RESEARCH ARTICLE
doi: 10.2306/scienceasia1513-1874.2016.42S.042

ScienceAsia 42S (2016): **42–48**

A study on encryption using three-dimensional cellular automata

S. Amirthalingam[a,*], **K. Latha**[b]

[a] Department of CSE, TRP Engineering College, Tiruchirappalli, Tamil Nadu, India
[b] Department of CSE, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamil Nadu, India

*Corresponding author, e-mail: amirtha08@gmail.com

Received 31 Aug 2014
Accepted 20 Jul 2016

ABSTRACT: With the exponential growth of information being transmitted as a result of various networks, the issues related to providing security to transmit information have considerably increased. Mathematical models were proposed to consolidate the data being transmitted and to protect the same from being tampered with. Work was carried out on the application of 1D and 2D cellular automata (CA) rules for data encryption and decryption in cryptography. A lot more work needs to be done to develop suitable algorithms and 3D CA rules for encryption and description of 3D chaotic information systems. Suitable coding for the algorithms are developed and the results are evaluated for the performance of the algorithms. Here 3D cellular automata encryption and decryption algorithms are used to provide security of data by arranging plain texts and images into layers of cellular automata by using the cellular automata neighbourhood system. This has resulted in highest order of security for transmitted data.

KEYWORDS: rules, decryption, layers, chaotic systems

INTRODUCTION

The concept of cellular automata (CA) was first proposed by Ulam et al and has attracted research scholars from various specializations [1]. CA is a mathematical computing model, programming complex operations with the help of available local information [2]. Different types of CA rules were developed over a long period and consisted of 1D and 2D CA rules [3]. CA in cryptography is popular due to its simplicity and at the same time its ability to handle complex situations [4]. In the early periods, 1D CA rules were developed and it was established that even these simple rules could analyse complex behaviour of various systems [5]. CA helps to predict global behaviour of a complicated system from local observations [6]. CA models were created and the simulations were run on a computer for obtaining various local as well as global configurations [7]. Recent works have shown that CA can be classified into ordered, complex or chaotic, based on the parameters in 2D CA rules [8]. To accurately model discrete dynamic systems, 2D CA rules and algorithms were proposed [9]. The CA rules were extended to image cryptography using wavelet image transforms [10]. To improve the security of the information transmitted, 3D CA rules and algorithms were developed to handle chaotic systems [11]. The concept of implementing object oriented encryption using layered CA was developed [12]. The behaviour of CA rules related to boot swap percolations benefited text and image secretly because of their interrelationships [13]. 3D CA rules are widely used for generating isotropic discrete waves on CA [14]. Guidelines were developed for symmetric key encryption in 3D CA algorithms [15]. Data encryption using 9's proved more lucid and secured [16]. Although enough work was carried out on 1D and 2D CA and suitable algorithms (AES, DES) were developed, discrete references were made on 3D CA rules applicable to 3D chaotic systems. The extension of 2D CA to 3D CA was mentioned in the literature [17]. By sequential application of nonlinear and linear CA rules, the order of security for the transmitted information in 2D and 3D CA has improved [18]. The equivalence of AES and DES algorithms and their analysis showed that the linear and nonlinear CA rules form a better substitution for AES and DES algorithms [19]. The work reported in this paper refers to analysing the 3D CA rules and developing suitable algorithms, coding and obtaining the results. Attempts are made to evaluate the proposed algorithms in terms of various matrices like resistance to brute force attack, creation of confusion, time taken for encryption, decryption,

and key generation, and it has been established that the proposed algorithms exhibit better security than the existing 1D and 2D CA algorithms.

Şiap et al[2] worked on configuration for 2D cellular automata (CA) with the rule 2460 N. Their main work was on reversibility of cellular automation with reference to configurations in CA. They developed algorithms using matrix representation of 2D CA. Jin et al[20] worked on image sharing based on neighbourhoods configurations and developed methods to share secret information using configurations available in 2D CA. Their work was to develop shared images having the same size of original information with no loss of resolution and having linear computational complexity. The simulated results demonstrated improved security of transmitted data since images contain large data and cannot be handled by usual cryptography or 1D. Chen et al[3] pioneered the security of images by making use of recursive automata substitution for image security. The pixels are replaced by recursive CA, which creates confusion and diffusion and helped in image data security. Machicao et al[21] made use of chaotic encryption method for security transmitted data based on life like CA. They applied the theory of chaos for cryptography. The CA searches for chaos property of data using different tests to identity the relation between chaos and randomness of data. This method was simpler compared to other methods. Jin[5], during the same period, worked on image encryption using elementary CA. They investigated the behaviour of a number of elementary CA. It was concluded that the behaviour satisfied the basic requirement of encryption process to transform the pixel values. They established that their method satisfied the properties of confusion and diffusion resulting in improved security for the transmitted data with no loss of information and was applicable to real time requirements. Bakhshandeh et al[7] worked on authenticated image encryption using chaotic maps and memory cellular data. Their work was based on 2D CA. They made use of a piecewise linear chaotic map to confuse the plain image and developed suitable diffusion methods. The chaotic maps provided further authenticity to know whether the data was tampered during transmission.

Wu et al[10] also worked on secret image transmission security using authentication and discrete wavelet transforms. They made use of 1D CA discrete wavelet transforms and hash functions in their proposed work. Their method enabled low computational costs, tamper detection, etc. Abdo et al[6] developed cryptosystem based on primary CA rules. They developed an algorithm based on primary or elementary CA with periodic boundary properties having unity attractors. Based on the encrypted image, the unity attraction changes. Their algorithms provided a high security level and prevention of statistical attacks. They developed a step by step method for the algorithm used, which consisted of generating parameters and their computation, security analysis, adjacent pixel analysis, key generation, sensitivity analysis, tests, etc. Ramírez-Torres et al[22] pioneered numerical implementation of real time encryption systems. They have numerically implemented encryption systems used in real time encryption purposes. The main contribution of their work was that there was no correlation between original signals and encrypted version, which made it highly secured. Wang et al[23] worked on 3D cellular automata for generating isotropic discrete waves on CA. The main focus was on analysing the possibility of computing isotropic figures on CA such as circles to spheres, etc. They used CA to analyse discrete universe consisting of 3D continuous space. Jaberi et al[8] worked on two layer CA based on cryptography. Their method worked better than MATLAB. The architecture developed by them also worked well for hardware implementations. They outlined the general characters of cryptography as privacy to information, context trustiness, and authentications deny avoidance, etc.

Nandi et al[11] made a primitive study on theory and application of CA in cryptography, which formed the basis for current research in the 2D and 3D CA works. Sahoo et al[24] did experimental work on encompression using 2D CA rules. They analysed the algebraic structure of periodic boundary 2D CA through the introduction of a matrix multiplication operation. Their method was also used for binary images. Das et al[4] proposed programmable CA using parallel AES encryption algorithms. In their method the combinational logic of each cell was not fixed, but controlled by a number of control signals. The PCA are modified CA, which has huge flexibility. Ganguly et al[1] made an exhaustive survey on cellular automata and came out with their conclusions. According to them, CA is a decentralized computing model with ability to perform complicated computations with the help of available information. They have listed different fields in which CA is used. It is basically a parallel processing device. The CA is used in social sciences, VLSI applications, pattern recognition, etc. Lafe[25] made data compression and encryption using CA transforms. They used a family of basic functions evolved from CA to compression

and encrypt data, which worked on CA transforms (CAT). Schonmann et al[13] worked extensively on the behaviour of CA related to bootstrap percolation. They have shown how percolations benefited because of their interrelationships. Hendi[26] worked on stream ciphering using 2D CA. The limitations of pseudo-random binary sequences were addressed by them. Somswara Rao et al[12] implemented object oriented encryption system using layered CA. Their work was to address the issues related to increased information threats, confidentiality, etc., which could not be addressed using existing CA algorithms. They proposed a strong time efficient crypto system with plain text, arranged into layers of binary digital planes and then encrypted as per CA rules. The system proposed by them exhibited better confusion and diffusion properties. Li et al[27] developed image water marking algorithms using 2D CA transforms. They proposed a novel watermarking systems based on maximum length CA and a 2D CA transform. They described different water marking techniques. Tripathy et al[15] developed guidelines and rules for lightweight CA based symmetric key encryption. They proposed black cipher supporting 128 bit block confirming the advanced encryption standards having high speed and low cost. Kansal et al[28] worked on idealized brain tumour growth dynamics using CA rules, the model developed by them was able to simulate tumour growth in three orders of magnitude using four microscopic parameters. Their results confirmed the real time values, thereby validating the model proposed by them. The model developed by them was a 3D CA which described the growth of turn or with respect to time.

Nagaraj et al[16] developed methods for encryption of data using 9's complement. The once security encryption developed by them proved more lucid, effective and complex from attackers view. The scheme was mathematically unbreakable. Mohsen et al[17] designed a reconfigurable image encryption processor using 2D CA generator. They analysed CA rules and proposed above model based on 2D CA as an image protector. A comparative study of the proposed method with the existing methods showed that the proposed method by them was superior in terms of throughputs, slices, and power consumption and correlation results. Phani Krishna Kishore et al[9] proposed encryption systems using layered CA (LRCA). They concluded that symmetric key algorithms execute much faster than asymmetric key algorithms. They proposed LRCA algorithms for data encryption. Panda[18] proposed encryption and decryption algorithms using 2D CA rules in cryptography. They used linear and nonlinear CA rules. First they applied nonlinear CA rules for both plain text and key. Then the linear periodic boundary CA rules were applied for decryption. Their algorithms were found to be superior to AES and DES algorithms and were more secured. Rama et al[29] made extensive studies on data encryption standard algorithms with CA rules. Their main work was on the use of CA for key generation in DES using rule 3D, which has excellent randomness. They concluded that in CA, extremely simple rules can produce more complex and random behaviour, providing high security for the transmitted data.

Panda et al[30] worked on developing encryption and decryption algorithms using 2D CA. Their method consisted of first applying nonlinear CA rules to plain text and key, then the PBCA rules are applied to the results and processed. The E and D were performed for 8 number of rounds to take care of the relations between plain text and cipher text, so that their algorithms is more secured that AES or DES. Panda et al[19] worked on equivalence of DES and AES algorithms in CA rules. They identified all the permutations and substitutions involved in AES and DES algorithms and compared with CA rules. They concluded that the permutations were equivalent to linear CA rules providing diffusion properties of cryptography, and substitution operations were equivalent to confusion properties of cryptography. Finally they concluded that instead of applying AES and DES algorithms the linear and nonlinear CA rules can be applied for better security of transmitted data. Luo et al[31] did extensive work on dynamical systems with multiple chaotic attractors and came out with their conclusions. According to them, the multiple chaotic attractors work well on dynamical systems. Gámez-Guzmán et al[32] worked on Synchronization of Chua's circuits with multi-scroll attractors and their applications to communication. Dedieu et al[33] worked on chaos shift keying modulation and demodulation of a chaotic carrier using self-synchronizing. Milanović et al[34] worked on improving masking algorithm for chaotic communications systems, which exhibited superior results compared to existing algorithms. Shackleford et al[35] worked on FPGAF implementation of neighbourhood of four cellular automata random number generators. Ling et al[36] designed an FPGA-based generator for chaotic frequency hopping sequences in cryptography. Stojanovski et al[37] developed a novel method of generating chaos based random numbers for 3D CA. Wang et al[23] designed and implemented FPGA group of 3D chaotic systems for

encryption and decryption. Wang et al[38] designed hyper chaotic system for 3D CA. Alvarez et al[39] did extensive research on cryptosystems and developed basic cryptographic requirements for chaos based cryptosystems. Yang et al[40] worked on application of numerical methods using MATLAB for 3D CA.

ISSUES AND CHALLENGES ASSOCIATED WITH 3D CA ALGORITHMS

Cellular automata

A cellular automaton is one whose cell values are updated based on the values of neighbourhood values as well as cellular automata rules. The classifications of cellular automata are:

(1) Null boundary cellular automata: A null boundary cellular automata is the one in which the extreme cells are connected to logic 0 states.
(2) Periodic boundary cellular automata: A periodic boundary CA is the one in which the extreme cells are connected to each other.
(3) Uniform cellular automata: A uniform cellular automata is the one in which same rules are applied to each cell.
(4) Hybrid cellular automata: if different rules are applied to different cells, then we call it as hybrid cellular automata.
(5) Linear cellular automata: if the rule of CA involves only XOR logic then it is called the linear rules, a cellular automata with all the cells having linear rules is called linear CA.
(6) Complement cellular automata: if the rule of cellular automata involve only XNOR logic then it is called the complement rules.
(7) Programmable cellular automata: A cellular automata is called programmable cellular automata if it employs some control signals. By specifying values of control signal at run time, programmable CA can implement various functions dynamically.

The following are the main issues and challenges:

(1) Reversibility of CA with reference to configuration in CA.
(2) Compared to plain text security, image security needs more detailed analysis.
(3) Chaotic encryption method needs to identify the chaos properly of the data using different tests.
(4) Developing crypto systems based on primary CA rules needs to identify periodic boundary properties having unity attractors.
(5) Numerical implementation of real time encryption systems needs careful analysis.

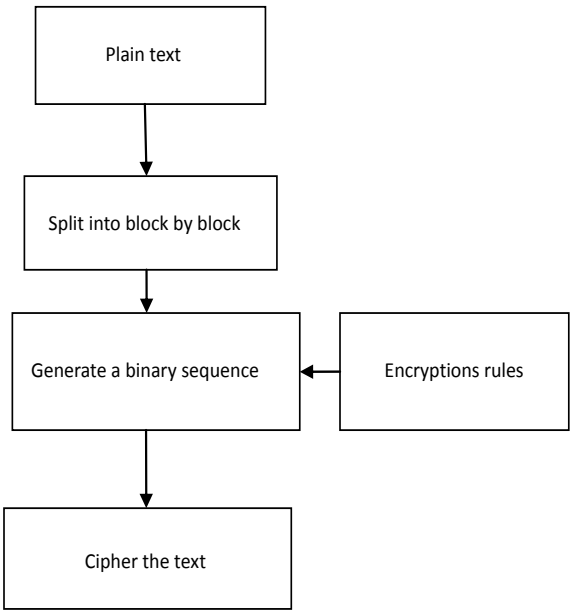

Fig. 1 Encryption process.

(6) Developing suitable CA transforms needs consideration of all the related factors.

SCOPE AND OBJECTIVE OF THE PRESENT WORK

The ways of doing encryption and decryption, encryption is the process of changing a plaintext into a cipher text. Fig. 1 presents the basic encryption process.

The scope of the present work is to develop algorithms for 3D CA rules to provide higher order of security for data and image transmission in cryptography.

FORMULATION OF PROBLEM

Although enough work was reported in the literature on development of 1D and 2D CA rule algorithms for cryptography, there are only discrete reference on development of 3D CA rules algorithms for encryption, decryption of data and image transmission with high security. Hence the formulation of the problem.

PRESENT WORK

Most of the transmitted data is secured from hackers through 1D and 2D CA algorithms. However, 3D CA rules can also be used for better security of data, especially when we deal with 3D chaotic systems, which are constructed by auto switched numerical

resolution of multiple 3D continuous chaotic systems. An attempt is made in this paper to develop 3D CA algorithms to solve problems of finite precision, resulting in high security and performance. The algorithms consist of data encryption and data decryption. The proposed algorithms, in addition to provide security to the data, are also useful for reducing negative influence of dynamic degradation in real time embedded systems. The 3D CA rules are similar to 1D and 2D CA rules and they make use of linear and nonlinear CA rules. To do so, the 3D chaotic systems, which are constructed using auto switched numerical resolutions, are identified, and linear and nonlinear CA rules are applied. First nonlinear CA rules are applied for both plain text and key, constituting encryption part. Next the decryption process is carried out similar to encryption in the reverse way. To avoid inter dependency between plain text and cipher text, 8 number of rounds are performed. The proposed algorithms provide better security to transmitted data, compared to advanced encryption standards (AES) and data encryption standards (DES) algorithms. The performance of a crypto system depends on how long it can be used before the key become hawked. Since the initial stage of a CA is the key to encryption, developing a chaotic system from the initial stage, which cannot be predicted or meddled, helps to realize highest security for transmitted data.

PROPOSED 3D CA ALGORITHMS FOR ENCRYPTION, DECRYPTION OF DATA AND KEY GENERATION

The linear and nonlinear CA rules are characterized by their Boolean functions. There are 2^{2^n} Boolean functions, out of which 2^n are linear and $2^{2^n} - 2^n$ are nonlinear. That is, in n variables, there are 2^n linear Boolean functions and the rest are nonlinear. The essential requirements of a Boolean function to be used for cryptography should include: balancedness, good linearity, high algebraic degree, good correlation immunity, simple implementation in hardware. The 3D CA algorithms for 3D chaotic system data transmission are proposed in this paper and are presented below.

Proposed encryption algorithms

Step 1: The plain text consisting of chaotic system data is split into blocks.
Step 2: Consider the first block.
Step 3: Each character in the block is considered and converted into 8 bit binary sequence.
Step 4: Each character binary sequence is arranged into layers.
Step 5: Encryption rules are applied to each layer to move to the next stage.
Step 6: All the layers are considered to form cipher text.
Step 7: All the characters are stored to complete the cipher text.
Step 8: Steps 3–7 are repeated until last block is reached.

Proposed decryption algorithms

It is basically the reverse process and consists of the following steps:
Step 1: Cipher text is split into blocks.
Step 2: The first block is considered.
Step 3: Each character in the block is considered and converted into 8 bit binary sequence.
Step 4: Each character binary sequence is arranged into layers.
Step 5: Decryption rules are applied to each layer to move to the next stage.
Step 6: All the layers are considered to form the plain text.
Step 7: All the characters are stored to form the plain text.
Step 8: Steps 3–7 are repeated for all the blocks.

Proposed key generation algorithms

(1) The key generation rules which are reversible are selected.
(2) The rules are indexed for both encryption and decryption.
(3) Random series of indexes are generated.
(4) Rule sets for both encryption and decryption are identified.
(5) The rules are shifted for each row for both encryption and decryption.

The performance and evaluation of the proposed algorithms will be discussed in the next section.

RESULTS AND DISCUSSION

The basic encryption and decryption CA rules for 1D and 2D are reviewed from the literature and the limitations that they contain are noted. Both text as well as image security problems are reviewed. Using chaotic maps, the 3D CA rules are generated for better security. The application of wavelet image transforms is considered for 1D and 2D CA rules. Layers CA rules are also reviewed. Algorithms for 3D CA for encryption, decryption and key generation are presented in the present work. As part of the evaluation of the performance of the decryption

3D CA algorithms, suitable coding is developed in VB 6.0 and when the program is run, it has yielded very encouraging results as stated below.

Resistance to brute force attack: for a hawker, there are 2^{128} possible combinations of keys and hence it is almost impossible to crack the information. Creation of confusion is better. The relation between key and cipher text is maximally complicated. Time taken for encryption, decryption and key generation is less. The time taken in the proposed 3D CA algorithms for cryptography is almost the same as AES and DES algorithms with a marginal edge over them.

CONCLUSIONS

The major contribution of present work is, to clearly analyse 3D CA algorithms for better security of transmitted data by arranging the plain text or images in layers of CA, resulting in an efficient neighbourhood system. This resulted a secured cryptography of transmitted data. In future this is implemented by using programmable cellular automata. The programmable cellular automata some control signals are needed to activate the encryption and decryption process.

REFERENCES

1. Niloy Ganguly (2003) *A Survey on Cellular Automata*, Centre for High Performance Computing, Dresden Univ of Technology, Dresden, Germany.
2. Şiap I, Akin H, Şah F (2010) Garden of eden configurations for 2-D cellular automata with rule 2460 N. *Inform Sci* **180**, 3562–71.
3. Chen RJ, Lai JL (2007) Image security system using recursive cellular automata substitution. *Pattern Recogn* **40**, 1621–31.
4. Das D, Misra R (2011) Programmable cellular automata based efficient parallel AES encryption algorithm. *Int J Netw Secur Appl* **3(6)**, 197–211.
5. Jin J (2012) An image encryption based on elementary cellular automata. *Optic Laser Eng* **50**, 1836–43.
6. Abdo AA, Lian S, Ismail IA, Amin M, Diab H (2013) A cryptosystem based on elementary cellular automata. *Comm Nonlinear Sci Numer Simul* **18**, 136–47.
7. Bakhshandeh A, Eslami Z (2013) An authenticated image encryption scheme based on chaotic maps and memory cellular automata. *Optic Laser Eng* **51**, 665–73.
8. Jaberi A, Ayanzadeh R, Mousavi ASZ (2012) Two layer cellular automata based cryptography. *Trends Appl Sci Res* **7**, 68–77.
9. Phani Krishna Kishore M, Kanti Kiran S, Bangaru Bhavya B, Harsha Chaitanya S (2011) A novel encryption system using layered cellular automata. In: *Proceedings of the World Congress on Engineering*, London, UK, pp 500–5.
10. Wu X, Sun W (2013) Secret image sharing scheme with authentication and remedy abilities based on cellular automata and discrete wavelet transform. *J Syst Software* **86**, 1068–88.
11. Nandi S, Kar BK, Chaudhuri PP (1994) Theory and Applications of Cellular Automata in Cryptography. *IEEE Trans Comput* **43**, 1346–57.
12. Somswara Rao C, Rao Attada S, Jayanthi Rao M, Nageswara Rao K (2011) Implementation of object oriented encryption system using layered cellular automata. *Int J Eng Sci Tech* **3**, 5786–95.
13. Schonmann RH (1992) On the behaviour of some cellular automata related to bootstrap percolation. *Ann Probab* **20**, 174–93.
14. Feschet F, Tougne L (2001) Generating isotropic discrete waves on cellular automata. *Int J Pattern Recogn Artif Intell* **15**, 1007–21.
15. Tripathy S, Nandi S (2009) LCASE: Lightweight Cellular Automata-based Symmetric-key Encryption. *Int J Netw Secur* **8**, 243–52.
16. Nagaraj S, Bhamidipati K, Ramachandra M (2010) Formal method of encryption using 9's complement. *Int J Comput Appl* **8**, 23–5.
17. Mohsen M, Zied G, Medien Z, Rached T (2009) Design of reconfigurable image encryption processor using 2-d cellular automata generator. *Int J Comput Sci Appl* **6**, 43–62.
18. Panda SP (2012) Encryption and decryption algorithm using two dimensional cellular automata rules and 1D CA based S-Box (1D Rule-30) in cryptography. *Int Refereed J Eng Sci* **1(2)**, 25–36.
19. Panda SP, Sahu M, Rout UP, Nanda SK (2011) Equivalence of DES and AES algorithm with cellular automata. *Int J Comm Netw Secur* **1**, 47–52.
20. Jin J, Wu Z (2012) A secret image sharing based on neighborhood configurations of 2-D cellular automata. *Optic Laser Tech* **44**, 538–48.
21. Machicao J, Marco AG, Martinez Bruno O (2012) Chaotic encryption method based on life-like cellular automata. *Expert Syst Appl* **39**, 12626–35.
22. Ramírez-Torres MT, Mejía-Carlos M, Murguía JS (2012) Numerical implementation of a real-time encryption system. *Procedia Eng* **35**, 182–91.
23. Wang ZL, Chen ZQ (2010) Design and implementation based on FPGA of a group of three-dimension chaotic system. In: *Proceedings of the 8th World Congress on Intelligent Control and Automation*, Jinan, China pp 70–4, [in Chinese].
24. Sahoo S, Sahoo S, Nayak BK, Choudhury PP (2008) Encompression using two-dimensional cellular automata rules, arXiv:0808.1470.
25. Lafe O (1997) Data compression and encryption using cellular automata transforms. *Eng Appl Artif Intell* **10**, 581–91.
26. Hendi HI (2007) Stream cipher using two dimen-

sional cellular automata. *J Univ Thi-Qar* **3(3)**, 1–9.
27. Li XW, Cho SJ, Kim ST (2012) Image watermarking algorithm using 2D cellular automata transform. *Int J Innovat Comput Inform Contr* **8**, 7249–62.
28. Kansal AR, Torquato S, Harsh IVGR, Chiocca EA, Deisboeck TS (2000) Cellular automaton of idealized brain tumor growth dynamics. *Biosystems* **55**, 119–27.
29. Rama R, Bala Suyambu J, Arokiaraj A, Saravanan S (2012) A study of DES algorithm with cellular automata. *Int J Innovat Manag Inform Prod* **4**, 10–6.
30. Panda SP, Sahu M, Rout UP, Nanda SK (2011) Encryption and decryption algorithm using two dimensional cellular automata rules in cryptography. *Int J Comm Netw Secur* **1**, 18–23.
31. Luo X, Small M, Danca MF, Chen G (2007) On a dynamical system with multiple chaotic attractors. *Int J Bifurc Chaos* **17**, 3235–51.
32. Gámez-Guzmán L, Cruz-Hernández C, López-Gutiérrez RM, García-Guerrero EE (2009) Synchronization of Chua's circuits with multi-scroll attractors: application to communication. *Comm Nonlinear Sci Numer Simul* **14**, 2765–75.
33. Dedieu H, Kennedy MP, Hasler M (1993) Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Trans Circ Syst II* **40**, 634–42.
34. Milanović V, Zaghloul ME (1996) Improved masking algorithm for chaotic communications systems. *Electron Lett* **32**, 11–2.
35. Shackleford B, Tanaka M, Carter RJ, Snider G (2002) FPGA implementation of neighborhood-of-four cellular automata random number generators. In: *Proceedings of the 2002 ACM/SIGDA 10th International Symposium on Field-Programmable Gate Arrays*, pp 106–12.
36. Ling C, Wu X (2001) Design and realization of an FPGA-based generator for chaotic frequency hopping sequences. *IEEE Trans Circ Syst I* **48**, 521–32.
37. Stojanovski T, Pihl J, Kocarev L (2001) Chaos-based random number generators. Part II: practical realization. *IEEE Trans Circ Syst I* **48**, 382–5.
38. Wang GY, Bao XL, Wang ZL (2008) Design and FPGA implementation of a new hyperchaotic system. *Chin Phys B* **17**, 3595–602.
39. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. *Int J Bifurc Chaos* **44**, 2129–51.
40. Yang WY, Cao W, Chung TS, Morris J (2005) *Applied Numerical Methods Using MATLAB*, Wiley.