side respectively. Amigo, *et.al* [11] have presented in their paper an attempt to handle the situation which arises out to the requirement of the design of chaotic cryptosystem which results to empirical approaches with trial and error setting.

2.3. Various Chaotic Text Encryption Technique

The advancement and development in constructing Text Chaotic cipher using 1-D and 2-D and multi-dimensional chaotic maps have been evolved with time.

Rhouma, *et.al* [12] have proposed a new cryptosystem that is faster and presented a uniform distribution in his cipher text. To increase the security, they uses the logistic map and a 3-dimensional piecewise linear chaotic map in the generation of the associations tables. Shih-Liang Chen *et.al* [13] have proposed a new chaotic map, Variational Logistic Map (VLM), modified from logistic map to be used in secure communication. Compared with classical logistic map, VLM has large parameter space without windows and can be implemented at low hardware cost. Luiz P.L. de Oliveira, *et.al* [14] have proposed a cryptosystem based on one-dimensional chaotic maps defined in the interval (0,10) for a positive integer parameter p, is a topological conjugacy between G and the shift map r on the space R of the sequences with 10 symbols. There are three advantages in comparison with the recently proposed cryptosystem based on chaotic logistic maps. Shujun Li *et.al* [15] have proposed a chaotic encryption scheme, which is based on a kind of computerized piecewise linear chaotic map (PWLCM) realized in finite computing precision and they have pointed out that Zhou's encryption scheme is not secure enough from strict cryptographic viewpoint. Kwok Wo Wong, *et.al* [16], have presented an algorithm for embedding compression in the Baptista-type chaotic cryptosystem. The lookup table that has been used for encryption was determined adaptively by the probability of occurrence of plaintext symbols. As a result, more probable symbols will have a higher chance to be visited by the chaotic search trajectory.

V. Guglielmi, *et.al* [17], has proposed two different discrete-time cryptosystems based on two-dimensional noninvertible maps. Chaotic attractors being thought of as pseudo-random generators, the key streams are some trajectories of the maps, whereas the cipher key is given by the initial conditions. They have proposed to use two-dimensional noninvertible maps presenting chaotic dynamics for encryption. Ing. Rostislav Hucka, et.al [18] has described how to create a ciphering algorithm, which is able to use long keys and variable key length. Discrete chaotic maps are effective way to encrypt and decrypt data. Designed algorithm was simple and offered good performance and reasonable security. Ercan Solak , *et.al* [19] have recently proposed, an encryption algorithm based on two-dimensional discretized chaotic maps. They have analyzed the security weaknesses of the proposal. Using the algebraic dependencies among system parameters, they have showed that its effective key space can be shrunk. They have also demonstrated a chosen- ciphertext attack that reveals a portion of the key. M. Kiran Kumar, *et.al* [20] has put forward a safe mechanism of data transmission to tackle the security problem of information which is transmitted in Internet. They have proposed a new technique on matrix scrambling which has been based on random function, shifting and reversing techniques of circular queue and gives statistical analysis, sequence random analysis, and sensitivity analysis to plaintext and key on the proposed

scheme and has shown that the new scheme has a very fast encryption speed and the key space was expanded and it could resist all kinds of cryptanalytic, statistical attacks, and especially chosen plaintext attack.

S. Nandi, *et.al* [21] has dealt with the theory and application of Cellular Automata group of even permutations which in turn is a subgroup of the permutation group. These functions have been implemented with a class of programmable cellular automata (PCA) built around rules 51, 153, and 195. Further, high quality pseudorandom pattern generators built around rule 90 and 150 programmable cellular automata with a rule selector (Le. combining function) has been proposed as running key generators in stream ciphers. Both the schemes have provided better security against different types of attacks. Jong-Seon No, *et.al* [22], has constructed a sets of Kasami and No sequences as a family constructed from m-sequences. New optimal families of binary sequences have been constructed from the Legendre sequences of Mersenne prime period. Maria de Miguel, *et.al* [23] have exposed the capacities that make elliptic curve cryptography the most suitable one to he implemented in environments with several constraints related to processor speed, bandwidth, security and memory and have analyzed several elliptic curve cryptosystems with other public key ones. Tommaso Addabbo, *et.al* [24] have formulated Nonlinear Congruential Generators (NLCGs) based on the digitized Rényi chaotic map and it has been considered for the definition of hardware-efficient Pseudo Random Number Generators (PRNGs). In detail, a theoretical result is being provided about the periodicity of the output sequences generated by the proposed NLCGs. Safwan El Assad, *et.al* [25] have designed and implemented under Matlab/ Simulink some efficient digital chaotic generators for data encryption/decryption process. Some of these generators (Logistic, PWLCM, Frey) are known, the others x cos(x), x exp [cos (x)], 2-D Tmap) are proposed. A number of designed generators contain cascaded layer to improve the statistical properties of the generated sequences. This technique increased the orbit cycle length.

Xianfeng Guo, *et.al* [26] have studied the security of the new encryption scheme and reports the following findings: (1) the sub-keys of any ciphertext can be obtained by using only two chosen cipher texts; (2) the underlying chaotic key stream sequence can be reconstructed as an equivalent key by some chosen plaintext and cipher text pairs. Furthermore, they have suggested a remedial improvement, which avoids the flaws while keeping all the merits of the original cryptosystem. Hans Dieter Schotten, et.al [27] have compared the peak and average correlation properties of binary families derived from 'Z4-linear' families of quadriphase sequences to the results for well-known 'linear' families. They have shown that these families have remarkably better periodic peak correlation parameters than 'linear' families but an improvement of the average mean-square correlation properties has not been found. A construction method based on linear optimization has been described by them which results in families with low average interference parameters. Feng Bao [28] has shown that Cellular automata provide simple discrete deterministic mathematical models for physical, biological, and computational systems. Despite their simple construction, cellular automata are capable of complicated behavior and to generate complex and random patterns. There have been constant efforts to exploit cellular automata for cryptography since the very beginning of the research on cellular automata. Muhab U, *et.al* [29] have described a single key stream cipher system based on one dimensional cellular automata random number generator with evolution. The robustness of the scheme against cryptanalytic attacks is being discussed and it has been shown that cryptanalysis required an exponentially growing amount of computational resources by them and gave a simple avalanche effect analysis to assess the cryptographic strength of the cipher. Petre Anghelescu, *et.al* [30] have presented a hardware implementation in a FPGA circuit of an efficient encryption algorithm based on hybrid additive programmable cellular automata (HAPCA). They have presented a novel approach for a high-speed encryption system prototyped using a single FPGA.

Ping Zhou, *et.al* [31] have applied chaotic encryption algorithm, the Elliptic Curve Cryptography algorithm to encrypt the plaintext information with FPGA encryption chip to encrypt and transmit the initial key to realize secure exchange. Alan J. Michaels, *et.al* [32] have introduced an efficient mechanism to generate a chaotic signal digitally, while tailoring waveform characteristics for maximum performance in various application spaces, overcoming known limitations in DSSS communications. Shuichi Aono, *et.al* [33] has proposed a cryptosystem using iterations of a chaotic map. This cryptosystem uses expansion map for encryption and decryption and was a symmetric key cryptography that has a public key. They have investigated the vulnerability of this cryptosystem. lker Dalkiran, *et.al* [34] have modeled cipher using Artificial Neural Network (ANN), to overcome disadvantages of chaotic systems, the dynamics of Chua's circuit namely x, y and z are ANNs that have some distinctive capabilities like learning from experiences, generalizing from a few data and nonlinear relationship between inputs and outputs. Shih-Liang Chen, et.al [35] have proposed a robust hyper-chaotic system that is practically ser- vice able in digital secure-communication. The system consists of many coupled robust logistic maps that form a hyper-chaotic system. The system has a very large key space which grows along with the system precision.

2.4. Cryptanalysis of Chaotic Ciphers

With the development of chaotic ciphers, new methods of cryptanalysis have been discovered by new researchers

according to the needs and ways to fulfill them for providing perfection in the developed ciphers.

Goce Jakimoski, *et. al* [36], have proposed the analysis of the impact of chaos-based techniques on block encryption ciphers. They have presented several chaos based ciphers. Using the well-known principles in the cryptanalysis they have showed 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. Ninan Sajeeth Philip, *et.al* [37], have discussed mixing of chaotic systems as a dependable method for secure communication. Distribution of the entropy function for steady state as well as plaintext input sequences are analyzed. It has been shown that the mixing of chaotic sequences results in a sequence that does not have any state dependence on the information encrypted by them. Hu Guojie, *et.al* [38] have analyzed the secure property of chaos communication system based on chaotic synchronization using the chosen ciphertext attack under Kerckhoff principle. They have pointed out that secure communication system based on chaotic synchronization is not highly secure as they can resolve the parameters (keys) of secure communication system by chosen-ciphertext attack. Gonzalo, Alvarez, *et. al* [39] have proposed ciphers which has been difficult to realize in practice with a reasonable degree of security. Likewise, they have been seldom accompanied by a security analysis. G. Álvarez, et.al [40] explained how to break a very recent block cipher algorithm based on the logistic map. This cryptosystem has used a 128-bit external key to derive the initial condition and number of iterations, but in a weak way allowing for attack. As a consequence, the complete 128-bit external key can be obtained in a few steps. Alvarez G, *et.al* [41] has described the basic and minimum requirements of any chaotic cryptosystems.

Sadok El Asmi, *et.al* [42] have quoted a new setting for the problem of channel identification. A new definition of identifiability for linear and nonlinear channel has been given, the fundamental link between the problem of observability of input-output system and the channel parameters, identification. A test of that definition has been provided in terms of ranks of Jacobean matrices. Alvarez, et. al [43] have presented an analysis of a recently proposed cryptosystem based on chaotic oscillators and feedback inversion. It has been shown that how the cryptosystem can be broken when duffings oscillators are considered. Some implementation problems of the system are also considered. Alvarez, *et.al* [44] have examined the performance of new cryptosystems based on chaotic dynamical systems properties and covered the latest advances in chaotic cryptography and discussed their practical uses and security levels. G. Alvarez, *et.al* [45], has presented the analysis of cryptosystem based on duffings oscillator. Implementations problems have been also discussed. Alvarez, Montoya, *et.al* [46] have analysed the security of two of the most new and interesting ones ciphers, which uses a dynamically updated look up table and also work as stream ciphers. Eli Biham, *et. al* [47], have presented in their paper a general framework for the application of the ideas of differential cryptanalysis to stream ciphers. It demonstrates that some differences in the key (or the initial state or the plaintext) are likely to cause predicted differences in the key stream or in the internal state. These stream differences can then be used to analyze the internal state of the cipher and retrieve it efficiently. These ideas have been applied to stream ciphers of various designs. Muhammad Asim *et.al* [48] have proposed, an efficient method for designing S-boxes based on chaotic maps. The proposed method was based on the mixing property of piecewise linear chaotic maps. The S-box so constructed has very low differential and linear approximation probabilities. The proposed S-box was more secure against differential and linear cryptanalysis compared to recently propose chaotic S-boxes. Shujun Li, *et. al* [49] pointed out in their paper that CKBA (Chaotic Key-based algorithm) proposed in IS-CAS2000 is very weak to the chosen/known plaintext attack with only one plain image. Experiments were made to show the feasibility of the chosen/known plaintext attack. Ruming Yin, *et.al* [50], designed application of linear cryptanalysis to a chaotic stream cipher by strictly using the basic design criterion of cryptosystem–confusion and diffusion. Linear cryptanalysis methods are rarely used to improve the security of chaotic stream ciphers.

3. CONCLUSION AND FUTURE SCOPE

Cryptography and cryptanalysis proves to be the necessary part of communication with the development and advancement of modern techniques in the field. Studies done on chaos and its analysis by many researchers cited in review give acquaintances with complex, strange and dynamic behavior of chaos and its application in many fields especially in cryptography They reported the possibility of using chaos in cryptography for developing secure ciphers as properties of chaotic nature promises to provide robustness against many common attacks which traditional ciphers could not. Many schemes have been invented by the research scholars out of which message-embedded scheme was found to be the recent third generation scheme. Application of chaos in the field led to an unlimited scope of constructing chaotic ciphers.

REFERENCES

[1] Ljupco Kocarev, “Chaos-Based Cryptography: A Brief Overview”, *IEEE Transactions on Non-Linear Dynamics and Chaos* ,1531(363), 6-21, 2001.

[2] Tao Yang, “A Survey of Chaotic Secure Communication Systems”, *International Journal of Computational Cognition*, 2(2), 81-130, 2004.

[3] Bogdan Cristea, Constantin Cehan, “Applications of Chaos Theory in cryptography”, *Military Equipment and*

Technologies Research International Conference, Bucharest, Romania, 1-5, 2002.

[4] Cristian-Iulian, Alexandru, "Chaos-based Cryptography a Possible Solution for Information Security", *Series III: Mathematics, Informatics, Physics, Bulletin of the Transilvania University of Bra¸sov* , 2(51), 113-126, 2009.

[5] Muhammed Rezal, "Chaos Based Cryptography, An Alternative to Algebraic Cryptography" *Int. J. Bif. Chaos*, 20(8), 2547-2551, 2010.

[6] David Arroyo, Gonzalo Alvarez, Veronica Fernandez, "On the Inadequacy of the Logistic Map for Cryptographic Applications*"*, *Aactas de la x recsi*, 77-82, 2008.

[7] Dubrova E., Teslenko M. and Tenhunen H., "On Analysis and Synthesis of (n, k)-non-linear Feedback Shift Registers," in *Design and Test* in Europe, 55(11), 1286-1291, 2008.

[8] Patidar Vinod and Sud K. K., "A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing", *Electronic J. of Theoretical Physics*, 6(20), 327-344, 2009.

[9] Wu C. W., Yang T., and Chua L. O., "On Adaptive Synchronization and Control of Nonlinear Dynamical Systems," *International Journal of Bifurcation and Chaos*, 6(3), 455-471, 1996.

[10] Floriane Anstett, Gilles Millerioux, and Gérard Bloch, "Chaotic Cryptosystems: Cryptanalysis and Identifiability", *IEEE Transactions on circuits and systems*, 53(12), 2673-2680, 2008.

[11] Millérioux G., Hernandez A. and Amigó J., "Conventional Cryptog- raphy andMessage-embedding*," in Proc. Int. Symp. Nonlinear Theory and its Applications*, Bruges, 35, 469-472, 2005.

[12] Rhouma Rhouma1, Belghith Safya2, "A Multidimensional Map for a Chaotic Cryptosystem", Syscom Laboratory, *Ecole Nationale d'Ingénieurs de Tunis*, Tunisia, 2005.

[13] Shih-Liang Chen, Shu-Ming Chang, TingTing Hwang ,Wen-Wei Lin, "A Fast Non-Linear Digital Chaotic Generator in Secure Communication", *National Science Council and National Center for Theoretical Sciences*, Taiwan.

[14] Oliveira de L. P. and Sobottka M., "*Cryptography with Chaotic Mixing"*, Chaos, Solutions and Fractals, 35(3), 466-471, 2008.

[15] Shujun Li, Guanrong Chen and Xuan Zheng, "Chaos-based Encryption for Digital Images and Videos," *Chapter 4 in Multimedia Security Handbook*, 110-121,2004.

[16] Wong W., Lee L. and Wong K., "A Modified Chaotic Cryptographic Method*"*, *Comput. Phys. Comm.*, 138, 234-236.

[17] V. Guglielmi 1, D. Fournier-Prunaret, A. K. Taha, P. Pinel, S. Rouabhi, "Two Encryption Schemes Using the Chaotic Dynamics of Two-Dimensional Noninvertible Maps", *IEEE Transactions on Circuits*, 1(1), 18-30, 2009.

[18] Rostislav Hucka, "A Ciphering Algorithm Based on Discrete Chaotic Map", *Dept. of Radio Electronics, Brno University of Technology*, 87-90, 2007.

[19] Solak E. "Cryptanalysis of Observer Based Discrete-time Chaotic Encryption Schemes*"*, *Int. J. Bifurc. Chaos*, 15(2), 653-658, 2005.

[20] M. Kiran Kumar, S. Mukthyar Azam, "Efficient Digital Encryption Algorithm Based on Matrix Scrambling Technique." *International Journal of Network Security & Its Applications (IJNSA)*, 2(4), 30-41, 2010.

[21] S. Nandi, B. K. Kar and P. Pal Chaudhuri, "Theory and Applications of Cellular Automata in Cryptography", *IEEE Transactions on Computers*, 43(12), 1346-1357, 1994.

[22] Jong-Seon No, Kyeongcheol Yang, Habong Chung and Hong-Yeop Song, "New Construction for Families of Binary Sequences with Optimal Correlation Properties", *IEEE Transactions on Information Theory*, 43(5), 1596-1602, 1997.

[23] Maria de Miguel de Santos', C. Sanchez-Avila" and R. Sanchez-Reillot, "Elliptic Curve Cryptography on Constraint Environments*"*, *IEEE Transactions on Information Theory*, 212-220, 2004.

[24] Tommaso Addabbo, Ada Fort, Santina Rocchi and ValerioVignoli, "On the Generation of Pseudo-Random Sequences Exploiting Digitized Chaotic Systems", *IEEE*, 639-642, 2007.

[25] Safwan El Assad, Hassan Noura, Taralova, "Design and Analyses of Efficient Chaotic Generators for Crypto-Systems", *Advances in Electrical and Electronics Engineering IAENG Special Edition of the World Congress on Engineering and Computer Science* , 3-12, 2008.

[26] Xianfeng Guo, Jiashu Zhang, Xianfeng Guo, "An Efficient Cryptanalysis of a Chaotic Cryptosystem and Its Improvement", *IEEE, College of Computer Science and Technology, Southwest University for Nationalities*, 578-581, 2010.

[27] Hans Dieter Schotten, "New Non-Linear Families of Code-Sequences with Correlation Properties Better Than Linear Families", *IEEE, Institute for Communication Engineering, Aachen University of Technology (RWTH)*, Germany, 378-382.

[28] Feng Bao, "Cryptanalysis of a Partially Known Cellular Automata Cryptosystem", *IEEE Transactions on Computers*, 53(11), 1493-1497, 2004.

[29] Muhab U, AbdulHameed, Ayman Mohammad, Bahaa Eldin, "A Cellular Automata Random Number Generator for Cryptographic Applications", *Computer and Systems Engineering Dept., Ain Shams University*, Cairo, Egypt.

[30] Petre Anghelescu, Silviu Ionita, Emil Sofron, "FPGA Implementation of Hybrid Additive Programmable Cellular Automata Encryption Algorithm", *IEEE, Eighth International Conference on Hybrid Intelligent Systems*, 96-101, 2008.

[31] Ping Zhou, Qun Ding, "The Key Exchange Research of Chaotic Encryption Chip Based on Elliptic Curve Cryptography Algorithm", *IEEE Second International Conference on Intelligent Computation Technology and Automation* , 689-693, 2009.

[32] Alan J. Michaels, David B. Chester, Harris Corp., GCSD, 2010, "Efficient and Flexible Chaotic Communication Waveform Family", *IEEE, Military Communication Conference*, 1250-1255.

[33] Shuichi Aono and Yoshifumi Nishio, "A Cryptosystem Using Expansion of Chaotic Map", *International Symposium on Nonlinear Theory and its Applications NOLTA'07*, 16(19), 220-223, 2007.

[34] Lker Dalkiran, Kenan Danis¸ Man, "Artificial Neural Network Based Chaotic Generator forcryptology," *Turk J Elec Eng. & Comp. Sci.*, 18(2), 225-240, 2010.

[35] Shih-Liang Chen, Shu-Ming Chang, Wen-Wei Lin, Ting-Ting Hwang, "Digital Secure-Communication Using Robust Hyper-Chaotic Systems", *National Science Council and National Center for Theoretical Sciences* in Taiwan, 1-20.

[36] Jakimoski G. and Kocarev L., "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps", *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 48(2), 163-169, 2001.

[37] Ninan Sajeeth Philip K. Babu Joseph, "Chaos for Stream Cipher", In Proc. of Recent Advances in Computing and Communications, Tata McGraw-Hill, pp. 35-42, 2000.

[38] H. Guojie, F. Zhengjin, and W. Lin (2002), "Analysis of a Type Digital Chaotic Cryptosystem," in *Proc. IEEE Int. Symp. Circuits Syst.*, 3, III-473-III-475.

[39] Li S., Alvarez G., Chen G., "Breaking a Chaos-based Secure Communication Scheme Designed by an Improved Modulation Method," *Chaos, Solitons and Fractals*, 25(1), 109-120, 2005.

[40] Alvarez G., Montoya F., Romera M, Pastor G., "Cryptanalyzing an Improved Security Modulated Chaotic Encryption Scheme Using Ciphertext Absolute Value", *Chaos, Solitons and Fractals*, 23 (5) 1749–1756, 2004.

[41] Alvarez G. and Li S., "Some Basic Cryptographic Requirements for Chaos-based Cryptosystems," *Int. J. Bifurc. Chaos*, 16(8), 2129-2151. 2006.

[42] Sadok El Asmi, "Nonlinear Identifiability: An Algebraic Approach", *Proceedings of the 3rd International Symposium on Image and Signal Processing and Analysis*, 1045-1047, 2003.

[43] Alvarez G., Arroyo D., and Nunez J., "Application of Gray Code to the Cryptanalysis of Chaotic Cryptosystems," *in 3rd International IEEE Scientific Conference on Physics and Control*, 374(1),44-49, 2007.

[44] Li S., Alvarez G., Chen G., "Breaking a Chaos-based Secure Communication Scheme Designed by an Improved Modulation Method, *Chaos, Solitons and Fractals*, 25(1), 109-120, 2005.

[45] Alvarez G., Montoya F., Romera M, Pastor G., "Cryptanalyzing an Improved Security Modulated Chaotic Encryption Scheme Using Ciphertext Absolute Value, *Chaos, Solitons and Fractals*, 23 (5) 1749-1756, 2004.

[46] G. Alvarez, F. Montoya, M. Romera, G. Pastor, "Cryptanalysis of Dynamic Look-up Table Based Chaotic Cryptosystems", Physics Letter A, 326, 211-218, 2004.

[47] Eli. Biham, "Cryptanalysis of Chaotic Map Cryptosystems," *Suggested at EUROCRYPT '91, Lecture Notes in Computer Science*, 547, 532-534, 1991

[48] Muhammad Asim and Varun Jeoti, "Efficient and Simple Method for Designing Chaotic S-Boxes", *ETRI Journal*, 30(1), 170-172, 2008.

[49] Li. Shujun, "Analyses and New Designs of Digital Chaotic Ciphers," *School of Electronic and Information Engineering, Xi'an Jiaotong University*, 2003.

[50] Ruming Yin, Jian Yuan, Qiuhua Yang, Xiuming Shan, Xiqin Wang, *"Linear Cryptanalysis for a Chaos-based Stream Cipher,"* World Academy of Science, Engineering and Technology ,60, 799-804, 2009.