Nonlinear dynamics, applications to chaos-based encryption

Zongchao Qiao

THESE DE DOCTORAT DE

L'ÉCOLE CENTRALE DE NANTES

ECOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies
de l'Information et de la Communication
Spécialité : *Automatique, Productique et Robotique*

Par

Zongchao QIAO

Nonlinear dynamics, applications to chaos-based encryption

Thèse présentée et soutenue à Nantes, le 25 Février 2021
Unité de recherche : UMR 6004, Laboratoire des Sciences du Numérique de Nantes (LS2N)

Rapporteurs avant soutenance :

Danièle FOURNIER-PRUNARET	Professeure des universités, INSA Toulouse
Moulay AZIZ-ALAOUI	Professeur des universités, Université Le Havre Normandie

Composition du Jury :

Président :	Christophe GUYEUX	Professeur des universités, IUT Belfort-Montbéliard, Belfort
Examinateurs :	Safwan EL ASSAD	Maître de conférences HDR, Polytechnique Nantes
	Ina TARALOVA	Maître de conférences, École Centrale de Nantes
Dir. de thèse :	Mazen SAAD	Professeur des universités, École Centrale de Nantes

ACKNOWLEDGEMENT

First and foremost, I would like to express my deepest gratitude to my superior, Associate Professor Ina Taralova, for her patience, warm encouragement and helpful guidance during the three years of my PhD study at Ecole Centrale de Nantes. I would also like to thank my director of the thesis, Professor Mazen Saad, for all his help and guidance. Their positive feedback always motivated me to pursue the best.

Many thanks to Professor Safwan El Assad who gave me lots of help and valuable suggestions. Also, I would like to thank Professor Danièle Fournier-Prunaret for her useful remarks in the frame of the CST (Comité de Suivi de Thèse).

I would also thank all my colleagues and staffs in group COMMANDE (Control) and laboratory LS2N for their help and support. Thank Ecole Centrale de Nantes that provided me with a great environment for working with the excellent researchers. Many thanks to my friends for their warm company and encouragement.

Besides, I would like to thank China Scholarship Council (CSC) for giving me the precious opportunity to work on such an interesting topic, and also Chinese Embassy for the care and concern during the three years, especially when we were under the threaten of COVID-19 pandemic.

I would also like to thank the reviewers of my thesis : Prof. Fournier-Prunaret and Prof. Alaoui, for their invaluable time, helpful comments and suggestions.

Finally, my sincere gratefulness goes to my family, especially my husband, for his unconditional love, continuous support, and constant encouragement, which makes me brave and confident to face the challenges in my academic research.

RÉSUMÉ

Les systèmes chaotiques présentent des comportements dynamiques non-linéaires complexes. Leurs propriétés spécifiques, comme l'ergodicité, la propriété de mélange topologique, les caractéristiques proches de celles d'un signal aléatoire, la forte sensibilité aux conditions et paramètres initiaux correspondent aux les exigences cryptographiques fondamentales des algorithmes de cryptage sécurisés, c'est-à-dire la confusion et la diffusion, selon la théorie de la sécurité de l'information de Shannon. De ce fait, la cryptographie basée sur le chaos est un excellent candidat pour la conception de crypto systèmes modernes, sécurisés et fiables.

Dans cette thèse, les spécificités des systèmes chaotiques, ainsi que les méthodes et outils pour leur analyse tels les points fixes et périodiques, les attracteurs chaotiques, les diagrammes de bifurcation, les bassins d'attraction, les exposants de Lyapunov etc, ont été revus du point de vue de la cryptographie. Grâce à cette analyse, nous avons souligné que dans le cas des applications cryptographiques, certaines caractéristiques spécifiques de ces systèmes, comme la chaoticité et la sensibilité aux conditions initiales doivent être amplifiées, tandis que d'autres caractéristiques comme certaines singularités (points fixes) doivent être évitées, ou remodelées (densité de probabilité de la fonction chaotique) pour satisfaire aux critères de sécurité.

Les crypto systèmes basés sur le chaos tirent pleinement parti de la dynamique chaotique pour obtenir des performances de confusion et de diffusion satisfaisantes. La confusion signifie une relation complexe entre le texte chiffré, la clé secrète et le texte, tandis que la diffusion souligne la grande sensibilité du texte chiffré au texte original. Cela signifie qu'un petit changement dans le texte original (par exemple, un pixel dans l'image originelle) entraînera une différence significative dans le texte chiffré.

Les crypto systèmes basés sur le chaos peuvent être classés en chiffrement par flux et chiffrement par blocs. Les chiffrements par blocs chiffrent le texte bloc par bloc pour obtenir de bonnes performances de confusion et de diffusion. Le flux de clés produit par un Générateur de Nombres Pseudo-Chaotiques (PCNG) est utilisé pour supporter les opérations de confusion et de diffusion. Un chiffrement par bloc sécurisé nécessite une structure complexe de confusion et de diffusion et un PCNG cryptographique qui peut générer des

nombres pseudo-chaotiques avec des caractéristiques souhaitées, à la fois chaotiques et pseudo-aléatoires. En revanche, les chiffrements par flux chiffrent le texte en continu en le masquant à l'aide de l'opérateur XOR avec un flux de clé généré par un PCNG. Outre la sécurité, la vitesse élevée est l'autre exigence majeure d'un chiffrement par flux.

Ces dernières années, bien qu'un certain nombre de crypto systèmes basés sur le chaos aient été proposés dans la littérature, beaucoup d'entre eux se sont avérés vulnérables à certains types d'attaques. Les problèmes existent principalement dans les aspects suivants :

Pour les chiffrements par blocs basé le chaos, d'une part, des niveaux insuffisants de confusion et de diffusion font que le processus de confusion et de diffusion doit être itéré plusieurs fois pour obtenir des performances de sécurité satisfaisantes, ce qui est inefficace car le message doit être traité plus d'une fois et donc la faible efficacité empêche en principe les chiffrements par blocs d'être appliqués dans les applications en temps réel. D'autre part, une stratégie de confusion et de diffusion pas assez complexe laisse une porte ouverte aux attaquants qui peuvent profiter de ce point faible pour éliminer l'effet de la confusion ou de la diffusion. Cependant, il a été prouvé qu'un schéma de diffusion uniquement ou un schéma de confusion uniquement peut être facilement craqué.

Pour les chiffrements par blocs basés sur le chaos et les chiffrements par flux basés sur le chaos, le PCNG joue un rôle crucial dans leur sécurité, notamment pour le chiffrement par flux dont la sécurité dépend fortement du PCNG cryptographique. Un PCNG est conçu sur la base d'opérations appropriées sur plusieurs cartes chaotiques. Il doit conserver des caractéristiques chaotiques, i.e. comportement pseudo-aléatoire et forte sensibilité à la clé secrète (composée des conditions initiales et des paramètres des cartes chaotiques adoptées), et présenter un comportement pseudo-aléatoire pour aider les chiffrements à résister à l'attaque en clair choisi, à l'attaque différentielle et à l'attaque statistique. En plus, un PCNG cryptographique nécessite également à un grand espace clé pour contrecarrer l'attaque de force brute. Cependant, dans la littérature existante, certains crypto systèmes publiés basés sur le chaos présentent des failles de sécurité : le flux de clés n'est pas produit par un PCNG et donc le flux de clés ne possède pas de caractéristiques aléatoires, ce qui provoque une fuite d'informations de la clé secrète et conduit ainsi à des failles de sécurité. En outre, certaines PCNGs proposées manquent d'analyse de sécurité complète d'un point de vue cryptographique. Par conséquent, ces PCNG ne peuvent pas être applicables aux crypto systèmes.

Pour tous les crypto systèmes basés sur le chaos, il est inévitable que les cartes chaotiques utilisées fonctionnant avec précision finie dans les appareils numériques présentent

une dégradation dynamique. Comme la majorité des cartes chaotiques sont basées sur des nombres réels, la plupart des PCNGs proposées utilisent les notations à virgule flottante. Cependant, ce type de données, en particulier format double précision, présente les inconvénients d'un coût de calcul élevé et d'une utilisation inefficace des ressources. En outre, en raison de la haute sensibilité des systèmes chaotiques et de la nature de précision finie des plates-formes logicielles et matérielles, les erreurs de troncature ou d'arrondi peuvent entraîner une grande différence dans la périodicité des nombres générés, ce qui peut nuire à la fiabilité de la sécurité du PCNG.

En résumé, les problèmes évoqués ci-dessus existent principalement dans la stratégie de confusion et de diffusion, la conception de PCNG cryptographique, et la question de la mise en œuvre (concernant le type de données des cartes chaotiques utilisées et le problème de la dégradation dynamique). Ces trois aspects fonctionnent conjointement pour influencer la qualité d'un crypto système basé sur le chaos.

Dans cette thèse, nous nous concentrons sur la question de l'utilisation de la dynamique chaotique en cryptographie visant à proposer de nouveaux crypto systèmes basés sur le chaos et de PCNGs qui soient sécurisés et fiables. Les contributions principales sont résumées ci-dessous.

1. Pour éviter les erreurs de quantification, de troncature ou d'arrondi lors de l'application numérique, les cartes chaotiques en une dimension (1D) fréquemment utilisées, y compris la carte logistique, la carte de la tente asymétrique, la carte chaotique linéaire par morceaux (PWLCM) et la carte chaotique d'ordre 3 de Chebyshev ont été reformulés sur un corps fini de N (N = 32) bits. La dégradation dynamique due à la précision finie a été analysée en termes de performances statistiques (période et histogramme) et de la contribution d'espace clé.

   Du point de vue de la mise en œuvre, par rapport aux crypto systèmes et PCNGs les plus fréquents qui utilisent les nombres réels avec une double précision, les nouveaux crypto systèmes et PCNG conçus basés sur les cartes chaotiques d'entiers 32 bits reformulées peuvent non seulement réduire les coûts de calcul et les ressources matérielles, mais également garantir que ces systèmes peuvent être implémentés dans différentes plates-formes d'exploitation en évitant les problèmes de quantification.

2. Un nouveau chiffrement par flux efficace basé sur le chaos a été développé et évalué dans [ii,iii]. Il est basé sur un nouveau PCNG sécurisé qui est construit à partir de les fonctions chaotiques reformulées utilisant des nombres entiers, i.e. la carte logistique,

la carte de la tente asymétrique et PWLCM. Le PCNG proposé n'utilise que quatre opérateurs XOR et un mécanisme de multiplexage pour pallier le problème de la dégradation dynamique. Ce PCNG innovant s'avère efficace et facile à mettre en œuvre.

Les tests effectués ont confirmé que le PCNG proposé possède de bonnes propriétés cryptographiques et passe avec succès le test des signaux aléatoires du NIST. En outre, le chiffrement par flux a été vérifié pour être sûr et fiable.

3. Un crypto système basé sur le chaos sécurisé et robuste basé sur des composants chaotiques et la S-box de AES (Advanced Encryption Standard) a été proposé dans [iv]. Il comprend un nouveau PCNG efficace, une diffusion globale et un chiffrement par blocs.

   Premièrement, ce PCNG est fondé sur la carte de la tente asymétrique et la carte chaotique d'ordre 3 de Chebyshev. Il peut éliminer le danger caché de détérioration de la sécurité causée par la dégradation dynamique et produire le flux de clés pour le schéma de confusion et de diffusion avec de bonnes caractéristiques cryptographiques, tels le grand nombre de clés pour empêcher l'attaque par force brute, la haute sensibilité à la clé secrète et le pseudo-aléatoire pour dissimuler la relation entre la clé secrète, le texte et le texte chiffré.

   En second lieu, la diffusion globale adopte une diffusion d'addition horizontale (HVD) et une diffusion d'addition verticale (VAD) suivie une cat map deux dimensions (2D) modifiée, qui réalise un bon niveau de diffusion.

   De plus, le chiffrement par bloc est basé sur une couche de confusion en utilisant l'AES S-box et une couche de diffusion qui est construite sur la cat map 2D modifiée et une opération d'addition clé. Il fonctionne en mode de chaînes de blocs de chiffrement (CBC), ce qui améliore les propriétés de confusion et de diffusion.

   Les analyses de sécurité et les résultats expérimentaux ont démontré que le crypto système proposé basé sur le chaos a des performances de confusion et de diffusion sécurisées et complexes, et il peut résister aux principales attaques connues avec succès.

4. Le PCNG est crucial pour la sécurité d'un crypto système basé sur le chaos. En dehors de cela, un PCNG est essentiellement un Générateur de Nombres Pseudo-Aléatoires (PRNG). Les PRNG sont des outils importants dans de divers domaines de l'ingé-

nierie. Ainsi, nous avons proposé une méthode de conception de PRNG universel qui est fondée sur un couplage innovant exploré en utilisant des cartes chaotiques sur le champ entier de 32 bits [v].

Cette méthode est fondée sur un couplage innovant. Nous avons analysé des matrices de couplage efficaces pour les schémas de couplage en 2D et 3D, qui « cassent » les orbites originales des cartes chaotiques adoptées et rendent leurs périodes très longues ce qui permet d'améliorer le caractère aléatoire et surmonter efficacement la dégradation dynamique due à l'implémentation numérique.

De plus, deux méthodes de contrôle de sortie, i.e. des méthodes de contrôle de sortie alternatives et dynamiques, ont été proposées pour augmenter la complexité des PCNG et améliorer l'imprévisibilité et les caractéristiques aléatoires des nombres pseudo-aléatoires produits.

En outre, étant donné que les PCNG basés sur le schéma de couplage 2D ont la faiblesse d'un nombre de clés réduit, une stratégie de conception de PCNG dont l'espace clé est extensible a été proposée fondée sur la carte de la tente asymétrique. L'espace clé étendu peut aider le crypto système à améliorer la capacité de résistance à l'attaque par force brute [vi,vii].

En résumé, nous avons analysé dans cette thèse les problèmes existants dans les crypto-systèmes basés chaos dans la littérature. Nous avons proposé de nouvelles idées et de nouveaux schémas pour les surmonter. Les études réalisées ont démontré la sécurité et la fiabilité des solutions proposées.

ABSTRACT

Chaotic systems exhibit complex nonlinear dynamical behavior. Their attractive characteristics, such as ergodicity, topological mixing property, random-like behavior, high sensitivity to initial conditions and parameters are highly consistent with the primitive cryptographic requirements for secure encryption algorithms, i.e. confusion and diffusion, according to Shannon's theory of information security, which renders the chaos-based cryptography an excellent candidate for the designs of secure cryptosystems.

In this thesis, the specificities of chaotic systems, together with the methods and tools for their analysis such as fixed and periodic points, chaotic attractors, basins of attraction, bifurcation diagrams, Lyapunov exponents etc have been analyzed and redefined from the perspective of cryptography. Thanks to this analysis, we have pointed out that for cryptographic applications, some specific features of these systems, such as chaoticity and sensitivity to initial conditions must be enhanced, whereas other features related to some singularities (fixed points and their preimages) must be avoided, or reshaped (e.g. unsatisfactory density of probability of the chaotic map) to satisfy the security criteria.

Chaos-based cryptosystems take full advantage of chaotic dynamics to achieve satisfactory confusion and diffusion performances. Confusion means a complex relationship between the ciphertext, the secret key, and the plaintext, while diffusion underlines the high sensitivity of the ciphertext to the plaintext. It means a tiny change in the plaintext will make a significant difference in the ciphertext.

Chaos-based cryptosystems can be classified into block ciphers and stream ciphers. Block ciphers encrypt the plaintext block by block to achieve high confusion and diffusion performance. The key stream produced by a pseudo-chaotic number generator (PCNG) is used to support the confusion and diffusion operations. A secure block cipher requires a complex confusion and diffusion structure and a cryptographic PCNG which can generate pseudo-chaotic numbers with desired chaotic features and pseudo-randomness. By contrast, stream ciphers encrypt the plaintext continuously by masking it using the XOR operator with a key stream generated by a PCNG. Apart from the security, high speed is the other major requirement of a stream cipher.

In recent years, although a number of chaos-based cryptosystems have been proposed in

the literature, many of them have been verified to be vulnerable to certain kinds of attacks. The problems mainly exist in the following aspects.

For chaos-based block ciphers, firstly, the insufficient level of confusion and diffusion makes the confusion and diffusion scheme have to be looped a couple of rounds to achieve a satisfactory security performance, which is inefficient for a block cipher because the plaintext needs to be scanned more than once. Therefore, the low efficiency hinders the block ciphers to be applied in real-time applications. Secondly, an insecure and not complex enough strategy of confusion and diffusion leaves an open door to attackers who can make use of this drawback to remove the confusion or diffusion effect. However, it has been proven that a diffusion-only scheme or a confusion-only scheme can be cracked easily.

For both chaos-based block ciphers and stream ciphers, the PCNG plays a crucial role in their security, especially for the stream cipher whose security depends strongly on the cryptographic PCNG. A PCNG is designed based on proper operations on multiple chaotic maps. It should maintain chaotic features, i.e. random-like behavior and high sensitivity to the secret key (composed by the initial conditions and parameters of the adopted chaotic maps), and exhibit pseudo-randomness to help the ciphers to resist the chosen-plaintext attack, the differential attack, and the statistical attack. In addition to this, a cryptographic PCNG also calls for a large key space to frustrate the brute-force attack. However, in the existing literature, some published chaos-based cryptosystems have security flaws : the key stream is not produced by a PCNG and thus the key stream does not possess randomness features, which causes information leakage of the secret key and thus leads to security vulnerabilities. Furthermore, some proposed PCNGs lack comprehensive security analysis from a cryptographic point of view. Hence, these PCNGs cannot be determined to be applicable to encryption systems.

For all chaos-based cryptosystems, it is inevitable that the used chaotic maps operating with finite precision in digital devices show dynamical degradation. Since the majority of the chaotic maps are based on real numbers, most of the proposed PCNGs use floating-point notations. However, this data type, especially the double precision notation, has disadvantages of high computation cost and inefficient resource utilization. Also, due to the high sensitivity of the chaotic systems and the finite precision nature of software and hardware platforms, the truncation or round-off errors may cause a big difference in the generated pseudo-chaotic numbers, which may undermine the PCNG's security reliability.

To sum up, the problems discussed above mainly exist in the strategy of confusion and diffusion, the cryptographic PCNG design, and the issue of implementation (regarding the

datatype of the used chaotic maps and the problem of dynamical degradation). These three aspects work jointly to influence the quality of a chaos-based cryptosystem.

In this thesis, we focus on the issue of using chaotic dynamics in cryptography aiming to propose new secure and reliable chaos-based cryptosystems and PCNGs. The main work is summarized as follows.

1. To avoid the quantization, truncation, or round-off errors in digital devices, the frequently-used one-dimensional (1D) chaotic maps including the logistic map, the skew tent map, the piece-wise linear chaotic map (PWLCM), and Chebyshev 3rd order chaotic map have been reformulated over an N-bit (N=32) finite integer field. The dynamical degradation caused by the finite precision definition has been analyzed in terms of the statistical (period length and histogram) performances and key space contribution.

   From the perspective of implementation, the new designed cryptosystems and PCNGs that are built upon the reformulated 32-bit integer chaotic maps can not only reduce the computational cost and hardware resources, but also ensure that these systems can be transplanted into different operation platforms without the quantization problems when compared to the most existing cryptosystems and PCNGs that used the real numbers with double precision.

2. A novel efficient chaos-based stream cipher has been developed and evaluated in [ii,iii]. It is based on a newly designed secure PCNG which is built on the reformulated integer chaotic maps, namely, the logistic map, the skew tent map, and PWLCM. The proposed PCNG only uses four XOR operators and a dynamic output control mechanism to palliate the problem of dynamical degradation, which is efficient and easy to implement.

   The conducted tests have confirmed that the proposed PCNG possesses good cryptographic properties and passes the NIST randomness test successfully. Also, the stream cipher has been verified to be secure and reliable.

3. A secure and robust chaos-based cryptosystem based on chaotic components and the AES (Advanced Encryption Standard) S-Box has been proposed in the work [iv], which is comprised of a new efficient PCNG, a global diffusion, and a block cipher.

   Firstly, this PCNG is based on the skew tent map and the Chebyshev 3rd order chaotic map. It can remove the hidden danger of deteriorated security caused by the dynamical degradation and produce the key stream for confusion and diffusion scheme with

good cryptographic features, such as the large key space to prevent the brute-force attack, the high sensitivity to the secret key and pseudo-randomness to conceal the relationship between the secret key, the plaintext and the ciphertext.

Secondly, the global diffusion adopts a horizontal addition diffusion (HVD) and a vertical addition diffusion (VAD) followed by a modified two-dimensional (2D) cat map, which can accomplish a good diffusion level. In addition, the block cipher is based on a confusion layer using the AES S-Box and a diffusion layer that is built on the modified 2D cat map and a key addition operation. It works in the cipher block chaining (CBC) mode, which enhances the confusion and diffusion properties.

The security analyses and the experimental results have demonstrated that the proposed chaos-based cryptosystem has secure and complex confusion and diffusion performances, and it can resist the main known attacks successfully.

4. The PCNG is crucial for the security of a chaos-based cryptosystem. Apart from this, a PCNG is basically a pseudo-random number generator (PRNG). PRNGs are important tools involving various engineering fields. Thus, we have proposed a universal PRNG design framework which is based on an explored smart coupling using chaotic maps over the 32-bit integer field [v].

   For the smart coupling, we have analyzed effective coupling matrices for 2D and three-dimensional (3D) coupling schemes. They can break the original orbits of the adopted chaotic maps and make their periods very long, and thus improve the randomness and overcome the dynamical degradation effectively.

   In addition, two output control methods, i.e. alternate and dynamic output control methods, have been proposed to increase the complexity of the PCNGs and enhance the unpredictability and randomness of the produced pseudo-random numbers.

   The smart coupling and the output control method compose the PRNG framework, based on which different chaotic maps can be chosen in order to design different PRNGs. NIST test has confirmed the pseudo-randomness of the proposed PRNGs. The results of the key space test and the key sensitivity test have demonstrated that the PRNGs also possess excellent cryptographic performances. Thus, the PRNGs (also can be called "PCNGs") can be used not only in any PRNG required applications, but also in cryptosystem designs.

   Furthermore, considering the PCNGs based on the 2D coupling scheme have the

weakness of small key space, a key space expandable PCNG strategy has been proposed based on the skew tent map. The expanded key space can help the cryptosystem to enhance the resistance ability to the brute-force attack [vi,vii].

To end up, this thesis has analyzed the existing problems in the designs of chaos-based cryptosystems in the literature and has proposed new ideas and schemes to overcome them. The conducted analyses and tests have demonstrated the security and reliability of the proposed solutions.

LIST OF PUBLICATIONS

---

i. Desislav Andreev, Simona Petrakieva, Ina Taralova, Zongchao Qiao. "Applying quantum machine learning approach for detecting chaotically generated fake usernames of accounts." The 13th International Conference for Internet Technology and Secured Transactions (ICITST – 2018), Dec 2018, Cambridge, United Kingdom

ii. Zongchao Qiao, Ina Taralova, Safwan El Assad. "A robust pseudo-chaotic number generator for cryptosystem based on chaotic maps and multiplexing mechanism." The 14th International Conference for Internet Technology and Secured Transactions (ICITST-2019), Dec 2019, London, United Kingdom

iii. Zongchao Qiao, Ina Taralova, Safwan El Assad. "Efficient pseudo-chaotic number generator for cryptographic applications." International Journal of Intelligent Computing Research (IJICR). 2020 March Volume 11, Issue 1 :1041-1048.
DOI : 10.20533/ijicr.2042.4655.2020.0126

iv. Zongchao Qiao, Safwan El Assad, and Ina Taralova. "Design of secure cryptosystem based on chaotic components and AES S-Box." AEU-International Journal of Electronics and Communications (2020) : 153205

v. Zongchao Qiao, Ina Taralova, Mazen Saad, Safwan El Assad. "Inverse logistic and skew tent map analysis for smart finite field coupling." The 13th CHAOS 2020 International Conference, June 2020, Florence Italy (turned into a virtual conference due to COVID-19)

vi. Zongchao Qiao, Ina Taralova, Safwan El Assad. "A reliable encryption oriented pseudo-chaotic number generator using a key space expandable strategy." The 15th International Conference for Internet Technology and Secured Transactions (ICITST-2020), Dec 2020, London, United Kingdom (turned into a virtual conference due to COVID-19)

vii. Zongchao Qiao, Ina Taralova, Safwan El Assad. "Pseudo-random key stream generation algorithm for encryption purposes." International Journal of Chaotic Computing (IJCC), 2020, Volume 7, Issue 1

TABLE OF CONTENTS

Résumé **3**

Abstract **9**

List of Publications **15**

Introduction **27**

Research background and motivation 27

Organization of the thesis and main contributions 31

1 Nonlinear dynamics and chaotic system **33**

1.1 Introduction 33

1.2 Historical perspective of chaotic dynamics 33

1.3 Fundamentals of nonlinear dynamical system 35

1.3.1 Continuous-time system 36

1.3.2 Discrete-time system 36

1.3.3 Notions of dynamical system 37

1.4 Fundamentals of chaotic dynamics 42

1.4.1 Definitions 42

1.4.2 Features 45

1.5 Paradigms of chaotic maps 51

1.5.1 Logistic map 53

1.5.2 Skew tent map 56

1.5.3 Piece-wise linear chaotic map (PWLCM) 58

1.5.4 Chebyshev chaotic map 60

1.5.5 Hénon map 62

1.5.6 Lozi map 63

1.5.7 Arnold's cat map 63

1.6 Conclusion 66

2 Chaos-based cryptography **67**
2.1 Introduction . . . 67
2.2 Introduction to chaos-based cryptosystem . . . 67
2.2.1 Cryptography . . . 67
2.2.2 Cryptosystem . . . 68
2.2.3 Chaos-based cryptosystem . . . 69
2.2.4 Cryptographic attacks . . . 71
2.3 State of the art . . . 73
2.3.1 Chaos-based image cryptosystem . . . 74
2.3.2 Pseudo-chaotic number generator . . . 76
2.3.3 Existing problems and solutions . . . 79
2.4 Conclusion . . . 81

3 One-dimensional chaotic maps over a finite integer field **83**
3.1 Introduction . . . 83
3.2 Reformulated chaotic maps over an integer field . . . 84
3.2.1 Logistic map . . . 84
3.2.2 Skew tent map . . . 85
3.2.3 Piece-wise linear chaotic map (PWLCM) . . . 86
3.2.4 Chebyshev chaotic map . . . 87
3.3 Effect of finite precision . . . 87
3.3.1 Period analysis in different precision N . . . 88
3.3.2 Histogram . . . 91
3.4 Key space contribution . . . 94
3.5 Conclusion . . . 95

4 Proposed chaos-based stream cipher **97**
4.1 Introduction . . . 97
4.2 Proposed stream cipher . . . 97
4.3 Performance analysis . . . 99
4.3.1 Performance analysis of the proposed PCNG . . . 99
4.3.2 Security analysis of the proposed stream cipher . . . 105
4.4 Conclusion . . . 110

5 Proposed secure and robust chaos-based image cryptosystem 113
5.1 Introduction . . . 113
5.2 Proposed cryptosystem scheme . . . 113
5.2.1 Encryption process . . . 113
5.2.2 Proposed PCNG . . . 114
5.2.3 Global diffusion . . . 115
5.2.4 Block cipher . . . 119
5.2.5 Decryption process . . . 121
5.3 Performance analysis . . . 122
5.3.1 Statistical analysis of the PCNG . . . 122
5.3.2 Security analysis of the cryptosystem . . . 124
5.3.3 Robustness analysis . . . 132
5.3.4 Computation time analysis . . . 135
5.4 Conclusion . . . 136

6 Exploring a smart coupling of chaotic maps for new pseudo-random number generators (PRNGs) 137
6.1 Introduction . . . 137
6.2 Two-dimensional coupling . . . 141
6.3 Three-dimensional coupling . . . 150
6.4 PRNG scheme based on chaotic coupling . . . 154
6.4.1 Two types of output control . . . 155
6.4.2 PRNG based on two-dimensional coupling . . . 156
6.4.3 PRNG based on three-dimensional coupling . . . 159
6.5 Key space expandable PRNG . . . 162
6.6 Conclusion . . . 165

7 Conclusion and perspectives 167
7.1 Conclusion of contributions . . . 167
7.2 Perspectives of future work . . . 169

Bibliography 169

LIST OF FIGURES

1.1 Preimages of the unstable fixed points 40
1.2 Different type of limit cycles [1] 41
1.3 A simple torus [2] 41
1.4 Smale horseshoe map [3] 44
1.5 Numerical simulation of the sensitivity to initial conditions in Lorenz system. A tiny change in 4-digit or 5-digital precision will cause qualitatively different orbits as system evolves. 45
1.6 Numerical simulation of the sensitivity to initial conditions in the logistic map (1.13). The initial conditions differing by 10^{-14} will cause a big difference in the produced sequences as the system evolves. 46
1.7 Representation of Lyapunov exponent estimation by tracing two orbits ($\{x_0, x_1, ..., x_i, ..., x_n\}$ and $\{x_0', x_1', ..., x_i', ..., x_n'\}$) evolving from a pair of nearby initial conditions (x_0 and x_0') differing by δ_0 47
1.8 Time series of each variable 49
1.9 Strange attractor of Lorenz system 50
1.10 Fractal in Julia set and Mandelbrot set [4] 51
1.11 Fractal existed in the bifurcation diagram of logistic map (self-similarity) . 52
1.12 Fractal existed in the strange attractor of Hénon map (self-similarity) 53
1.13 Lyapunov exponents diagram 54
1.14 Logistic map 54
1.15 A trajectory of the logistic map 55
1.16 Numbers produced by the logistic map 55
1.17 Probability density function 55
1.18 Histogram 55
1.19 Skew tent map 56
1.20 Bifurcation diagram of skew tent map 57
1.21 Lyapunov exponents by parameter p 57
1.22 A trajectory of the skew tent map 58
1.23 Histogram of a sequence produced by skew tent map 58

1.24 PWLCM 59
1.25 Bifurcation diagram of PWLCM 59
1.26 Lyapunov exponents of PWLCM 59
1.27 A trajectory of PWLCM 60
1.28 Histogram of a sequence produced by PWLCM 60
1.29 Chebyshev maps 61
1.30 Bifurcation diagram of chebyshev map 61
1.31 Lyapunov exponents by parameter γ 61
1.32 Density diagram 62
1.33 Histogram of 3rd order Chebyshev chaotic map 62
1.34 Bifurcation diagram of Hénon map 63
1.35 Lyapunov exponents of Hénon map 63
1.36 Attractor of Lozi map 64
1.37 Effect of Arnold's cat map 65

2.1 Encryption and decryption 68
2.2 Cryptographic elements in a symmetric-key cryptosystem 69
2.3 Scheme of the chaos-based cryptosystem 69
2.4 Scheme of the confusion-diffusion in chaos-based cryptosystem 71

3.1 Reformulated logistic map 84
3.2 Reformulated skew tent map 85
3.3 Reformulated PWLCM 86
3.4 Reformulated Chebyshev 3rd order chaotic map 87
3.5 Orbit of a chaotic system with finite precision 88
3.6 Transient length and period length tested in the above reformulated integer chaotic maps ($N = 32$) 90
3.7 Histograms of the above reformulated integer chaotic maps (red curve in the figure represents the averages of each 100 classes) 93
3.8 Histogram of a sequence generated by logistic map with $N = 16$ bits finite precision (Initial condition $X(0) = 8323$ is created randomly) 94

4.1 The proposed PCNG scheme for the stream cipher 98
4.2 Histogram of the produced key stream 101
4.3 The approximation of the probability density of the key stream X 102

4.4 Proportion of bit 0 and 1 in binary bit stream . . . 103
4.5 Plain and ciphered images and their histograms . . . 106
4.6 Correlation between adjacent pixels of $Pepper$ in horizontal (H), vertical (V) and diagonal (D) directions in plain and ciphered image . . . 109

5.1 Encryption process . . . 114
5.2 Pseudo-chaotic number generator (PCNG) . . . 115
5.3 Horizontal addition diffusion (HAD) and vertical addition diffusion (VAD) 116
5.4 HAD and VAD for processing an image with three color planes . . . 117
5.5 Eight test images with different sizes and features . . . 118
5.6 Mean D_H versus the round times rg in global diffusion$(\%)$ . . . 119
5.7 CBC mode . . . 120
5.8 Decryption process . . . 122
5.9 Histogram of the produced key stream . . . 123
5.10 The approximation of the probability density of the key stream . . . 123
5.11 Proportion of numbers of bit $'0'$ and $'1'$ . . . 124
5.12 Plain and ciphered $Lena/Goldhill/White/Black$ images and their histograms . . . 127
5.13 Correlation between adjacent pixels of $Pepper$ in three directions (H, V, D) in plain and ciphered image . . . 130
5.14 Hamming distance . . . 130
5.15 Comparison with AES-CBC . . . 130
5.16 Robustness against salt and pepper noise . . . 133
5.17 Robustness against occlusion attack . . . 134
5.18 Encryption time percentage of each component of the proposed cryptosystem for $Lena$ image with size 512×512 . . . 136

6.1 Difference between the orbit x^1 produced by the coupling scheme (6.3) and the original chaotic orbit produced by the tent map (6.1). n is the number of iterations ; the same initial conditions as in the Lozi's work : $x_0^1 = 0.330, x_0^2 = 0.3387564,\ x_0^3 = 0.50492331,\ x_0^4 = 0.0$ . . . 139
6.2 x^1 in the phase space (x_n^1, x_{n+1}^1) . . . 140
6.3 Performance of the output sequence y (length of y is 998930 which is produced by 10^9 iterations of x^1, x^2, x^3, x^4 ; the initial condition is : $x_0^1 = 0.330, x_0^2 = 0.3387564,\ x_0^3 = 0.50492331,\ x_0^4 = 0.0$.) . . . 141

6.4 2D coupling structure 142
6.5 Performance of the output sequence $X1$ [5] 144
6.6 Performance of the output sequence $X1$, $X2$ [6] 145
6.7 Histogram 147
6.8 χ^2_{exp} results versus the coupling parameter e 149
6.9 $X1$ in the phase space 149
6.10 3D coupling structure 150
6.11 Histogram of X1 generated by "SPC" 152
6.12 χ^2_{exp} results in the coupling "SPC" versus the coupling parameter $(e1, e2)$ [7] . 153
6.13 Phase space of X1 generated by "SPC" [8] 154
6.14 Alternate output control 155
6.15 Dynamic output control 156
6.16 PRNG scheme based on 2D coupling 157
6.17 PRNG scheme based on 3D coupling 160
6.18 Key space expandable PRNG scheme 163

LIST OF TABLES

1 A partial list of the relationship between the properties of chaotic system and cryptosystem 28

4.1 Time consuming results 100
4.2 P-value and Proportion results of NIST test 104
4.3 Results of the χ^2 test and entropy test 107
4.4 Correlation coefficient results 108
4.5 Hamming distance and NPCR/UACI results 110

5.1 D_H versus the round times rg in global diffusion$(\%)$ 119
5.2 P-values and Proportion results of NIST test 125
5.3 Statistic test results 126
5.4 Correlation coefficient values 129
5.5 NPCR and UACI results 131
5.6 Comparison on confusion property 131
5.7 Comparison on diffusion property 132
5.8 ET and NCpB results 135

6.1 Periods of $X1$ when $e1 = e2 = e3 = e4$ (using the same conditions with Figure 6.5) 144
6.2 Coupling performance [9] 147
6.3 Coupling performance of the produced sequence $X1$ [10] 151
6.4 Security test results 158
6.5 Statistical test results (alternate output method) 158
6.6 Statistical test results (dynamic output method) 158
6.7 NIST test results(coupling "SS") 159
6.8 Security test results 160
6.9 Statistical test results (alternate output method) 161
6.10 Statistical test results (dynamic output method) 161
6.11 NIST test results (coupling "SPC") 161
6.12 NIST test results (coupling "SSS") 162

6.13 Security and statistical test results 164
6.14 NIST test results (j=2,3) 164
6.15 NIST test results (j=4) 165

INTRODUCTION

Research Background and Motivation

Nowadays, the rapid development of information and network technology has brought an era of information explosion. Information security has attracted a high attention. Since the digital images, offering more visual information, are stored or exchanged via not only the insecure public channels such as Internet and mobile networks for personal or company use, but also through satellites in the aerospace domain of research [1], image security has become a crucial issue of great importance. There is an increasing need for secure and efficient cryptosystems.

Different from the text message, digital images have intrinsic features such as the high correlation between the adjacent pixels, bulk data capacity and high redundancy [2]. Amongst the most widely used cryptosystems, AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are authoritative traditional encryption algorithms that play an important role in protecting the information security in the world. But owing to their weak diffusion performance, they are not suitable for image encryption situations [3]. Over the years, chaotic systems appeared as excellent candidates for the designs of secure image cryptosystems.

Chaotic systems exhibit complex nonlinear dynamics. In the 20th century, chaotic dynamics went through the process of being discovered, being studied, and flourishing. Since 1990s, the interesting relationship between chaotic dynamics and cryptography has achieved considerable attention from researchers : the attractive characteristics of chaotic systems, such as ergodicity, topological mixing property, high sensitivity to initial conditions and parameters and random-like behavior are highly consistent with the primitive cryptographic requirements for secure encryption algorithms, i.e. confusion and diffusion, according to Shannon's theory of information security. Many chaotic properties have their corresponding counterparts in traditional cryptosystems and this can be found in Table 1 [4, 5].

TABLE 1 – A partial list of the relationship between the properties of chaotic system and cryptosystem

Chaotic property	Cryptographic property	Description
Ergodicity	Confusion	The output has the same distribution for any input
Topological mixing property	Confusion	The relationship between input and output is intricate
High sensitivity to initial conditions and parameters	Diffusion	A tiny change in the input can cause a big difference at the output
Random-like behavior	Random-like output	Any input can produce a random-like output
Deterministic systems	Deterministic encryption/ decryption algorithm	A deterministic scheme can generate pseudo-random outputs
Complex nonlinear dynamics	Nonlinear transformation and complex algorithm	A simple system has a high nonlinear dynamical complexity

A secure cryptosystem requires a good quality of confusion and diffusion. That means it demands a nonlinear complex relationship between the ciphered image and the plain image. It is embodied in a uniformly distributed and random-like ciphered image and a high sensitivity of the ciphered image to its plain image and secret key, etc.

Nowadays, chaotic systems have been considered to be promising in the research of image cryptosystems [6]. Many chaos-based cryptosystems have been proposed. They can be classified into chaos-based block ciphers and chaos-based stream ciphers.

A chaos-based block cipher encrypts the input plaintext block by block. The encryption scheme uses chaotic components to achieve the confusion and diffusion. The parameters needed in the encryption come from a key stream which is a pseudo-random sequence generated by a pseudo-chaotic number generator (PCNG). The level of confusion and diffusion that the encryption algorithm can achieve and the quality of the PCNG are crucial to the security of a block cipher.

A chaos-based stream cipher encrypts the plaintext continuously by masking it using the XOR operation with the key stream that is produced by a PCNG. The security of the stream cipher depends highly on the cryptographic quality of the chaotic key stream. Apart from the security, high speed is the other main requirement of a stream cipher.

For both types of cryptosystems, the key stream acts a pivotal role in the encryption process. It is produced by a PCNG which is designed based on several nonlinear chaotic maps and can generate pseudo-random numbers with enhanced chaotic features and good randomness. The initial conditions and parameters of the PCNG constitute the secret key of the cryptosystem. To ensure security, besides the randomness, the PCNG should have a large key space to resist the brute-force attack and exhibit high sensitivity to its secret key. That means, including the large key space, the PCNG should possess both chaotic and pseudo-random properties.

According to our knowledge, in the literature, although plenty of chaos-based encryption algorithms have been proposed, many of them have been verified to be vulnerable to certain kinds of attacks. The drawbacks normally lie in the aspects including insecurity, inefficiency, high consumption of computation time, difficulties of implementation, etc. More specifically, to pursue high security and robust chaos-based cryptosystems, the existing problems shown in the following cannot be ignored.

(1) Insufficient level of confusion and diffusion causes inefficiency

Confusion and diffusion are two primitive properties for strong encryption algorithms proposed by Claude Shanoon [7]. For this, chaos-based block ciphers are designed using confusion-diffusion scheme. Basically, the good confusion means that the cryptosystem is able to achieve a complicated relationship between the ciphered image, the plain image, and the secret key so as to frustrate the attempts to look for redundancies and statistical patterns by studying the ciphered image. Usually, it can be achieved by the operations of permutation (permute the order of pixels of the plain image) and substitution (substitute the plain image to change its original statistical property). Diffusion operations aim to spread out the influence of each bit of the plain image over as many pixels of the ciphered image as possible in order to increase the sensitivity of the ciphered image to a tiny change of the plain image.

Due to the insufficient level of confusion and diffusion, the confusion-diffusion scheme have to be looped a couple of rounds (iterations) to obtain a satisfactory security level. In each round (iteration), the whole image has to be scanned more than once, which causes low efficiency for the encryption algorithm and thus hinders the cryptosystem to be applied in real-time applications.

(2) Insecure and not complex enough strategy of confusion and diffusion causes an information leakage of the key stream, even the secret key, leading to insecurity

The confusion and diffusion are insecure and not complex enough, which leaves an

open door to attackers who can remove the confusion effect or diffusion effect and make it easy to crack a diffusion-only or permutation-only scheme [8, 9]. In the analysis of confusion or diffusion, it is usually possible that the key space can be reduced and the key stream can be recovered, which is not resistant to attacks.

(3) The key stream not produced by a PCNG causes the information leakage of the secret key

The key stream serves the confusion and diffusion operations and it is significant that the key stream is chaotic and pseudo-random. The PCNG has complex inner dynamics that can conceal the relationship between the secret key and the produced key stream. However, many existing designs just use simple mathematical functions or chaotic maps to produce the key stream. This can be easily cracked if the attackers use small size image with special features to disclose the relationship between key stream and the secret key. Besides, if single chaotic maps are used to generate key stream, their functions can be observed by plotting the generated key stream (x) in the phase space (x_n, x_{n+1}). Exposing the chaotic functions to attackers also leaves a security hazard.

(4) Lack of cryptographic PCNG for encryption purposes

Majority of proposed PCNGs lack comprehensive security analysis from a cryptographic point of view. Some of them either do not satisfy the randomness test or do not provide the security analysis such as key space and secret key sensitivity analysis. Thus, we can not be sure whether these PCNGs have the potential for the design of secure cryptographic systems [10, 11].

(5) Dynamical degradation of chaotic systems over finite precision platforms

The special features of chaotic systems including random-like behavior and high sensitivity to initial conditions render the latter suitable for designing PCNGs and cryptosystems.

However, the digital devices which operate with finite precision will not support the theoretical properties of chaotic systems that are exhibited in the infinite precision environment. Thus, dynamical degradation is inevitable. Due to quantization, truncation or round-off errors, the used chaotic maps may lose chaotic features owing to the finite precision. Therefore, they may drop into periodic behavior or even fixed points. As a result, the chaotic system has a risk of losing randomness, which damages the reliability of the PCNG and leads to a security breach of the cryptosystems.

In addition to this drawback, most of the proposed chaos-based cryptosystems use floating-point numbers. From the hardware perspective, the computation of floating-point numbers has the disadvantages of slow data transfer and inefficient resource utilization

when compared to the fixed-point numbers or integer numbers.

To sum up, the problems primarily exist in the strategy of confusion and diffusion (problems (1) and (2)), PCNG (problems (3) and (4)) and the issue related to implementation (problem (5)). These three aspects work together to influence the quality of a new proposed image cryptosystem. The quality includes the security, performance, and ease of implementation that are exactly the three main criteria to evaluate new cryptosystems proposed by [4].

Secure cryptosystems are always in demand. It is significant to find efficient methods to design new secure cryptosystems. To this end, it is important to explore practical modes for designing cryptographic PCNGs with large key space and good randomness properties. Also, it is necessary to find proper ways to overcome the dynamic degradation of chaotic maps to ensure a high reliability of a cryptosystem.

Organization of the thesis and main contributions

In this section, we will talk about the main content of the thesis. In this process, organization of the thesis and the main contributions will be presented.

The thesis focuses on the issue of using chaotic dynamics to the design of secure chaos-based cryptosystems and PCNGs.

For this, Chapter 1 firstly introduces the basis of nonlinear dynamics and chaotic systems. Chapter 2 gives the introduction to chaos-based cryptography. Also we make a detailed literature analysis and discuss the existing problems as well as current solutions.

The main contributions are summarized as follows.

(1) Use integer arithmetic to overcome the problems caused by floating-point notation

In Chapter 3, to avoid the quantization, truncation or round-offs operations encountered in software or hardware applications, the commonly used one-dimensional (1D) chaotic maps, including logistic map, skew tent map, piece-wise linear chaotic map (PWLCM) and Chebyshev 3rd order chaotic map, are reformulated over an N-bit (N=32) integer field. This not only guarantees the reproducibility of chaotic iterations over any kind of operation platforms with different decimal precision, but also decreases the utilization of hardware resources when compared to the floating-point notation.

(2) Propose a new secure stream cipher

Redefining the chaotic maps over a finite integer field only cannot remove the dynamical degradation. To palliate this problem, in Chapter 4, we introduce an original PCNG

scheme which is based on the logistic map, PWLCM and skew tent map. It only uses four XOR operations and a dynamic output control method, which is easy to implement. The proposed PCNG has good cryptographic properties and it can pass the NIST randomness test successfully. Based on this PCNG, a new efficient stream cipher is proposed. This stream cipher shows good statistical and security properties.

(3) Design a new secure and robust chaos-based image cryptosystem (block cipher) with good confusion and diffusion properties

Insufficient level of confusion and diffusion in the encryption algorithm is dangerous for the security of a cryptosystem. In Chapter 5, a secure robust cryptosystem based on chaotic components and the AES S-Box is proposed, which contains an efficient PCNG, a global diffusion and a block cipher. The PCNG, defined over a finite field, eliminates the risk of deteriorated security resulting from the dynamical degradation when chaotic maps defined on real numbers are numerically implemented. The global diffusion increases effectively the diffusion properties among the pixels of an image. The block cipher composed of the AES S-Box works in cipher block chaining (CBC) mode, which reinforces the performances of confusion and diffusion.

The proposed chaos-based cryptosystem can resist the main known attacks in the literature successfully, and it is suitable for practical implementations.

(4) Explore a new smart chaotic coupling method for pseudo-random number generator (PRNG) design

A PCNG is important for the security of chaos-based cryptosystems. It is primarily a PRNG. PRNGs are essential tools in a great number of applications. Chapter 6 investigates a new smart coupling for PRNG designs. The PRNG schemes have been proposed based on the smart coupling structure and two output control methods, i.e. alternate and dynamic output control methods. Different coupling combinations of the chaotic maps and two output control methods are integrated into a family of PRNGs. Furthermore, a key expandable strategy is presented for expanding the key space to improve the cryptosystem's resistance to the brute-force attack.

The proposed PRNGs can produce pseudo-random numbers with good cryptographic properties and they can be used in any designs of stream ciphers or block ciphers for encryption purposes. In addition to this, it also can be applied in PRNG required applications.

Finally, Chapter 7 concludes the thesis and gives the perspectives of this subject.

CHAPITRE 1

NONLINEAR DYNAMICS AND CHAOTIC SYSTEMS

1.1 Introduction

Chaotic systems exhibit special complex nonlinear dynamic behavior. First of all, the major discoveries in the history of chaotic dynamics will be briefly presented in Section 1.2. Then, we will give the fundamentals of nonlinear dynamical system related to chaotic systems in Section 1.3. After that, Section 1.4 is focused on chaotic systems. Although, up to now, there is not a universally agreed mathematical definition of the chaotic system, three well accepted definitions, that is Li-Yorke, Devaney and Smale definitions, will be introduced in Section 1.4.1. They describe chaotic dynamics from different perspectives for revealing its specific properties. In addition to the definitions, some typical features appear to be important in the study of complex chaotic dynamics. And they will be discussed in detail in Section 1.4.2. After that, several representative low-dimensional chaotic maps will be analyzed in Section 1.5.

1.2 Historical perspective of chaotic dynamics

Chaotic dynamics is considered to be the third major discovery of physics in the 20th century together with the relativity theory and quantum mechanics. Similar to the previous two revolutions, chaos also breaks the canon of Newtonian mechanics. The most passionate advocates of the new science once said : "Relativity, quantum mechanics and chaos are three things in the twentieth-century that science will always remember" [12, 13].

The first discovery of chaotic behavior can be dated back to 1890 when Poincaré, a French mathematician, conducted an in-depth study on the three-body problem. He found that in the there-body problem, the interaction between them showed huge complexity, and

it had no accurate solutions. Besides, by applying relevant knowledge of dynamics and topology, he discovered that, within a certain range, the solution of the three-body problem was random [14]. This finding indicated that even in a certain (deterministic) system, the trajectory of the system might be extremely unstable, and any slight change in the initial condition would lead to completely different results. This is the first time that many scientists begin to realize that there might exist inherent randomness, i.e. chaotic dynamics, in a deterministic system [15, 16].

The 1960s and 1970s were an era of rapid development in the field of chaotic dynamics research. Around 1960, based on the study of the stability of motion in the Hamiltonian system, Kolmogorov, Arnold and Moser proposed the famous KAM theorem in hamiltonian mechanics, which laid the foundation for chaos theory [17].

In 1963, Lorenz published an influential paper called “Deterministic nonperiodic flow” in “Journal of the Atmospheric Sciences”. In this paper, he proposed a three-dimensional (3D) autonomous system to describe weather change. This is the famous Lorenz system which is the first chaos model with a mathematical description. He found the evolution of weather was closely related to the initial conditions. In other words, in a deterministic dynamical system, a slight change in the initial condition will cause a significant difference in the output, which is exactly the typical feature of chaos : high sensitivity to the initial condition. He also gave a beautiful metaphor known as “butterfly effect” to describe this behavior [18].

In 1964, Sharkovsky proposed the famous theorem about the coexistence of cycles with different periods in a continuous map of an interval into itself, and he gave also the period ordering [19]. In addition, Hénon proposed a two-dimensional (2D) discrete-time dynamic system, that’s Hénon map, which is one of the most studied chaotic maps. In 1971, D.Ruelle and F.Takens published a famous paper "On the essence of turbulence", which used chaos to explain the nature of turbulence for the first time. They found that the dynamic system has a particularly complex new attractor and they coined it as “strange attractor". Also, they introduced it into the dissipative system and proved that the motion related to this strange attractor is chaotic [20].

Also, in the study of turbulence, Smale discovered a "horseshoe" structure, that is “Smale horseshoe attractor” [21]. It can be seen as taking two arbitrary points on a dough and the dough is stretched and then folded continuously, which makes it intricately nested in itself and thus forms the Smale horseshoe attractor. This figurative metaphor reveals the complex nature of the chaotic system. This is another important chaotic attractor after the

Lorenz attractor.

In the paper of “Period three implies chaos”, Li and Yorke initiated "chaos". Since then, “chaos” has been officially used in the research field [22].

In 1976, May.R published a paper "Simple mathematical models with very complicated dynamics" in "Nature" [23]. In the paper, he analyzed a prey-predator model, i.e. logistic map that was firstly studied by P.J. Myrberg [24]. Also, he pointed out that period-doubling bifurcation and chaos existed in such an apparently simple 1D map. Then, two years later, Feigenbaum proposed two universal constants that lead from period-doubling bifurcation to chaos : the convergence constant δ and the scaling constant α, which laid the foundation for the study of the chaotic behavior of 1D maps.

In 1989, from the perspective of topology, Devaney gave another mathematical definition of chaos, which indicated that a chaotic system should have sensitivity to initial condition, topological transitivity and periodic point density [25, 26]. Up to now, the Devaney definition, the horseshoe chaos proposed by Smale and the chaos definition proposed by Li-Yorke are regarded as the three alternative definitions of chaos.

Since the 1990s, the study of chaotic dynamics has developed rapidly. A number of research work has been done to investigate the theoretical properties of chaotic systems [27–30]. Nowadays, theory of chaos is important not only in the field of meteorology, turbulence and biology, but also in many other disciplines, such as mathematics, physics [31], chemistry [32], economics [33, 34], sociology, philosophy, engineering, information science, etc.

1.3 Fundamentals of nonlinear dynamical system

A dynamical system is described by a mathematical model in which the explaining functions represent the evolution of a solution with time and, sometimes, with other varying parameters. If a dynamical system can be described using a set of linear functions, it is considered to be a linear dynamical system. However, most phenomena in nature are nonlinear. A nonlinear dynamical system is used to describe a physical model that can be represented by a set of nonlinear equations such as algebraic, differential, integral, functional, difference, or abstract operator equations [35]. In reality, nonlinear dynamical systems can depict a great variety of scientific and engineering phenomena. The theory of nonlinear dynamical system is very important to analyze and solve the problems in various disciplines including but not limited to mathematics, physics, chemistry, biology, economics,

medicine, and engineering. In this chapter, we just focus on the fundamentals related to chaotic systems and pay special attention to some features which are particularly important from the prospective of cryptography applications.

1.3.1 Continuous-time system

Most continuous-time nonlinear dynamical systems can be described by a differential equation :

$$\dot{\mathbf{x}} = \mathbf{f}\left(\mathbf{x}, t; \mathbf{p}\right), \ t \in [t_0, \infty) \tag{1.1}$$

where $\mathbf{x} = \mathbf{x}\left(t\right)$ is the *state* of the system that usually belongs to a bounded region $\Omega_{\mathrm{x}} \subset \mathbb{R}^{\mathrm{r}}$, where n denotes the dimension of state variable $\mathbf{x}$; the initial time is t_0 and the initial condition is $\mathbf{x}_0 = \mathbf{x}\left(t_0\right) \in \Omega_{\mathrm{x}}$; $\mathbf{p} \subset \mathbb{R}^{\mathrm{m}}$ is the vector of system *parameters* that usually varies within a bounded range and often there is $m \leqslant r$; $\mathbf{f}$ is a nonlinear or piece-wise linear function that depicts explicitly a specified system defined by physical, technological or other reasons.

1.3.2 Discrete-time system

Different from the continuous-time system where the states vary by continuous time, the discrete-time system, also called the discrete system or map, has its states only at regularly distributed instants. A discrete-time nonlinear dynamical system can be described by a difference equation or a map :

$$\mathbf{x}_{n+1} = \mathbf{f}\left(\mathbf{x}_n, n; \mathbf{p}\right), \ n = 0, 1, 2... \tag{1.2}$$

where n is the time index ; $n = 0$ means the initial time ; $\mathbf{x}_0$ is the initial condition for the state x. Other notations are similarly defined as those in the continuous-time system (1.1).

In a discrete-time system, the current state $\mathbf{x}_n$ is the iteration result of its previous state $\mathbf{x}_{n-1}$ by function $\mathbf{f}$ and the previous one $\mathbf{x}_{n-1}$ also has same mode with $\mathbf{x}_{n-2}$, so that the state of the system can be presented by the initial condition $\mathbf{x}_0$:

$$\begin{aligned} \mathbf{x}_n &= \mathbf{f}\left(\mathbf{x}_{n-1}\right) = \mathbf{f}^{[2]}\left(\mathbf{x}_{n-2}\right) = ... = \mathbf{f}^{[n]}\left(\mathbf{x}_0\right) \\ &= \underbrace{\mathbf{f} \circ \cdots \circ \mathbf{f}}_{n \ times}\left(\mathbf{x}_0\right) \end{aligned} \tag{1.3}$$

where symbol " $\circ$ " denotes the composition of two functions.

We shall see in the following chapters that, in the chaos-based cryptosystems, in theory, both continuous-time and discrete-time systems can be used. However, in reality, digital operating platforms cannot support the continuous nature of the system variables, or signals. So, to perform the continuous-time system on digital devices, discretization of the continuous states or discrete approximations of the system have to be applied. In addition, finding the solutions of differential functions costs computational capacity and hardware resources [11]. By contrast, the discrete-time systems accomplish by iterative functions defined over a discrete time domain. Hence, there are no discretization operations and no heavy computational burden. Thus, discrete systems are more suitable to cryptosystem applications. In this work, we choose to cope with the discrete chaotic maps for encryption design. In the following, we will mainly deal with the discrete systems, but the typical examples using continuous-time systems will be introduced as well in this chapter.

1.3.3 Notions of dynamical system

- *Autonomous* and *Nonautonomous*

Definition 1.1. [35] *A nonlinear system (1.1), (1.2) is said to be autonomous, if its describing function* **f** *is independent explicitly on time (t in (1.1), n in (1.2)). In this case,*

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}; \mathbf{p}) \tag{1.4}$$

$$\mathbf{x}_{n+1} = \mathbf{f}(\mathbf{x}_n; \mathbf{p}) \tag{1.5}$$

Otherwise, if the describing function **f** *depends explicitly on time, i.e, (1.1), (1.2), the system is said to be nonautonomous.*

It should be noted that, **f** is not the same function for the continuous system (1.4) and discrete system (1.5).

In this thesis, the dynamical systems we adopted for cryptography are all autonomous.

- *Phase space*

Phase space, also called *state space*, represents the entire space that comprises all states (**x** in (1.1),(1.4) and (1.2),(1.5)) of a dynamical system. For an n-dimensional system, the phase space expands by its evolving states **x**. For a 1D discrete system, phase space can be constructed by the iteration states in the space (x_n, x_{n+1}), and the graph shown in the phase space coincides with the graph of the 1D function.

- *Orbit*

The evolution of a dynamical system is embodied in a *trajectory* of the states traveled from the initial state $\mathbf{x}_0$ in the phase space. This trajectory is called an *orbit* of the system. The dynamics of the system can be observed by its orbits in phase space.

- *Deterministic system*

A dynamical system is *deterministic*, if there is a unique consequence to every change of the system's parameters or initial conditions. Otherwise, it is *stochastic* or *random*, if there exists more than one possible consequence for a change in its parameters or initial conditions according to some probability distribution [35].

Chaotic system is deterministic, which indicates different orbits started from different initial conditions will never intersect (in infinite precision conditions). In other words, it guarantees the uniqueness of the evolution of a system for a given initial condition. This property links chaotic dynamics and cryptography : due to the deterministic dynamics, unique chaotic sequence can be only generated by a chaotic system using unique specific initial condition and parameters. This corresponds the uniqueness of the key stream (pseudo-random numbers from a PCNG) to a specified secret key (initial conditions and parameters).

- *Fixed point*

Fixed point, also called *equilibrium point* and *invariant point*, of a dynamical system is an equilibrium state x_{fp}. According to [36], there are the following definitions and theorems.

Definition 1.2. *If f is a function and $f(c) = c$, then c is a fixed point (x_{fp}) of f.*

For the continuous time system (1.4),

$$\mathbf{f}\left(x_{fp}; \mathbf{p}\right) = 0 \tag{1.6}$$

For the discrete time system (1.5), if it describes a 1D chaotic map, the fixed points are the intersections of $\mathbf{f}\left(\mathbf{x}; \mathbf{p}\right)$ with the function $\mathbf{f}\left(\mathbf{x}\right) = \mathbf{x}$, meaning the orbits remain locked at the fixed point despite the iteration evolving. That is,

$$x_{fp} = \mathbf{f}\left(x_{fp}; \mathbf{p}\right) \tag{1.7}$$

Theorem 1.3. *Let $I = [a, b]$ be a closed interval and $f : I \to I$ be a continuous function. Then f has a fixed point in I.*

Proof. *If $f(a) = a$ or $f(b) = b$, then $x_{fp} = a$ or b. If $f(a) \neq a$ and $f(b) \neq b$. Let $g(x) = f(x) - x$. As $f(a) \neq a$ and $f(a) \in [a, b]$, $f(a) > a$. Likewise, $f(b) < b$. Hence, $g(a) = f(a) - a > 0$ and $g(b) = f(b) - b < 0$. Since $g(x)$ is the difference of continuous functions, it is a continuous function. According to the Intermediate Value Theorem (Bolzano Theorem)* [1]*, there exists $c \in [a, b]$ such that $g(c) = 0$. But $g(c) = f(c) - c = 0$ so that $f(c) = c$. Thus, $x_{fp} = c$. Theorem 1.3 has been proven to be true.*

Theorem 1.3 states that if a dynamical system can be described by a continuous function which maps in a closed invariant set, it has at least one fixed point.

Theorem 1.4. *Let x_{fp} be a fixed point of a function f. f is differentiable at x_{fp} and suppose its derivative $f'(x)$ is continuous. If $|f'(x_{fp})| < 1$, then there exists an open interval U containing x_{fp} such that whenever x is in U, then $f^{[n]}(x)$ converges to x_{fp} and x_{fp} is said to be a stable fixed point. If $|f'(x_{fp})| > 1$, then there exists an open interval containing x_{fp} such that all points in the interval that are not equal to x_{fp} must leave the interval under iteration of f.*

Loosely speaking, if the nearby orbits of the fixed point evolve toward it, the fixed point is *stable* or *attractive* ; if they move away from it, it is said to be *unstable* or *repulsive*.

In the design of chaos-based cryptosystem, both the stable and unstable fixed points must be avoided carefully. Otherwise, the orbits can be locked into the fixed points and lose the chaotic properties, which is an undesired behavior when applying chaotic systems to cryptography.

Definition 1.5. *The point x is an eventually fixed point of a function f if there exists N such that $f^{n+1}(x) = f^n(x)$ whenever $n \geqslant N$.*

Definition 1.5 states that there exist a type of points that are eventually fixed points. This type of points are *preimages* (backward iterates) of the fixed points. An example can be found in the logistic map ((1.13) in Section 1.5.1) : $x_{n+1} = f(x_n) = \mu x_n(1 - x_n)$. If $\mu = 4$, the point $x_n = 0$ is an unstable fixed point, while its preimages $x_{n-1} = 1$ and $x_{n-2} = \frac{1}{2}$ are not fixed points. But $f(1) = 0$ and $f^{[2]}(\frac{1}{2}) = 0$. So after one iteration, point $x_{n-1} = 1$ is fixed at 0 ; after two iterations, point $x_{n-2} = \frac{1}{2}$ is fixed at 0. Likewise, the point $\frac{1}{4}$ also leads to the fixed point $\frac{3}{4}$ after one iteration. Their orbits can be seen in Figure 1.1.

1. Weisstein, Eric W. "Bolzano's Theorem." From MathWorld–A Wolfram Web Resource. https ://mathworld.wolfram.com/BolzanosTheorem.html

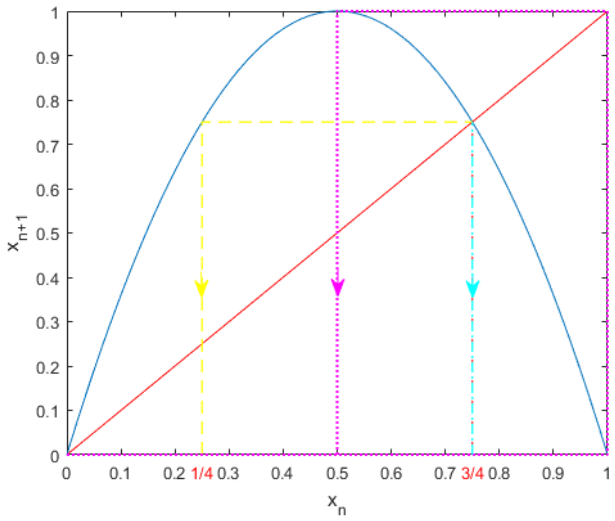


FIGURE 1.1 – Preimages of the unstable fixed points

Theoretically, in the logistic map, one fixed point (x_{fp}) corresponds to two preimages. These two preimages correspond to 2^2 preimages. Therefore, one fixed point (x_{fp}) has $2+2^2+2^3+2^4+...+2^n$ (n backward iterations) preimages, and all of them will lead to the fixed point (x_{fp}). If the initial condition of a chaotic map accidentally (randomly) coincides with one of the preimages of x_{fp}, after a number of iterations, its orbit will be eventually locked into x_{fp}. Since huge amount of preimages of the fixed point exist, ensuring chaotic behavior while avoiding all the preimages is quite a tricky task. This is not specific only for the logistic map, since the majority of 1D chaotic maps show similar cases.

- *Periodic point*

Definition 1.6. *For a discrete dynamical system (1.5), the point x is a periodic point of f with period k if $f^{[k]}(x) = x$. In other words, a point is a periodic point of f with period k if it is a fixed point of $f^{[k]}$. The periodic point x has prime period k_0 if $f^{[k_0]}(x) = x$ and $f^{[n]}(x) \neq x$ whenever $0 < n < k_0$. That is, a periodic point has prime period k_0 if it returns to its starting place for the first time after exactly k_0 iterations of f* [36].

Definition 1.7. *The set of the iterates started with a periodic point x is called a periodic orbit or a periodic cycle* [36].

Definition 1.8. *The point x is eventually periodic of a function f with period k if there exists N such that $f^{[n+k]} = f^{[n]}(x)$ whenever $n \geqslant N$* [36].

- *Limit cycle*

Limit cycle is a closed periodic orbit of a continuous dynamical system. It can be seen in the phase space. Figure 1.2 shows the different type of limit cycles, where (a) is an *inner limit cycle*, (b) an *outer limit cycle*, (c) a *stable limit cycle*, (d) an *unstable limit cycle*, (e) and (f) *saddle limit cycles*.

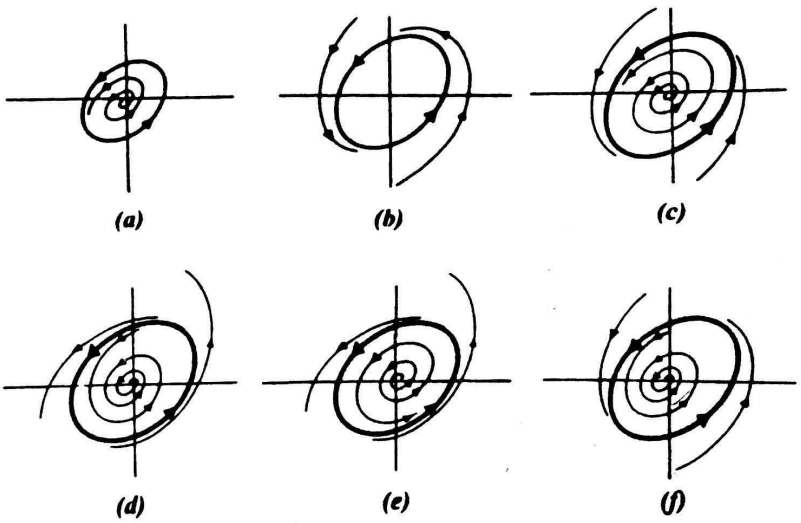


FIGURE 1.2 – Different type of limit cycles [2]

- *Torus*

A torus is also a closed curve in the phase space of a continuous dynamical system. It corresponds to a quasi-periodic motion that shows a coexistence of multiple incommensurate frequencies.

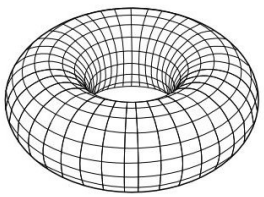


FIGURE 1.3 – A simple torus [3]

2. Reference [35]
3. $https://commons.wikimedia.org/wiki/Category:Torus\#/media/File:Simple_Torus.svg$

- *Attractor*

In the nonlinear dissipative dynamical system, the volume of phase space formed by the state evolution decreases with time [37]. The orbits in the phase space (S) may eventually converge to a subset $A \subset S$ that is referred as an *attractor*. Strictly speaking, according to [38], there are following definitions :

Definition 1.9. *A set A is an invariant set by f if $f(A) = A$.*

Definition 1.10. *A closed invariant set A is an attracting set if an arbitrary small neighborhood U of A exists such that $f(U) \subset U$ and $f^{[n]}(x) \to A$, when $n \to \infty$ for any $x \in U$.*

Definition 1.11. *An attractor is an attracting set which is topologically transitive, i.e. if for any two open sets $U, V \subset A$, a positive integer k exists such that $f^{[k]}(U) \cap V \neq \varnothing$, or equivalently a point $p \in A$ exists the orbit of which is dense in A.*

Definition 1.12. *The basin of attraction $D(A)$ (or simply the basin) of an attracting set A is the open set of all the points x such that $f^{[n]}(x) \to A$, when $n \to \infty$.*

Typically, the basic attractor can exhibit different geometries such as fixed point, periodic point, torus, and strange attractor.

- *Strange attractor*.

A strange attractor is a complex attractor that shows sensitivity to its initial conditions with a *fractal* geometry. It is a typical characteristic of chaotic dynamics [35]. We will have detailed discussions in Section 1.4.2.

1.4 Fundamentals of chaotic dynamics

1.4.1 Definitions

Chaotic dynamics exhibits a random-like behavior. This kind of randomness is not induced by an external random input, but by the system itself. Unlike other known deterministic systems, the orbit of a chaotic system is unpredictable in a long term. Although chaotic behavior is disordered apparently, it has an ordered structure inside.

Chaotic dynamics is a ubiquitous phenomenon in nature. However, there is no universally agreed definition of chaos so far. The existing definitions given in mathematical terms

describe chaos from different perspectives. Among them, three well accepted ones are Li-Yorke definition, Devaney definition and Smale definition that describe chaos from orbits aspect, topological aspect and geometrical aspect respectively.

In 1975, Tianyan Li and his supervisor James Yorke gave the first definition of chaos and they also coined the term "chaos".

Li-Yorke Definition [22] A continuous map $f : I \to I$ is called chaotic in the sense of Li and Yorke if it satisfies :

(1) for any $k = 1, 2, 3...$, f has periodic points ;

(2) there exists an uncountable subset $S \subset I$ with the following conditions :

(a.) $\forall\ x, y \in S$, $\lim\limits_{n\to\infty} \inf \left|f^{[n]}(x) - f^{[n]}(y)\right| = 0$;

(b.) $\forall x, y \in S,\ x \neq y$, $\lim\limits_{n\to\infty} \sup \left|f^{[n]}(x) - f^{[n]}(y)\right| > 0$;

(c.) $\forall x \in S$, y is a periodic point of f, $\forall\ y$, $\lim\limits_{n\to\infty} \sup \left|f^{[n]}(x) - f^{[n]}(y)\right| > 0$.

This definition indicates that a deterministic system can exhibit periodic or aperiodic behavior using different initial conditions. Any two different aperiodic orbits can be very close to each other and can move away from each other. Any aperiodic orbit cannot be approximated by a periodic orbit, that is, there exists no asymptotic periodic point in this area.

Devaney Definition [25, 26] A continuous map $f : S \to S$, where S is generally a compact and invariant set in $\mathbb{R}^n$, is said to be chaotic if :

(1) f displays a sensitive dependence on initial conditions, namely, $\exists\ \varepsilon > 0$, $\forall x$ and its neighborhood U, there exists $x, y \in U$, $n \in \mathbb{Z}^+$ that satisfies

$$\left|f^{[n]}(x) - f^{[n]}(y)\right| > \varepsilon\ ;$$

(2) f is transitive on S, namely, for any pair of nonempty open sets $U \subset S$ and $V \subset S$, there is an integer $k \in \mathbb{Z}^+$, and satisfies

$$f^{[k]}(U) \cap V \neq \varnothing\ ;$$

(3) the periodic points of f are dense in S.

The sensitivity of f to its initial conditions means two very close points x and y, under the influence of f , will move away from each other within the attractor. Thus, the chaotic orbit is unpredictable in a long term. Notice that, it is unnecessary that all the points close to x should be evolving separately from x, but there must exists at least one such point.

The topological transitivity means that for any point in any set U, under the influence

of f, it can appear in any other set V. This implies the chaotic orbits are ergodic.

The periodic point density seems a paradox of chaos since a random-like evolution in time is based on the existence of a dense distribution of periodic points, which are unstable and determine the complex dynamics of chaotic nonlinear dynamical systems. However, this property just reveals the chaotic behavior is not completely disordered, but it contains order in an apparent disorder.

In Devaney's definition, the sensitivity to initial conditions and the topological transitivity indicate chaotic dynamics has randomness features, and meanwhile, the periodic point density implies chaotic dynamics has regularity inside.

Smale Definition S. Smale introduced a "Smale horseshoe map" to define chaos geometrically. This map describes a class of chaotic maps f of the square that transform from its definition region S to itself. This process is squishing the square in a direction first, and then stretching it into a long strip in other direction, and then folding the strip into S in a shape of horseshoe, which can be described in Figure 1.4.

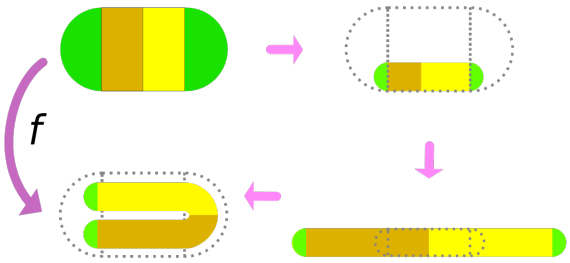


FIGURE 1.4 – Smale horseshoe map [4]

The nonlinear operations of stretching and folding lead to a topological *mixing* which makes the dynamical orbit exhibit complex behavior in the phase space. Stretching makes orbits evolve separately and folding makes the points in separated orbits possible to be close to each other. Continuous stretching and folding in the phase space make the orbits interwoven and entangled, separated and assembled, thus this can completely hides the initial conditions and also all the connections between the past states and the future states. Eventually the map will exhibit chaotic behavior. In addition, mixing makes a small area element undergo considerable distortions and it is wrapped densely over the attractor. Thus, mixing implies *ergodicity*, i.e. the orbits of a chaotic system will pass close to nearly all the dynamical states in its attractor [37]. Smale definition also graphically explains the chaotic features proposed in Li-Yorke and Devaney definitions.

4. $https://en.wikipedia.org/wiki/Horseshoe_map\#/media/File:Smale_Horseshoe_Map.svg$

1.4.2 Features

Although there is no unified definitions, chaos has been widely acknowledged that it possesses a commonly accepted concepts and properties.

High sensitivity to initial conditions and parameters

A typical feature of chaotic dynamics is its high sensitivity to initial conditions and parameters : two similar (close without being identical) initial conditions or parameters can give rise to two dramatically different future orbits. Thus, an arbitrary small change or perturbation of the current state may cause significantly different future behavior. This phenomenon is known as "butterfly effect", a famous metaphor that was firstly proposed by Lorenz, who used the flapping wing of a butterfly to represent a small change in the initial conditions of a dynamical system, and this flapping would cause a chain of events that may greatly alter the future weather meaning the evolving orbits would change significantly [39].

Lorenz system is a simplified model of the Earth atmosphere. Due to the large sequence and limited computing power in 1960s, he split the large data into subsequences with smaller sizes and initiated the next subsequence with the previous result with a lower precision. However, he noticed that the model did not duplicate the expected evolution. A simulation of this behavior based on Lorenz system can be found in Figure 1.5, where y_0 is the initial condition of a variable (y) in Lorenz map (1.12).

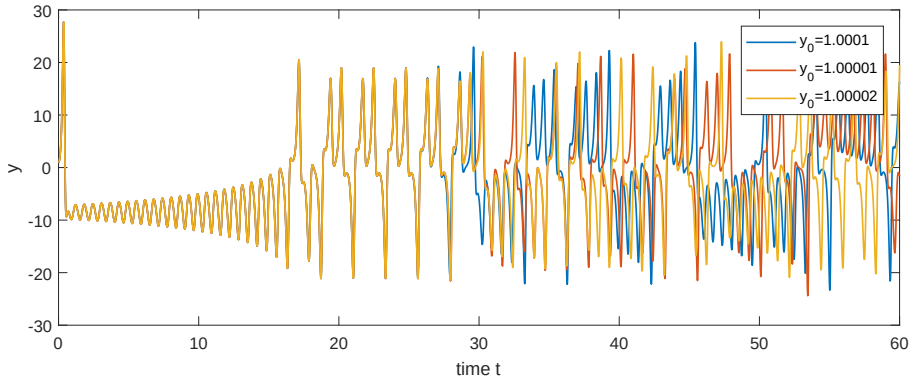


FIGURE 1.5 – Numerical simulation of the sensitivity to initial conditions in Lorenz system. A tiny change in 4-digit or 5-digital precision will cause qualitatively different orbits as system evolves.

The high sensitivity behavior also can be observed in discrete chaotic maps. For instance, in the logistic map (1.13), if there is a tiny difference in the initial conditions (x_0), as can be seen from Figure 1.6, the produced chaotic sequences will exhibit a big difference as the system evolves.

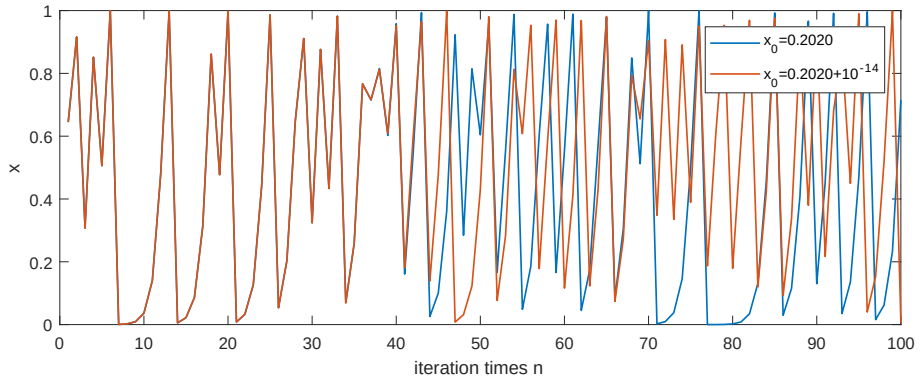


FIGURE 1.6 – Numerical simulation of the sensitivity to initial conditions in the logistic map (1.13). The initial conditions differing by 10^{-14} will cause a big difference in the produced sequences as the system evolves.

It should be noticed that chaotic systems, being deterministic, are short-term predictable within a certain allowable small tolerance. However, due to the high sensitivity to initial conditions, chaotic systems are long-term unpredictable. This is the crucial distinction with the general nonlinear deterministic dynamical systems where the future behavior can be predicted from the initial condition.

Therefore, this property can allow to distinguish chaotic system from other deterministic dynamical systems [35].

Positive Lyapunov exponent

The high sensitivity existed in chaotic systems can be evaluated by the positive Lyapunov exponents. Lyapunov exponent is an important measure to qualitatively and quantitatively describe the characterization of a dynamical behavior. It measures the average exponential rate of divergence of nearby orbits. A positive Lyapunov exponent indicates the system is chaotic and the larger this value is, the stronger the chaotic performance is.

Considering a chaotic system **f**, there is an initial condition $\mathbf{x}_0$ and a nearby point $\mathbf{x}_0 + \delta_0$ as shown in Figure 1.7. After n iterations, the states evolving from these initial conditions

may separate by δ_n. If the orbit travels exponentially fast, approximately, δ_n satisfies :

$$\delta_n \approx \delta_0 e^{n\lambda} \tag{1.8}$$

where λ is the Lyapunov exponent.

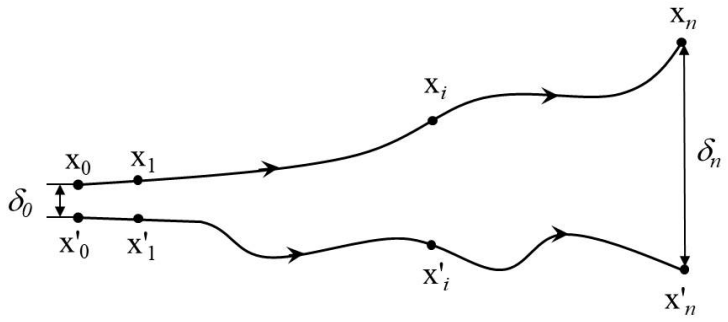


FIGURE 1.7 – Representation of Lyapunov exponent estimation by tracing two orbits ($\{x_0, x_1, ..., x_i, ..., x_n\}$ and $\{x_0', x_1', ..., x_i', ..., x_n'\}$) evolving from a pair of nearby initial conditions (x_0 and x_0') differing by δ_0

Thus, Lyapunov exponent (λ) can be estimated by

$$\lambda = \lim_{n\to\infty} \lim_{\delta_0\to 0} \frac{1}{n} \ln \frac{\delta_n}{\delta_0} \tag{1.9}$$

For 1D discrete chaotic maps $x_{n+1} = f(x_n)$, recalling (1.3), that is $x_n = f(x_{n-1}) = f^{[2]}(x_{n-2}) = ... = f^{[n]}(x_0)$, Lyapunov exponent ($\lambda$) can be further deduced by :

$$\begin{aligned} \lambda &= \lim_{n\to\infty} \lim_{\delta_0\to 0} \frac{1}{n} \ln \frac{\delta_n}{\delta_0} \\ &= \lim_{n\to\infty} \lim_{\delta_0\to 0} \frac{1}{n} \ln \left| \frac{f^{[n]}(x_0+\delta_0) - f^{[n]}(x_0)}{\delta_0} \right| \\ &= \lim_{n\to\infty} \frac{1}{n} \ln \left| \left(f^{[n]}\right)'(x_0) \right| \end{aligned} \tag{1.10}$$

Since

$$\left(f^{[n]}\right)'(x_0) = \left.\frac{\mathrm{d}f^{[n]}(x)}{\mathrm{d}x}\right|_{x=x_0} = f'(x_{n-1}) f'(x_{n-2}) \cdots f'(x_0) = \prod_{i=0}^{n-1} f'(x_i),$$

then

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \ln \left| \prod_{i=0}^{n-1} f^{'}(x_i) \right| = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| f^{'}(x_i) \right| \tag{1.11}$$

According to Lyapunov exponent (λ) calculated in (1.10), (1.11), $\lambda < 0$ indicates the orbits started from two nearby points will converge to a stable equilibrium after multiple iterations, which corresponds to the fixed point or the periodic point ; $\lambda > 0$ indicates the nearby points will move away from each other, which means a chaotic motion ; $\lambda = 0$ means the bifurcation points that imply a collision or a change of stability (i.e. appearance or disappearance of periodic or chaotic orbits).

Strange attractor

In a usual dynamical system, normally, an attractor is an invariant set with integer dimensions that implies a bounded region where the trajectory of a dissipative dynamical system is asymptotically localized. It means the final state of motion. All the other points in phase space will converge to the attractor.

However, by contrast, the attractor in chaotic system can be different from the above one. In chaotic system, there exist two contrary motions : on one hand, the dissipation plays a stabilizing role on the whole to shrink the trajectories ; on the other hand, from a local perspective, due to the extreme sensitivity of the chaotic system to its initial conditions, adjacent orbits repel and separate from each other. Thus, in the entire phase space, distant orbits converge to a limited range (i.e. chaotic attractor), while locally, the orbits move apart from each other. In this way, the chaotic orbit can move closer, and then move apart, and then fold back to move closer, and then separate. Repeating infinitely this movement (convergence and divergence) forms a complex structure : strange attractor.

Strange attractor is originally termed by D.Ruelle and F.Takens [20]. The word "strange" is based on not only the trajectory knotty discussed above, but also the complex structure and specific properties of the chaotic attractors that will be detailed in the following subsection. In other words, a strange attractor is a bounded attractor which, on one hand, shows high sensitivity to initial conditions, and on the other hand, is a kind of dense set and thus cannot be decomposed into two invariant subsets covered by disjoint open sets [35]. It reflects a seemingly ordered geometric structure in phase space of a chaotic orbit, while in time evolution, the orbit exhibits a random-like behavior. Strange attractor is often used to characterize chaotic dynamics. But it should be noted that not all strange attractors imply chaotic dynamics [40].

For illustration, consider a well-known strange attractor "Lorenz strange attractor" in Lorenz system which is a simplified model of convection in the atmosphere defined by three ordinary differential equations :

$$\begin{cases} \dot{x} = \sigma (y - x) \\ \dot{y} = \rho x - y - xz \\ \dot{z} = xy - \beta z \end{cases} \tag{1.12}$$

where x, y, z are three variables and parameters σ, ρ and β are all positive values. When $\sigma = 10$, $\rho = 28$, $\beta = \frac{8}{3}$, the system is chaotic.

The Lorenz strange attractor in time series is plotted in Figure 1.8, where the evolving states seem disordered.

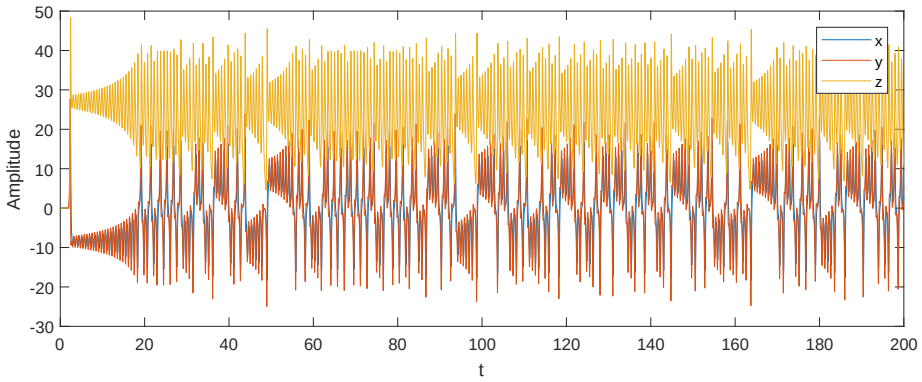
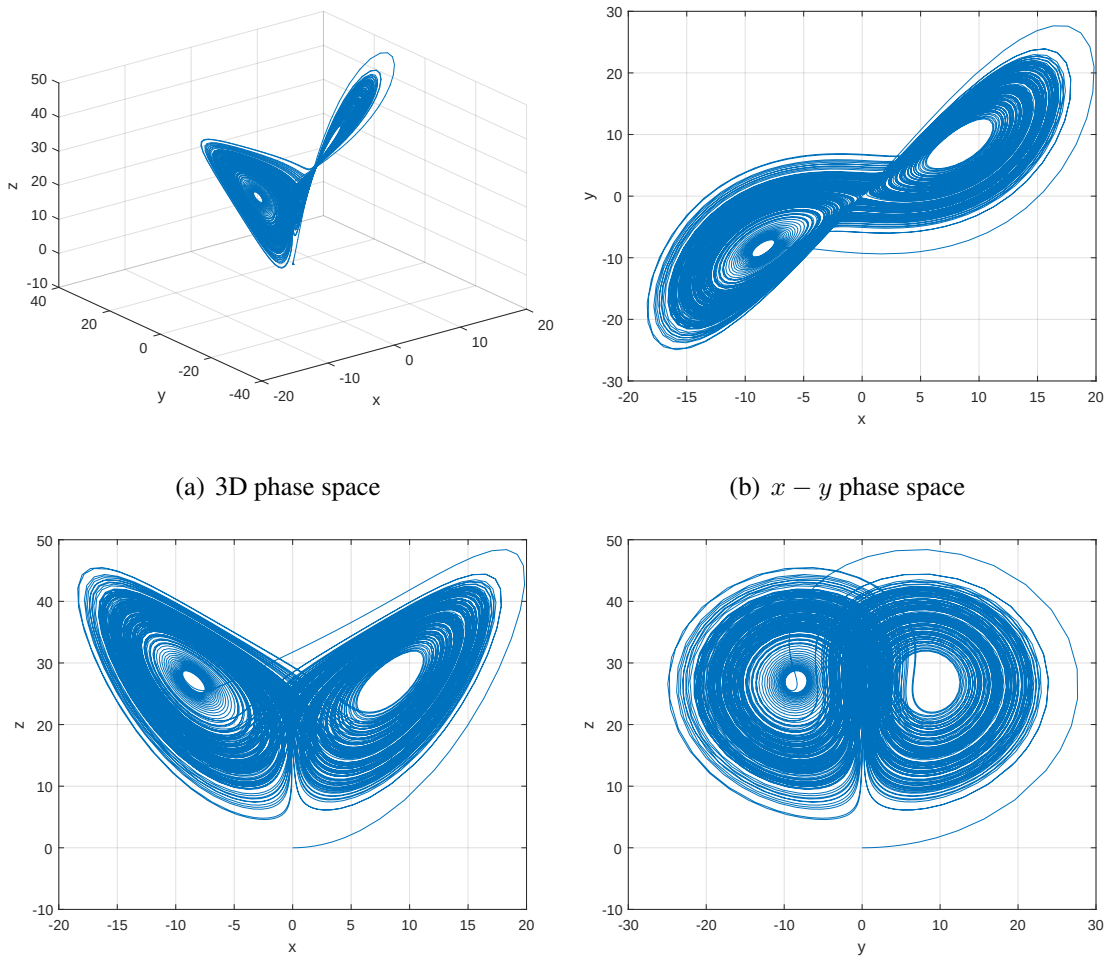


FIGURE 1.8 – Time series of each variable

However, the Lorenz strange attractor in phase space shown in Figure 1.9 displays a specific shape. Especially, in $x - z$ phase space (see Figure 1.9(c)), the strange attractor shows the famous "butterfly" shape. Nevertheless, although it looks like it has a pattern, the orbits never intersect in the 3D phase space and it is completely arbitrary that the orbit travels in the "butterfly".

A strange attractor has a complex structure. The complexity of chaotic dynamics and strange attractor has a strong link to fractal that is characterized with non-integer dimension and self-similarity. In addition, the complexity is also embodied in the finite Kolmogorov-Sinai entropy that is another important feature of chaotic systems and strange attractors.



(a) 3D phase space

(b) $x - y$ phase space

(c) $x - z$ phase space

(d) $y - z$ phase space

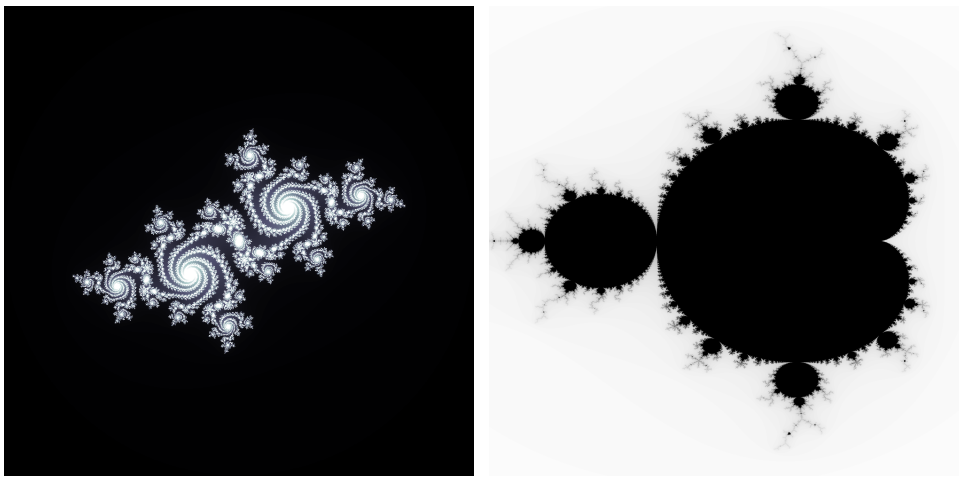
FIGURE 1.9 – Strange attractor of Lorenz system

Fractal and self-similarity

A fractal is a special set that does not look like the Euclidean set such as point, line, and plane, etc. A fractal has a fractional dimension and a certain self-similarity. Fractal was first coined by Mandelbrot who studied fractals of Julia set and Mandelbrot set that showed a beautiful symmetry and self-similarity as shown in Figure 1.10 : a portion of the figure has the same structure and complexity as the entire picture.

A chaotic dynamical systems sometimes exhibit fractal structure. Typical examples can be found in the bifurcation diagram of logistic map (see Equation (1.13) in the following

5. Reference [41]



(a) Julia set (b) Mandelbrot set

FIGURE 1.10 – Fractal in Julia set and Mandelbrot set [5]

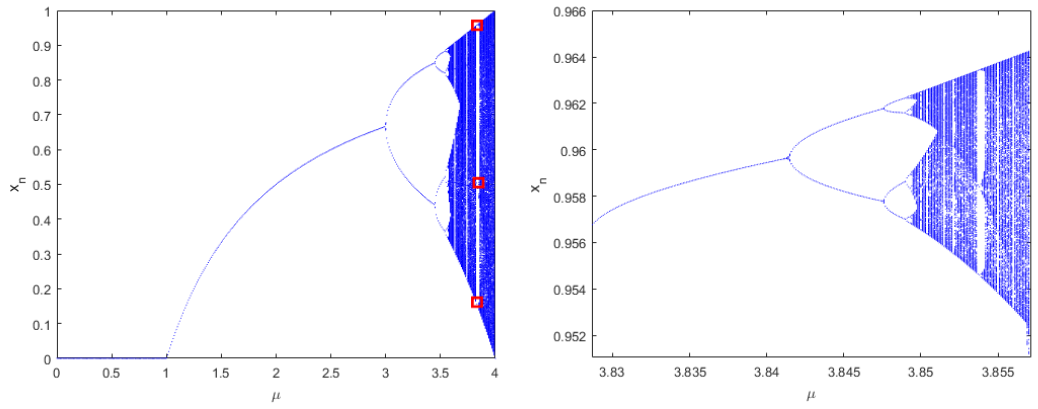
Section 1.5.1) in Figure 1.11 where μ is the parameter and x_n stands for the states when the number of iterations (n) is $n \to \infty$, and in the phase space of Hénon map (see Equation (1.20) in the following Section 1.5.5) in Figure 1.12 where its state is represented by (x, y).

Chaotic dynamics has the universally accepted characteristics including the detailed aforementioned ones : high sensitivity to initial conditions, positive Lyapunov exponent, strange attractor and complex dynamics, fractal and self-similarity. There also exist other criteria for chaotic system such as finite Kolmogorov-Sinai entropy, positive topological entropy, continuous power spectrum, etc. Here, we just have discussed the most distinct and important features of chaotic dynamics in this subsection.

1.5 Paradigms of chaotic maps

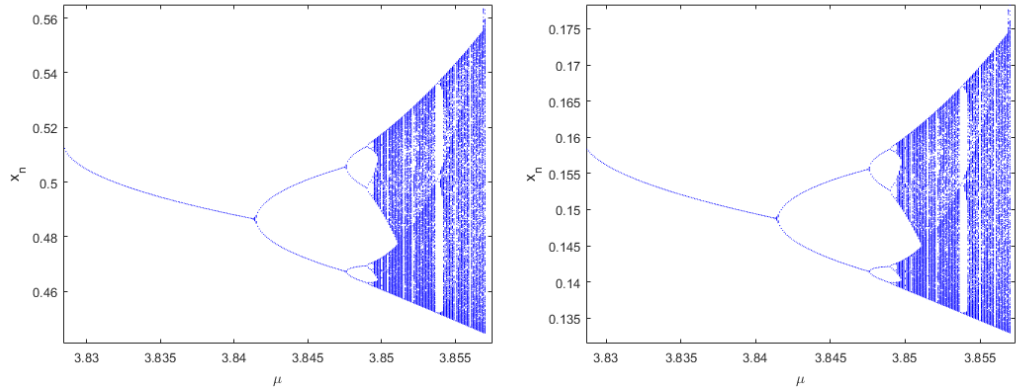
Chaotic dynamics is ubiquitous in nature and chaotic behavior can be found in many physical systems and mathematical maps.

There are the well-known continuous-time maps : Lorenz map, Chen system, Van de Pol system, Rössler system, Duffing system, etc. However, compared to discrete maps, they are not suitable to be applied in cryptography for the reasons that have been discussed in Section 1.3.2. For discrete chaotic maps, their rich dynamics and the advantage of ease of implementation act as the good qualities that make them suitable for cryptosystem implementation. Meanwhile, we should note that, they cannot be applied in cryptosystems



(a) Bifurcation diagram (period-three window marked in red boxes)

(b) Enlarged area of the top red box of (a)



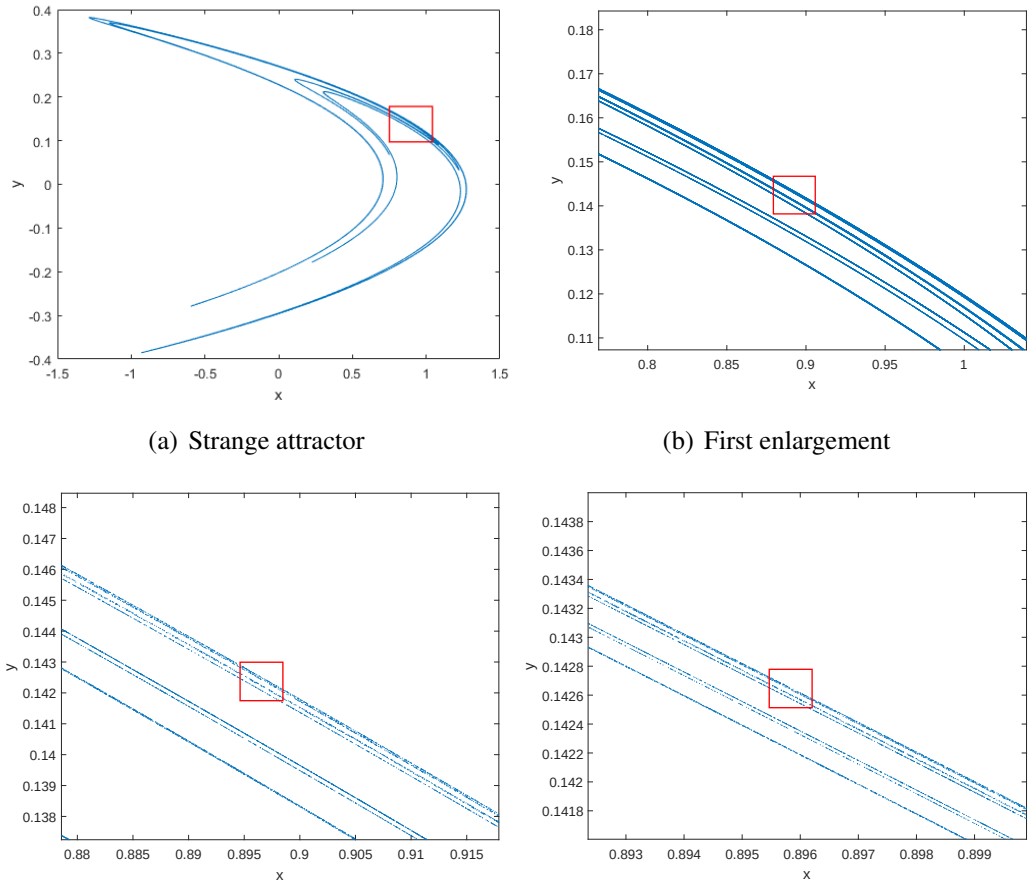
(c) Enlarged area of the middle red box of (a)

(d) Enlarged area of the bottom red box of (a)

FIGURE 1.11 – Fractal existed in the bifurcation diagram of logistic map (self-similarity)

alone. Because the discrete chaotic maps also have the disadvantages of short periodic orbits under finite precision digital implementations and easily recognized functions, which will lead to insecurity. But, the drawbacks can be overcome by proper operations based on multiple discrete chaotic maps, for instance, coupling different chaotic maps [42], mixing chaotic orbits [43], and using linear feedback shift register (LFSR) technique [44], et etc.

Thus, we focus on several typical discrete chaotic maps in this section. In the following chapters (Chapter 3, 4, 5, 6), based on the discrete chaotic maps, we will reformulate them and design efficient coupling scheme to develop PCNGs for chaos-based cryptosystems.



(a) Strange attractor

(b) First enlargement

(c) Second enlargement

(d) Third enlargement

FIGURE 1.12 – Fractal existed in the strange attractor of Hénon map (self-similarity)

1.5.1 Logistic map

Logistic map is one of the most studied chaotic maps among the simplest nonlinear maps and it appears frequently in the chaos-based cryptosystem designs. Logistic map is a simplified predator-pray model which is firstly studied by P.J. Myrberg [24] and then popularized by Robert May [23]. Its function is :

$$x_{n+1} = f(x_n) = \mu x_n \left(1 - x_n\right), x_n \in [0, 1] \tag{1.13}$$

where x_n is the state of n-th iteration, x_0 is the initial condition, and $\mu \in (0, 4]$ is the control parameter.

Bifurcation diagram shows the behavior of a dynamical system with respect to the parameters. Bifurcation diagram of logistic map has been shown in Figure 1.11. It corresponds

to the diagram of Lyapunov exponents by varying parameter μ (see Figure 1.13). When $\mu = 4$, the logistic map has the biggest Lyapunov exponent that is approximately equal to 0.6928, which implies it reaches the highest chaotic dynamics. Therefore, in the following, we choose $\mu = 4$ for the logistic map.

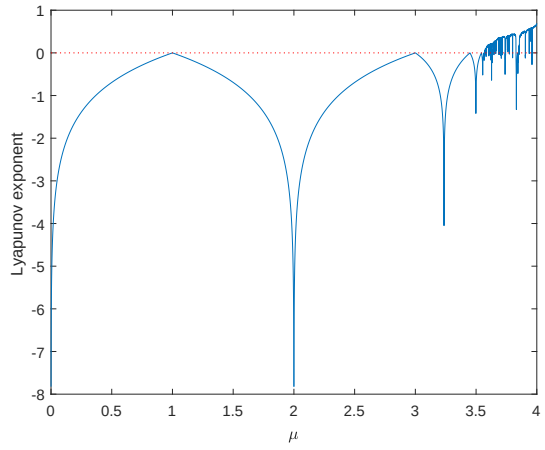


FIGURE 1.13 – Lyapunov exponents diagram

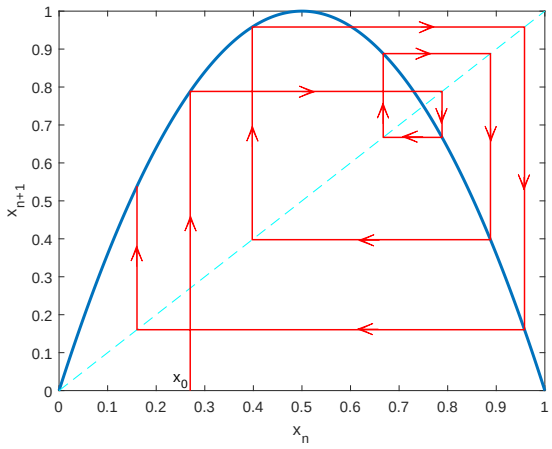


FIGURE 1.14 – Logistic map

The equation of the logistic map can be seen in the phase space ($\mu = 4$) shown in blue in Figure 1.14 where the red curve shows the iterated orbit.

Let $x_{n+1} = x_n$, i.e. $x = f(x) = \mu x(1 - x)$, the fixed point x_{fp} of the map can be found : $x_{fp} = 0$ and $x_{fp} = \frac{\mu-1}{\mu}$. According to Theorem 1.4, the stability can be examined by the derivative $f'(x) = \mu - 2\mu x$. Hence, when $\mu = 4$, logistic map has two unstable fixed points : $x_{fp} = 0$ and $x_{fp} = \frac{3}{4}$ (the intersections of the blue solid curve of logistic function and the cyan dashed line of the bisector $x_{n+1} = x_n$ shown in Figure 1.14).

If the logistic map is iterated 400 times, the trajectory can be illustrated by Figure 1.15, from which we can observe that the trajectory appeared in the area near to the value 0 and 1 seems denser than that appeared in the middle area ($x_n \in [0.2, 0.8]$). More visually, according to Figure 1.16 which plots 4000 successive produced numbers (x_n) marked with "$*$", it obviously demonstrates that the density of marks is higher in the band where x_n near to value 0 and 1 than in the middle range ($x_n \in [0.2, 0.8]$).

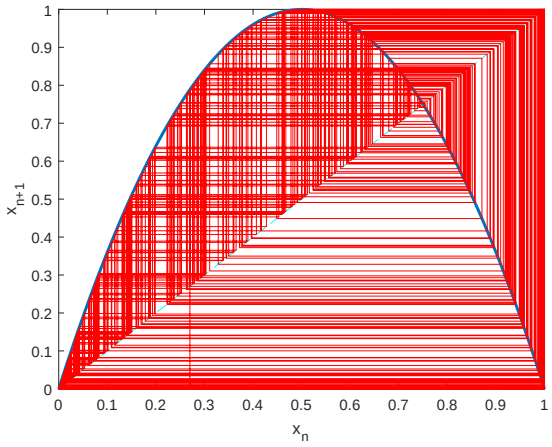


FIGURE 1.15 – A trajectory of the logistic map

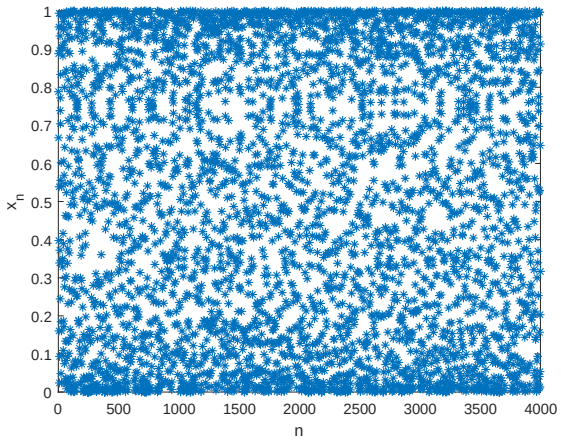


FIGURE 1.16 – Numbers produced by the logistic map

The distribution of the sequence produced by the logistic map has been investigated mathematically by Ulam et von Neumann [45] and A.Lasota et M.C.Mackey [46]. According to their works, the probability density of the produced numbers of logistic map is

$$\rho(x) = \frac{1}{\pi\sqrt{x(1-x)}} \tag{1.14}$$

If we plot $\rho(x)$ as a function of x in Figure 1.17, we can observe clearly that the produced numbers have a bigger probability to locate near to 0 and 1 than in the middle region.

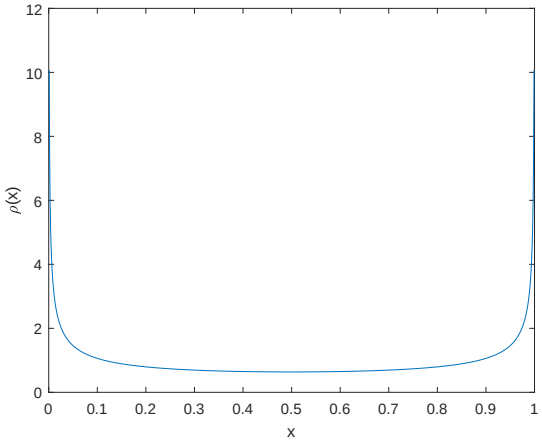


FIGURE 1.17 – Probability density function

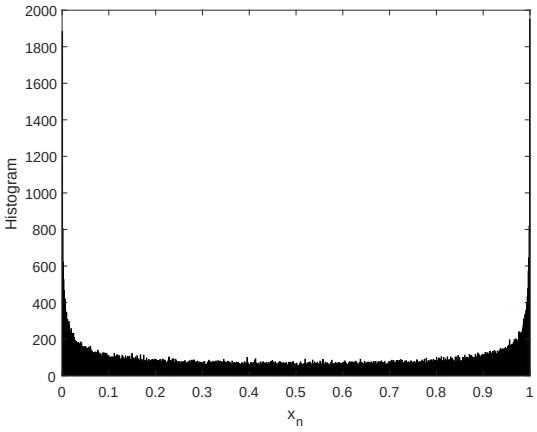


FIGURE 1.18 – Histogram

The histogram of the iterated sequence with the length of 10^5 produced by the logistic

map in 1000 classes is shown in Figure 1.18. It can be seen that that the distribution of the produced sequence is highly consistent the density diagram (Figure 1.17), and it is not uniformly distributed in the definition region $[0, 1]$.

In summary, the logistic map has the largest positive Lyapunov exponent when $\mu = 4$, which implies chaotic behavior and indicates it can be used in chaos-based cryptosystem design. However, the density analysis and the histogram have shown that the produced sequence does not exhibit uniform distribution, which implies that the logistic map can not be regarded as a pseudo-random source for encryption purposes. Therefore, as we explained in the beginning of this section, the logistic map cannot be used alone in a cryptosystem design unless there are additional components and proper operations to palliate the above drawbacks existing in the logistic map.

1.5.2 Skew tent map

Skew tent map is derived from the classical tent map but it achieves better statistical performances. Skew tent map defined in real domain $(0, 1)$ is given by Equation (1.15).

$$x_{n+1} = f_s(x_{n-1}, p) = \begin{cases} \frac{x_n}{p}, & 0 \leqslant x_n < p \\ \frac{1-x_n}{1-p}, & p \leqslant x_n \leqslant 1 \end{cases} \tag{1.15}$$

where $\{x_n, n = 1, 2, 3, ...\}$ represents the state and $p \in (0, 1)$ is the control parameter.

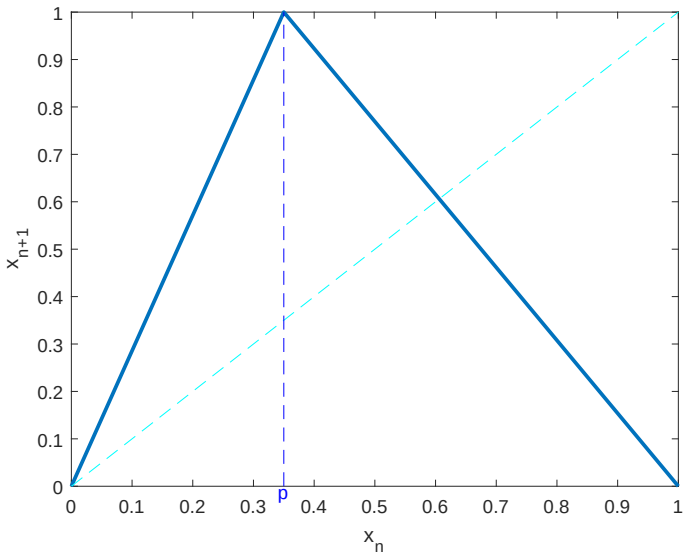


FIGURE 1.19 – Skew tent map

The skew tent map for a given parameter value p is displayed in Figure 1.19, where there exist two unstable fixed points : $x_{fp} = 0$ and $x_{fp} = \frac{1}{2-p}$.

The bifurcation diagram is plotted in Figure 1.20, from which we can find that although there exists a small blank area, the skew tent map shows excellent chaoticity in its definition region. Note that, the blank area is corresponding to the unstable point $x_{fp} = \frac{1}{2-p}$. Since $p \in (0, 1)$, $x_{fp} = \frac{1}{2-p} \in (\frac{1}{2}, 1)$. Thus, the area appears in the region $(0.5, 1)$ [29]. The good chaoticity also can be verified by its Lyapunov exponent diagram shown in Figure 1.21 : the Lyapunov exponents by varying parameters (p) are always positive and the maximum value 0.6973 is achieved when $p = 0.5$. At this parameter, the chaoticity of the skew tent map is equivalent to that of the logistic map.

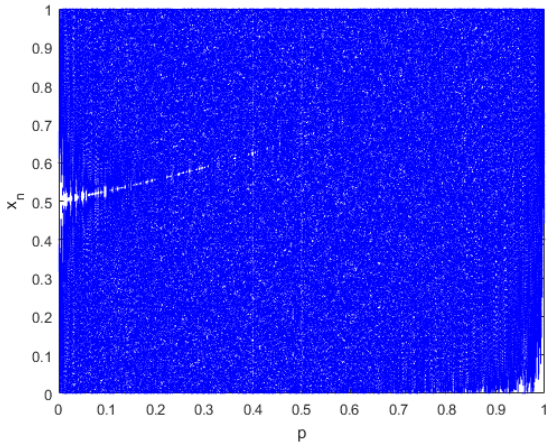


FIGURE 1.20 – Bifurcation diagram of skew tent map

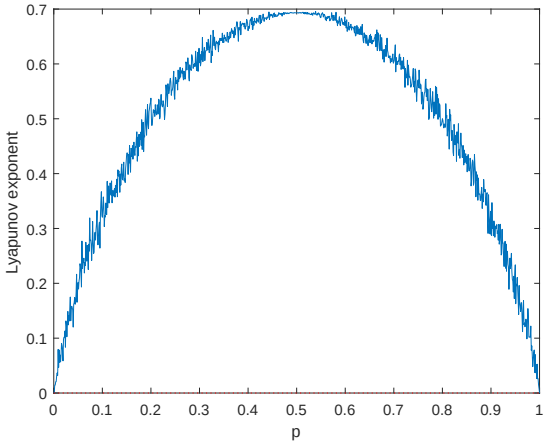


FIGURE 1.21 – Lyapunov exponents by parameter p

It has been verified that the produced sequences of the skew tent map obeys the uniform invariant distribution and the probability distribution function is $\rho(x) = 1$ [47, 48]. Figure 1.22 shows a trajectory $(400$ iterations) of the skew tent map indicating that the trajectory seems distributed evenly in the phase space. In addition, the histogram of a produced sequence with the length of 10^5 has been plotted in Figure 1.23, which shows more visually that the skew tent map has much better statistical uniformity than the logistic map.

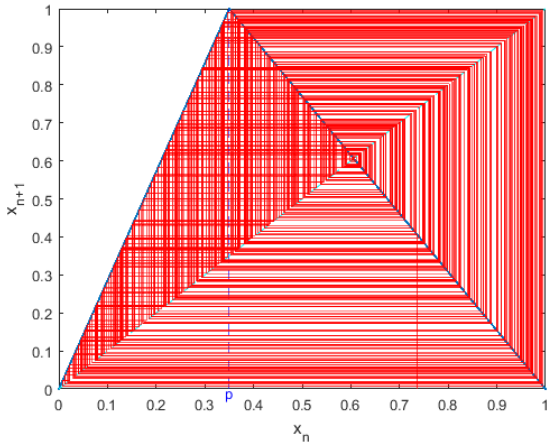


FIGURE 1.22 – A trajectory of the skew tent map

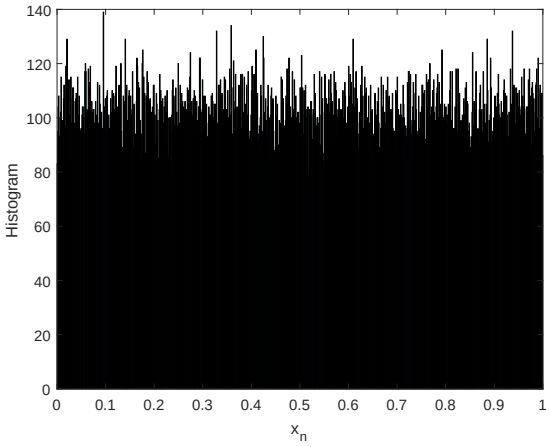


FIGURE 1.23 – Histogram of a sequence produced by skew tent map

1.5.3 Piece-wise linear chaotic map (PWLCM)

Piece-wise linear chaotic map (PWLCM) refers to a family of maps and skew tent map is also a piece-wise linear chaotic map. But, in this thesis, "PWLCM" specifies the following map with 4 slopes :

$$x_{n+1} = f_p\left(x_{n-1}, p_p\right) = \begin{cases} \frac{x_n}{p_p}, & 0 \leqslant x_n < p_p \\ \frac{x_n - p_p}{0.5 - p_p}, & p_p \leqslant x_n < 0.5 \\ \frac{1 - p_p - x_n}{0.5 - p_p}, & 0.5 \leqslant x_n < 1 - p_p \\ \frac{1 - x_n}{p_p}, & 1 - p_p \leqslant x_n \leqslant 1 \end{cases} \tag{1.16}$$

where $\{x_n, n = 1, 2, 3, ...\}$ represents the iteration state and $p_p \in (0, 0.5)$ is the control parameter.

PWLCM for a given parameter p_p is displayed in Figure 1.24, where there are four unstable fixed points : $x_{fp} = 0, \frac{p_p}{0.5+p}, \frac{1-p_p}{1.5-p_p}, \frac{1}{1+p_p}$.

Bifurcation diagram and Lyapunov exponent diagram have been plotted in Figure 1.25 and Figure 1.26, which have demonstrated the good chaotic property of PWLCM. The minimum Lyapunov exponent is equivalent to that of the logistic map when $\mu = 4$ and skew tent map when $p \approx 0.5$, while the maximum Lyapunov exponent value is 1.386 that is obtained when $p_p \approx 0.25$. Thus, PWLCM has stronger chaoticity than logistic map and skew tent map.

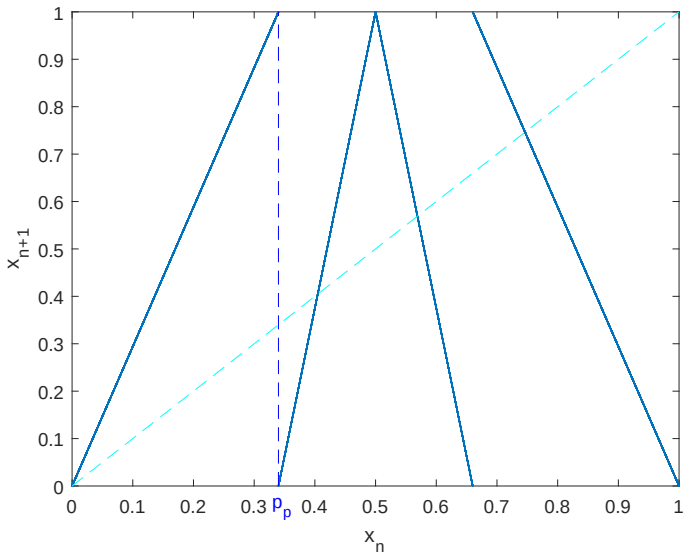


FIGURE 1.24 – PWLCM

A trajectory of PWLCM is shown in Figure 1.27. The histogram shown in Figure 1.28 (10^5 number of x_n in 1000 classes) indicates that the produced sequences of PWLCM have an approximate uniform distribution which also can be seen in the histogram of skew tent map (see Figure 1.23). In the work of [30], the authors have derived and determined the invariant density of a type of piece-wise linear maps with 3 slopes, which also can indicate the good uniformity property of piece-wise linear chaotic maps than the chaotic maps with nonlinear derivatives, e.g. logistic map, to some extent.

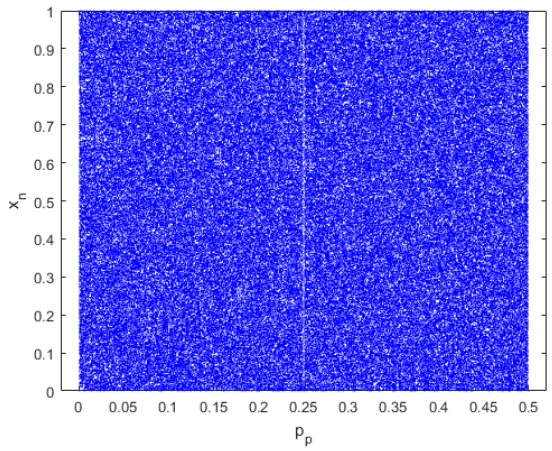


FIGURE 1.25 – Bifurcation diagram of PWLCM

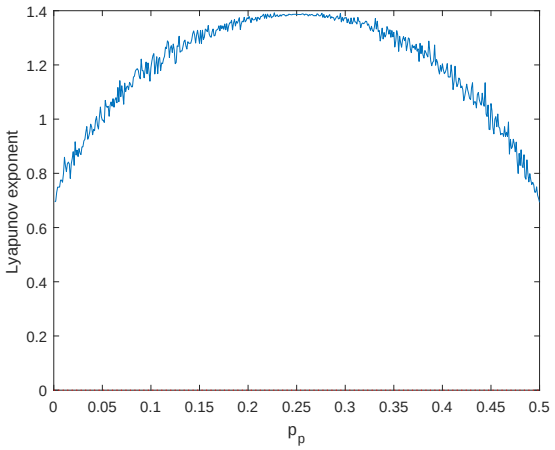


FIGURE 1.26 – Lyapunov exponents of PWLCM

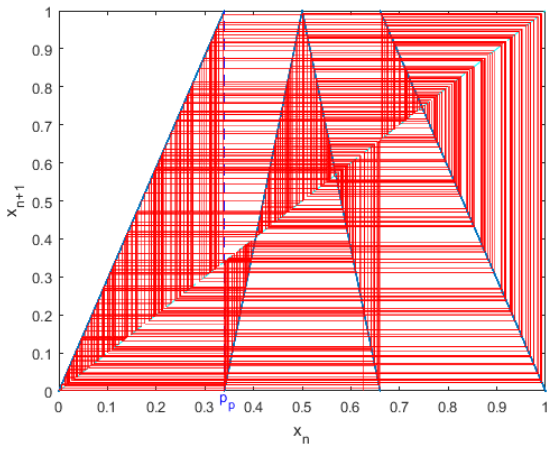


FIGURE 1.27 – A trajectory of PWLCM

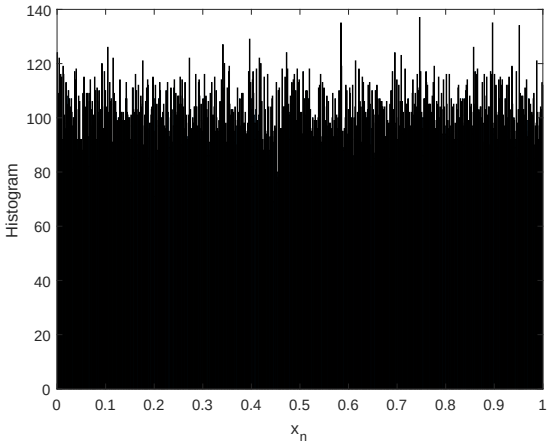


FIGURE 1.28 – Histogram of a sequence produced by PWLCM

1.5.4 Chebyshev chaotic map

Chebyshev map is also a 1D typical chaotic map. It is defined over the real domain $[-1, 1]$:

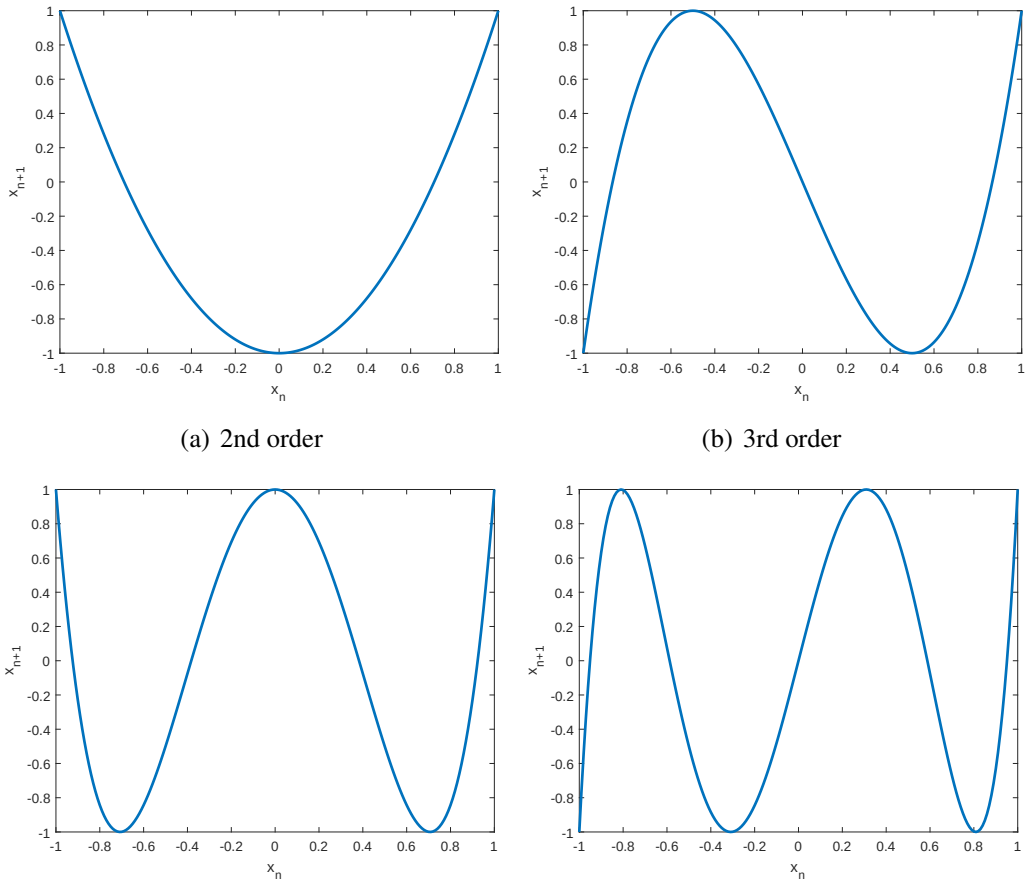
$$x_{n+1} = \cos\left[\gamma \operatorname{arc}\cos\left(x_n\right)\right], x_n \in [-1, 1] \tag{1.17}$$

where the initial condition x_0 and the state x_n vary in $[-1, 1]$; γ is the parameter that determines the order of the map. Depending on different γ, Chebyshev map in first to fourth orders, noted by $T_\gamma, \gamma = 1, 2, 3, 4, 5$, are presented as follows :

$$\begin{aligned}
x_{n+1} &= T_1\left(x_n\right) = x_n \\
x_{n+1} &= T_2\left(x_n\right) = 2x_n^2 - 1 \\
x_{n+1} &= T_3\left(x_n\right) = 4x_n^3 - 3x \\
x_{n+1} &= T_4\left(x_n\right) = 8x_n^4 - 8x_n^2 + 1 \\
x_{n+1} &= T_5\left(x_n\right) = 16x_n^5 - 20x_n^3 + 5x_n
\end{aligned} \tag{1.18}$$

Chebyshev maps from 2nd order to 5th order can be seen in Figure 1.29.

Bifurcation of the above Chebyshev maps is shown in Figure 1.30, which indicates the chaotic dynamics may occur when the order of the map $\gamma \geqslant 2$. This can be verified by the Lyapunov exponent diagram shown in Figure 1.31. The chaoticity increases as the parameter γ increases.



(a) 2nd order (b) 3rd order

(c) 4th order (d) 5th order

FIGURE 1.29 – Chebyshev maps

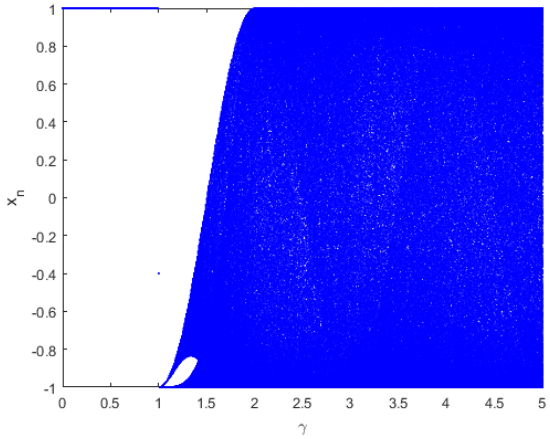


FIGURE 1.30 – Bifurcation diagram of chebyshev map

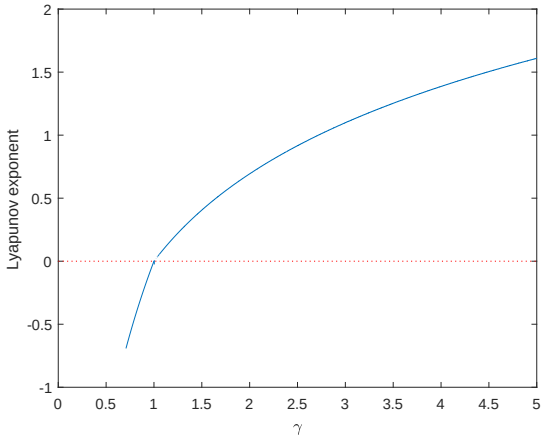


FIGURE 1.31 – Lyapunov exponents by parameter γ

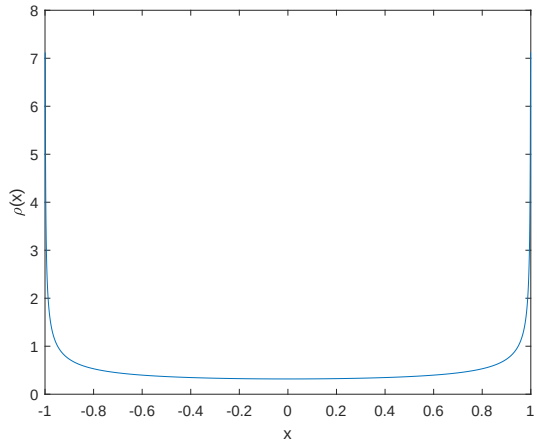


FIGURE 1.32 – Density diagram

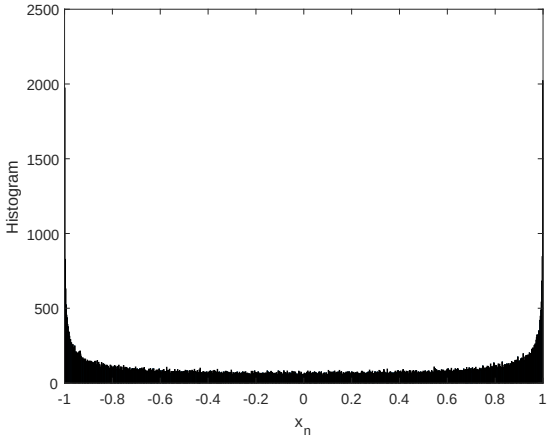


FIGURE 1.33 – Histogram of 3rd order Chebyshev chaotic map

The probability density function of Chebyshev chaotic maps is [49] :

$$\rho(x) = \frac{1}{\pi\sqrt{1-x^2}},\ x \in [-1,1] \tag{1.19}$$

It is obvious that Chebyshev chaotic maps do not obey the uniform distribution. Figure 1.32 displays the probability density function. Besides, this conclusion also can be drawn from the histogram of 3rd order Chebyshev map shown in Figure 1.33.

Considering the 3rd order Chebyshev map possesses relatively higher Lyapunov exponent compared with 2nd order map and lower computational consumption compared with 4th order map and 5th order map. We choose the 3rd order Chebyshev map in our works.

1.5.5 Hénon map

The Hénon map is a 2D discrete-time chaotic map [50] which exhibits a horseshoe structure. It is defined by :

$$\begin{cases} x_{n+1} = -ax_n^2 + y_n + 1 \\ y_{n+1} = bx_n \end{cases} \tag{1.20}$$

where a and b are the real parameters. When $a = 1.4$ and $b = 0.3$, the Hénon map displays a strange attractor in the phase space that has been shown in Figure 1.12(a).

If $b = 0.3$ is fixed and a varies in the range of $[0, 1.5]$, the bifurcation diagram has been

shown in Figure 1.34. The estimated Lyapunov exponents have been plotted in Figure 1.35 which corresponds to its behaviour (chaotic or periodic) with respect to the parameter a, and is coherent with the bifurcation diagram shown in Figure 1.34.

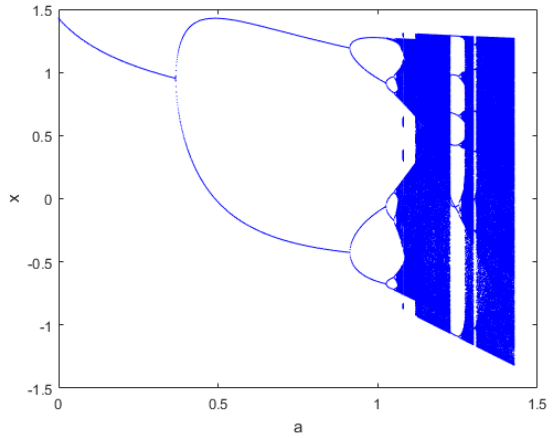


FIGURE 1.34 – Bifurcation diagram of Hénon map

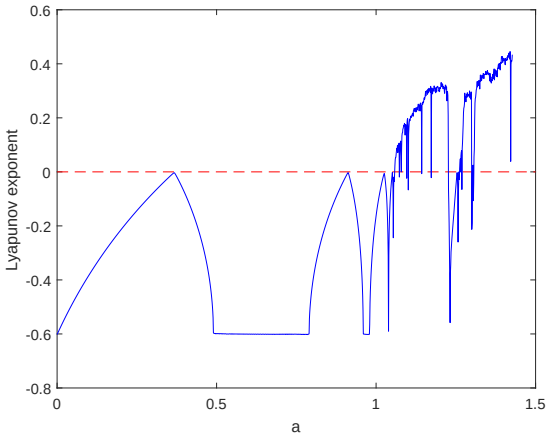


FIGURE 1.35 – Lyapunov exponents of Hénon map

1.5.6 Lozi map

Based on Hénon map, a French mathematician René Lozi proposed an piece-wise linear version chaotic map : Lozi map [51] :

$$\begin{cases} x_{n+1} = -a\,|x_n| + y_n + 1 \\ y_{n+1} = bx_n \end{cases} \tag{1.21}$$

where a and b are real parameters.

Lozi map is a simplified version of Hénon map, but it has good chaotic performance. The strange attractor when $a = 1.7$, $b = 0.5$ is shown in Figure 1.36

1.5.7 Arnold's cat map

Arnold's cat map, one of the famous 2D chaotic maps, is a mixing discrete map which performs an area preserving stretch and fold mapping named after V.Arnold who demonstrated its mixing effects using an image of a cat [52]. It is often used in the chaos-based cryptosystem for image permutation purposes.

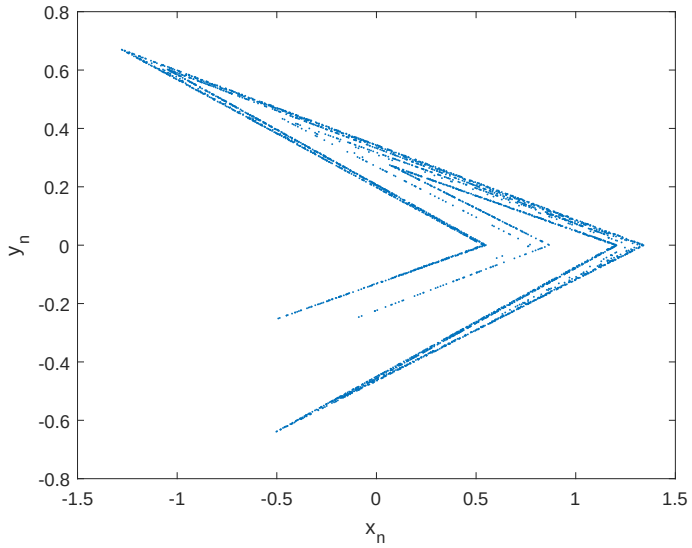


FIGURE 1.36 – Attractor of Lozi map

The original form of this map is :

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod\ 1) \tag{1.22}$$

where $x_n, y_n \in [0, 1]$; (x_n, y_n) is the original position that is mapped into a new position (x_{n+1}, y_{n+1}).

The Lyapunov exponents (λ) can be obtained by calculating the eigenvalues (σ) of the cat matrix [53] :

$$\begin{vmatrix} 1-\sigma & 1 \\ 1 & 2-\sigma \end{vmatrix} = \sigma^2 - 3\sigma + 1 = 0,$$

so

$$\sigma_{\pm} = \frac{3 \pm \sqrt{5}}{2}.$$

Hence, two Lyapunov exponents (λ_1, λ_2) are

$$\lambda_1 = ln\,(\sigma_+) = ln\left(\frac{3+\sqrt{5}}{2}\right) > 0$$

$$\lambda_2 = ln\,(\sigma_-) = ln\left(\frac{3-\sqrt{5}}{2}\right) < 0$$

where the positive λ_1 has implied the cat map is chaotic.

The determinant of the cat matrix $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ is 1, which indicates that it is a area-preserving transformation.

The effect of Arnold's cat map on a unit square has been shown in Figure 1.37, from which we can find that there are two operations that cause chaotic behavior, i.e. stretching ((x_n, y_n) multiplied by the cat matrix makes (x_{n+1}, y_{n+1}) larger) and folding (modulus operation $(mod\ 1)$ makes (x_{n+1}, y_{n+1}) back to the unit square).

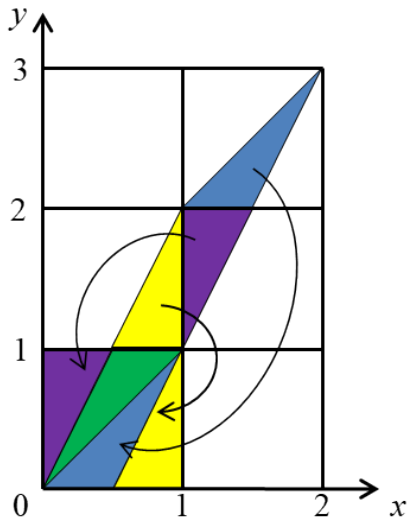


FIGURE 1.37 – Effect of Arnold's cat map

Arnold's cat map can be discretized and extended to the 2D integer domain [54] :

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & u \\ v & 1+u\times v \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod\ M) \tag{1.23}$$

where $x_n, y_n, x_{n+1}, y_{n+1}, u, v \in \{0, 1, ..., M-1\}$ and $M \in \mathbb{Z}^+$.

This form has attracted lots of attention since it can be used directly in an image encryption algorithm to accomplish permutation in an image of size $M \times M$. However, the quantization of Arnold's cat map causes that the 2D cat map (1.23) has a finite period, which may be a weakness in cryptography [54, 55]. In addition, for the equation (1.23), when $(x_n, y_n) = (1, 1)$, the used parameters u and v can be easily retrieved by tracing the position $(x_{n+1}, y_{n+1}) = (1+u, v+1+u\times v)$, and that is a weakness for the encryption algorithm Also, it has a fixed point problem, which means the element (pixel from the plain

image to be encrypted) at the first position ($(0, 0)$ in (1.23)) keep unchanged regardless the number of iterations, i.e. if $(x_n, y_n) = (0, 0)$, $(x_{n+1}, y_{n+1}) = (0, 0)$ and the following iterations will be fixed at $(0, 0)$. Thus, adopting the 2D cat map in cryptography for permutation needs to overcome the above problems to ensure security.

1.6 Conclusion

Chaotic behavior is ubiquitous in nature. It was firstly discovered in the late 19th and early 20th centuries, and then deemed to be the third major discovery of physics in the 20th century. Nowadays, chaotic dynamics plays an important role in many fields, from mathematics and physics to engineering and cryptography.

Chaos is a special phenomenon in dynamical systems. In this chapter, firstly, we summarized the influential discoveries in the history of chaos which made the chaos theory come to light gradually. Secondly, we introduced the fundamentals of nonlinear dynamical systems that is relevant to chaotic dynamics. Then, concentrating on chaotic systems, three definitions have been discussed : Yi-Yorke definition describes chaotic behavior from orbits aspect ; Devaney definition is a relatively widely acknowledged definition that points out that the high sensitivity, transitivity and dense periodic points constitute the kernel of the chaotic dynamics ; Smale definition gives a geometrical description of chaotic dynamics that explains the chaotic motion and the above two definitions. In addition to the definitions, chaotic features were discussed. Chaotic dynamics has it own specific features. The most typical ones have been discussed in this chapter, such as high sensitivity to initial conditions and parameters, positive Lyapunov exponent, strange attractor, fractal and self-similarity.

Chaotic maps can be classified to continuous-time maps and discrete-time maps on one hand. In practical applications, digital devices will not support the infinite precision continuous nature. Since the discrete-time chaotic maps achieve chaotic dynamics though iterative chaotic maps, they do not need discretization and do not have the heavy computational burden when compared to the continuous-time systems. Discrete-time chaotic maps are more suitable to be directly applied in cryptosystems.

On the other hand, there are high-dimensional and low-dimensional discrete-time chaotic maps. We adopt the low-dimensional ones in our work due to their rich chaotic properties and ease of implementation. In the last section, we presented several low-dimensional chaotic maps which are also commonly used in the design of chaos-based cryptosystems.

CHAPITRE 2

CHAOS-BASED CRYPTOGRAPHY

2.1 Introduction

In the previous chapter, we have introduced the basis of chaotic dynamics theory and several low-dimensional chaotic maps that are widely used in the chaos-based cryptosystems. In this chapter, we first give the introduction to the chaos-based cryptosystem in Section 2.2 which includes cryptography, cryptosystem, chaos-based cryptosystem and the common cryptographic attacks. Then the state of the art of the chaos-based cryptosystems will be discussed in detail in Section 2.3. The literature analysis focuses on the confusion-diffusion structured chaos-based encryption schemes and PCNG designs. After that, we will elaborate the existing problems and solutions. Finally, Section 2.4 concludes this chapter.

2.2 Introduction to chaos-based cryptosystem

2.2.1 Cryptography

Cryptography is a technique for ensuring the information security. It hides the confidential information into an unreadable form by encryption in order to protect the information from being intercepted by potential enemies, hackers or the public so that only authorized receivers or users can recover the information correctly by decryption.

The encryption and decryption can be described by Figure 2.1. The plaintext is the confidential message. Encryption is a certain algorithm that uses the secret key to camouflage the plaintext to hide the true message, and then outputs the ciphertext. In the process of decryption, only the correct secret key can decrypt the ciphertext to recover the plaintext.

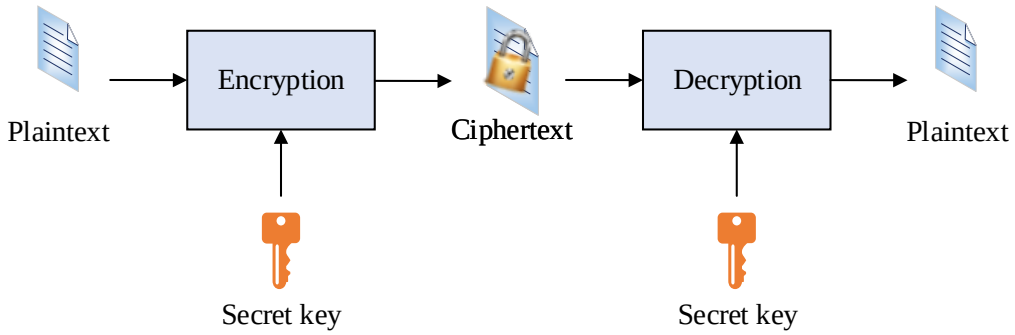


FIGURE 2.1 – Encryption and decryption

2.2.2 Cryptosystem

The secret key for encryption and decryption can be the same or different. This depends on the type of cryptosystems. Typically, cryptosystems can be classified into two types : symmetric-key (private-key) algorithm and asymmetric-key (public-key) algorithm.

Symmetric-key algorithms use the same secret key for encryption and decryption, and the secret key needs to be securely protected. While different keys serve the asymmetric-key algorithm : usually, one key is publicly known and there are two different private keys serving encryption and decryption. Asymmetric-key cryptosystems are slow, and thus they are usually used to deal with small amount of data, such as secret key agreement, digital signature, and authentication, etc. The most widely used asymmetric-key cryptosystem is RSA (Rivest–Shamir–Adleman encryption algorithm). By contrast, symmetric-key cryptosystems are fast and efficient, and they are more suitable for tackling large amounts of data at a high speed [4]. In this thesis, we focus on the symmetric-key cryptosystem.

The symmetric-key cryptosystem contains the cryptographic components, such as plaintext, ciphertext, key space, and their relationships, which can be described formally by the following mathematical notation and figure 2.2 [56] .

A cryptosystem is a five-tuple (P, C, K, E, D) and it satisfies the following conditions :

1. P is a finite set of possible plaintexts ;

2. C is a finite set of possible ciphertexts ;

3. K, the key space, is a finite set of possible keys ;

4. E and D represent the sets of all possible encryption and decryption rules respectively and both are related to K and P ;

5. For each key $k \in K$, there is an encryption rule $e(k, p) \in E$ and a corresponding

decryption rule $d(k, c) \in D$, such that $d(k, e(k, p)) = p \in P$.

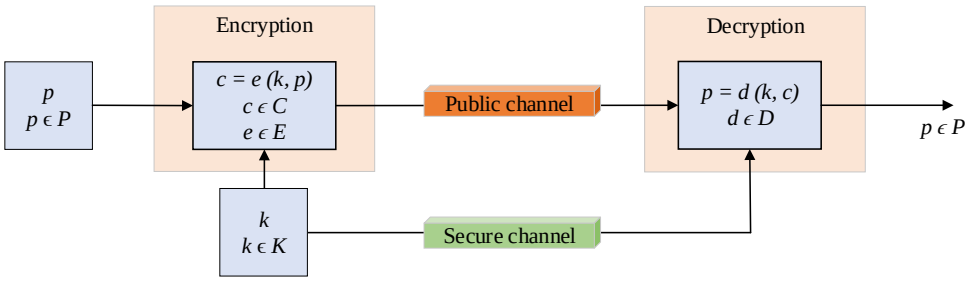


FIGURE 2.2 – Cryptographic elements in a symmetric-key cryptosystem

2.2.3 Chaos-based cryptosystem

According to the existing literature, most of the chaos-based cryptosystems are symmetric-key cryptosystems. For simplicity, the term of chaos-based cryptosystem used in the following means the symmetric-key chaos-based cryptosystem, unless otherwise specified.

Chaos-based cryptosystems adopt the chaotic elements in the process of key generation, and encryption and decryption algorithms, which can be described in Figure 2.3.

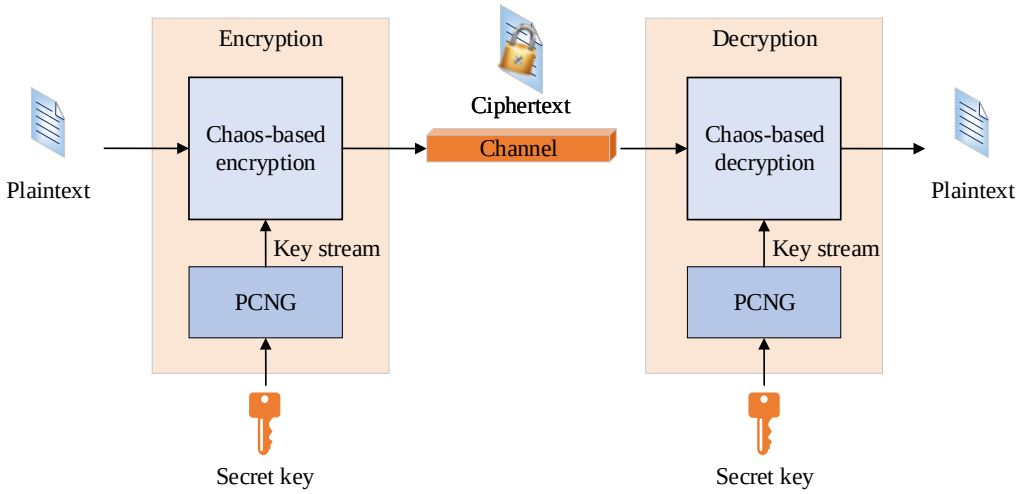


FIGURE 2.3 – Scheme of the chaos-based cryptosystem

In a chaos-based cryptosystem, plaintext (original message) is encrypted into the unreadable ciphertext by the chaos-based encryption algorithm with a secret key. In this process,

the PCNG, controlled by the secret key, provides the key stream for the encryption algorithm. At the authorized receiver (user), the plaintext can be recovered by decrypting the ciphertext with the identical secret key.

In the process of encryption and decryption, chaotic components play an important role not only in producing cryptographic key stream for encryption and decryption algorithms, but also in achieving a good confusion and diffusion quality in encryption algorithm. For this, the PCNG should be able to produce pseudo-random numbers as the key stream that exhibits good randomness and has high sensitivity to the secret key (also called "seed" for a PRNG). Also, the confusion and diffusion operations should be sufficient and complex enough to ensure the high security of a cryptosystem.

According to the different encryption concepts, the chaos-based cryptosystems can be further classified into stream ciphers and block ciphers.

Stream ciphers encrypt the plaintext by applying the XOR (exclusive OR) operation between the plaintext and the key stream continuously. This is an one-time pad process, which means the key stream produced by a certain secret key only can be used once for encryption algorithm. In the process of decryption, the plaintext can be recovered using XOR operation between the cipertext and the identical key stream. The security of a stream cipher depends strongly on the performances of the PCNG. A reliable PCNG should have a large key space, high sensitivity to the secret key and pseudo-random properties. Security and high speed performance are the main requirements of a good stream cipher.

Block ciphers encrypt the plaintext block by block. They obey the Shannon's theory of information security that requires a high level of confusion and diffusion properties for a secure cryptosystem. The block cipher based on confusion and diffusion scheme can be described by Figure 2.4. In the encryption process, the secret key is used to control the PCNG to generate the key stream (K_c, K_d) for confusion and diffusion operations. The confusion and diffusion can be repeated r_c and r_d times respectively and the whole confusion-diffusion operation also can be repeated r times to meet the security requirements.

Confusion means using of transformations to complicate dependence of the statistics of the ciphertext on the statistics of the plaintext. **Diffusion** aims to spread the influence of a single element of the plaintext over as many elements of the ciphertext as possible [57].

Considering the input plaintext is an image, the confusion means the relation between the secret key, the plain image and the cipher image is complex and concealed. In general, the confusion layer contains permutation operations which are used to relocate the pixel

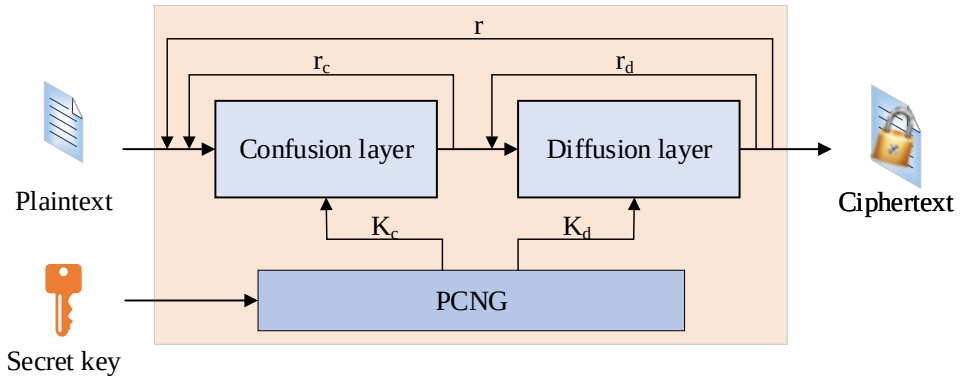


FIGURE 2.4 – Scheme of the confusion-diffusion in chaos-based cryptosystem

positions and substitution operations which change the pixel values. The diffusion layer focuses on how to spread the influence of each bit of the plain image to the ciphered one in order to change the statistical properties of the plain image and ensure that the ciphered images encrypted from the similar plain images are totally different even if their plain images are just a tiny (one bit) different [7, 58, 59].

Both stream ciphers and block ciphers require a good quality key stream, which emphasizes the important role that PCNG plays in the security of a cryptosystem. The PCNG, also called chaotic generator or chaotic PRNG, is designed based on several nonlinear chaotic maps and can generate pseudo-random numbers with enhanced chaoticity and good randomness.

2.2.4 Cryptographic attacks

Cryptanalysis and cryptography constitute cryptology.

When performing cryptanalysis on a cryptosystem, there is a general assumption that the cryptanalyst knows exactly the encryption algorithm and how it works. In other words, the cryptanalyst knows everything about the cryptosystem except the secret key. This assumption is reasonable, since encryption algorithms have to be sold to multiple users in the market and thus the encryption algorithm is easy to be known by public. Consequently, reverse engineering is always possible to reveal all details on how a cipher works [4].

According to [56], there are four known attacks on cryptosystems that are listed as follows.

1. Ciphertext-only attack : the attacker only has some cipheretexts.

2. Known-plaintext attack : the attacker only has some pairs of plaintexts and the cor-

responding ciphertexts.

3. Chosen-plaintext attack : the attacker has temporary access to the encryption process and he can encrypt some specific plaintexts to obtain their corresponding ciphertexts.

4. Chosen-ciphertext attack : the attacker has temporary access to the decryption process and he can use some specific ciphertexts in decryption to obtain their corresponding plaintexts.

For the attacker, the last two attacks are easier than the others and are possible. Thus, if a cryptosystem can resist the chosen-plaintext/ciphertext attack, they can resist all above attacks and the cryptosystem can be considered to be secure.

Apart from the above four types of attacks, there are common attacks as well : brute-force attack, statistical attack, and differential attack.

Brute-force attack works by trying every possible secret key with the hope of eventually finding the correct one. As the key space increases, the amount of computational time for the attacker to obtain the secret key increases drastically. Thus, a large key space is demanded to make the brute-force attack impractical.

Statistical attack aims to extract the relationships between the plain image and the ciphered image by exploiting the statistical weaknesses in a cryptosystem. According to Shannon's theory of information and communication, it is possible to break many types of cryptosystems by statistical attack [60]. Statistical attack can be thwarted if the ciphered image shows a uniform distribution and no statistical correlation between ciphered image, plain image and the secret key. Thus, the redundancy in plain image should be dissipated by diffusion, and meanwhile, the complexity relationship between ciphered image, plain image and secret key should be increased by confusion operation.

Differential attack studies how differences in the plaintext can affect the resultant difference at the ciphertext. It abuses pairs of plaintext and corresponding ciphertext to seek for the secret key using reduced amount of time. In other words, adversary can make a small change in the plaintext and then trace this difference to observe whether the ciphertext exhibits non-random behavior or other properties or relations between plaintext that can be exploited to recover the secret key. Differential cryptanalysis is a general form of cryptanalysis and it is primarily applicable to block ciphers, but also to stream ciphers and cryptographic hash functions. To defeat the differential attack, the ciphertext should have a high sensitivity to even a tiny change in the plaintext.

For all these attacks, the objective is to obtain the secret key, which is a vital component for a secure cryptosystem. The importance of the secret key also can be found in the Kerck-

hoff's principle that goes as "A cryptographic system should be secure even if everything about the system, except the key, is public knowledge", which means that the security of cryptosystem totally depends on the secret key. That indicates, even the attackers get access to the whole communication system except the secret key and they try to explore the relation between system and plaintext or secret key, they are highly unlikely to succeed even though they experiment with lots of plaintext or other ways. For this purposes, good confusion and diffusion properties must be satisfied.

2.3 State of the art

Most existing conventional encryption methods, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Rivest–Shamir–Adleman algorithm (RSA) cannot provide expected high speed in encryption applications owing to their heavy burden of computational complexity. Also, the insufficient diffusion level of the above methods is not suitable to encrypt the digital image and video that have a big data size and a strong correlation between pixels [61, 62]. Therefore, it is necessary to find new secure image encryption methods to improve the security of modern cryptosystems.

The perfect nature of chaotic dynamics, such as random-like behavior, high sensitivity to initial conditions and aperiodicity make it an excellent candidate for cryptography. In 1989, Robert and Matthews investigated the logistic map in cryptography for the first time [63]. Since then, applying chaotic dynamics for image encryption purposes has attracted the attention of many researchers. Over the last decades, many chaos-based cryptosystems have been proposed in the literature.

Confusion-diffusion strategy and PCNG design are two crucial and indivisible components in chaos-based image cryptosystems. To make things more clearly, section 2.3.1 will discuss the chaos-based cryptosystems but puts the emphasis on the confusion-diffusion schemes ; since PCNGs have a tight relationship with stream ciphers, section 2.3.2 will talk about the research status of PCNGs. In the research field of chaos-based image encryption algorithm, some existing problems and solutions will be discussed in section 2.3.3.

2.3.1 Chaos-based image cryptosystem

In 1998, Fridrich adopted a 2D chaotic map to construct a permutation-diffusion cipher structure that conforms to the confusion-diffusion concept. Fridrich's structure could eliminate the visual redundancy among pixels and proved that chaotic dynamics was applicable for image encryption purposes [64]. Since then, the confusion-diffusion concept based on chaotic systems has been considered as an efficient method with research potential in image cryptosystems [58, 59].

As discussed in Section 2.2.3, the confusion operation contains permutation and substitution operations ; the diffusion operation focuses on spreading the influence of each bit in the plain image to the cipher image. Based on this concept, various approaches have been proposed in the recent years.

Generally, the permutation can be achieved commonly by the following three methods.

The first type of permutation is based on sorting [65, 66]. That means the encryption algorithms permute the image pixels according to the order of sorting a chaotic sequence whose length is contingent upon the size of the plaintext. However, if the plaintext is very large, this kind of permutation will have a disadvantage of heavy computational burden.

The second method exists in the bit-level confusion. This kind of cryptosystems works in bit-level instead of pixel-level. That means, the pixels of original input plain image are converted from integers to bits, and then the permutation can be accomplished by shifting bits positions. Another advantage of this kind of permutation is that the bit-level permutation can change the pixel value so that it can achieve a diffusion effect at the same time [44, 67–69]. But, if an image is in a size of $R \times C$ (R : rows and C : columns) and each pixel is in 8-bit, bit-level permutation requires 8 times of $R \times C$ operations to shift the bit positions, which requires a considerable computation power especially when the plain image is very large.

The third type of method permutes the image based on the 2D discrete chaotic maps, such as Arnold's cat map [70], Standard map [71] and Baker map [72]. However, they have low secret key space and one can recover the image after a certain number of map iterations [73]. Also, they have the fixed point problem : for Arnold's cat map and Standard map, the pixel at the position $(1, 1)$ is fixed ; for Baker map, the pixels at the position $(1, 1)$ and (N, N) (last pixel position) both remain unchanged after any number of iterations. These weaknesses will be very helpful for cryptanalysts or attackers to identify key vulnerabilities and break encryption systems [74, 75]. As an improvement, 3D maps have been introduced in [71, 76–78] ; the modified cat map and standard map have been proposed to overcome

the above mentioned problems [44, 71, 74].

For substitution purposes, substitution box (S-box), a type of basic nonlinear element in encryption algorithm, is the core of the famous AES and DES encryption algorithms [79]. Due to the properties such as non-linearity, differential uniformity and strict avalanche criterion, S-box has been considered to be an important tool in substitution operations [80]. Based on different algorithms on diverse chaotic maps, many new constructed S-boxes have been proposed [81–83]. In [84], a new structure of S-box based on logistic map and tent map is used in an image encryption system, where the plain image is divided into groups and dynamic S-box strategy is applied for different groups. In [85], a new image encryption scheme is designed based on a compound chaotic map and a strong S-box that is constructed by a logistic-since system. Authors in [86] have proposed two chaotic S-box schemes that are based on discrete chaotic maps using floating-point arithmetic and fixed-point arithmetic.

According to the different ways that how a slight change affects the ciphertext, most of the proposed diffusion algorithms can be categorized into two types.

The first type is : a slight change in the plaintext directly affects the ciphertext though the diffusion operations [74, 87]. But changing the pixel in different positions leads to different diffusion performance. Thus, usually, it needs more than one round of the diffusion operation, which causes computational consumption.

The second type is : a slight change in the plaintext first changes the initial conditions or parameters of the chaotic system in order to utilize the high sensitivity of chaotic system to achieve a huge different key stream, and then the changed key stream leads to a totally different ciphertext. That means, key stream for confusion-diffusion depends on not only the secret key, but also the original plain image. Thus, it should have a high resistance to chosen-plaintext attacks [88–90]. Some papers achieve this objective by relating statistical value (e.g. the sum of all pixels of an image) of the plain image to the secret key so as to change the key stream [91]. But there exists a risk of collision : the key stream may keep unchanged when pixels are changed but it results in the same statistical value.

Apart from these effective techniques and methods, the strategy of how to use them properly for a secure and robust image cryptosystem is an important issue. A good strategy is a good synergism of confusion and diffusion. In [92], a cryptosystem based on confusion-diffusion structure is proposed that uses a new constructed S-box based on a chaotic sine map for substitution, Hénon map for permutation and the hyper chaotic Lü map for producing the key stream. This permutation operates in bit-level, which accom-

plishes the diffusion effect simultaneously. Paper [93] has proposed a chaotic system that integrates the well-known 1D chaotic maps in a power-exponential structure two by two. The confusion-diffusion works in a sorting method based on the different chaotic systems. In [94], a symmetric color image encryption is developed based on tent map, Chebyshev map and piecewise linear chaotic map using a simultaneous confusion-diffusion operation that integrates the confusion and diffusion operations into a stage and makes them interact each other for higher diffusion property.

In addition, other encryption strategies have been brought out for the sake of high security and efficiency. Dependent diffusion and the aforementioned simultaneous confusion-diffusion have been presented in the literature, where the stage of confusion and diffusion can interact each other to improve the resistance capacity to attacks [2, 74, 94]. Plain image related encryption algorithm makes the generated dynamic key stream depending on both secret key and input plain image to achieve high cryptosystem's sensitivity to plaintext by creating different key streams for different input images [80, 95–98]. Self-adaptive methods divide a plain image into parts and make them encrypt each other in turn, which also can bring big differences in the ciphered image if the original plain image is slightly modified [99, 100]. Hash functions are designed to improve the security of cryptosystems [101, 102].

Not only the chaotic maps, other techniques also can incorporate chaotic dynamics for encryption purposes, for instance, DNA encoding [103, 104], compressed sensing [105–107], quantum coding [108], fractional Fourier transform [109], wavelet transform [110, 111], random grids [112] and elliptic curve ElGamal [113]. Also, hash function But all in all, chaotic dynamics is the pivotal component that is the core idea for the chaos-based encryption algorithms.

2.3.2 Pseudo-chaotic number generator

Different from the true random number generators (TRNGs) that come from the natural phenomena that are hard to control and utilize, PRNGs are easier to generate and reproduce pseudo-random numbers. Pseudo-random numbers are not true random, but look random. They are generated by a PRNG which is a deterministic system and each produced number uniquely depends on its previous one (called "seed"). If the initial seed is known, the pseudo-random sequence can be reproduced. This is an important feature since, in cryptosystem, the identical key stream must be reproduced in decryption algorithm using the identical secret key of the encryption process. Besides, pseudo-random numbers should

exhibit the highly similar statistical behavior as the true random numbers. The typical properties of pseudo-random numbers are uniform distribution, independence between two pseudo-random sequences produced by different seeds, and long periods [114]. There are commonly used test suites for evaluating the randomness property of a produced pseudo-random sequence, such as NIST (National Institute of Standard and Technology) test [115], TestU01 [116], ENT and DIEHARD [117]. Among them, NIST test suite is the most frequently used in the cryptographic applications.

PCNG is a chaotic PRNG. Since PCNGs generate a pseudo-random sequence as the key stream for the encryption algorithm, a properly designed PCNG has a crucial influence on the security of a cryptosystem, especially for the stream ciphers.

The initial conditions and parameters of the PCNG constitute the secret key of a cryptosystem. According to Kerckhoffs' principle and Shannon's information security theory, the PCNG is crucial to the security of a cryptosystem and it should possess a large key space and be able to produce the key stream with pseudo-randomness and high sensitivity properties in order to ensure a high level of resistance to the common attacks.

In general, low-dimensional chaotic maps have the advantages of simple structure and relatively easy implementation, but they cannot be used alone to design PCNGs owing to their uneven distribution orbits with low periodicity and small key space. Nevertheless, a proper method of combining low-dimensional chaotic maps has been proven to be efficient for PCNG design. To enhance the chaotic property and increase the unpredictability, based on several low-dimensional chaotic maps, many effective approaches have been proposed.

Basically, a PCNG can be achieved in a cascade structure or a parallel structure. A cascade structure can enhance chaotic property using the idea that the output of one chaotic map is the input of the another chaotic map. But this structure has limited contribution to enlarging the key space and it can accumulate the errors caused by dynamical degradation over finite precision platforms [118]. A parallel structure means the adopted chaotic maps are arranged in parallel. It can expand the key space effectively because the initial conditions and parameters for each adopted chaotic maps can be a part of the secret key [119]. But it needs further methods to integrate the multiplex chaotic sequences and enhance the chaotic property. To this end, many effective methods have been proposed and they are discussed in the following.

Coupling method has been proven to be efficient to design PCNGs. It makes the employed chaotic maps interact with each other's behavior (orbit) and, in this way, the nonlinear behavior can be greatly complexified. Based on tent and logistic maps, O.Garasym

et al. explored a chaotic coupling method with topology network to design PCNG [42]. R. Lozi brought out a weak coupling approach to hide the chaotic functions and enhance the chaotic dynamics [120]. M.Sahari et al. proposed a PCNG for a color image encryption algorithm by coupling PWLCM and an enhanced 2D logistic maps [121]. C.Zhu et al. presented a PCNG based on a coupled logistic-tent chaotic system that gained a wider parameter range and better chaotic features [122]. O.Jallouli et al. [123] designed and implemented two stream ciphers working on 32-bit based on three discrete chaotic maps : PWLCM, skew tent map and logistic map. The first stream cipher adopts a weak coupling scheme [120] to couple the chaotic maps, while the second one uses a binary diffusion matrix to achieve a good coupling effect. These two coupling methods work with a multiplexing technique, which makes the proposed stream ciphers robust to generate uniformly distributed and pseudo-random featured ciphered image. Furthermore, mixing is another effective strategy to integrate the multiplex chaotic sequence. R. Hamza proposed a PCNG based on a combination of the three coordinates of the Chen chaotic orbits and it adopted the approach of cascading and mixing the orbit samples to overcome the degradation problem during the finite precision computations [43]. In [44], the authors implemented a robust PCNG for a block cipher by connecting skew tent map and PWLCM map in parallel, and in this PCNG, a linear feedback shift register (LFSR) was designed to ensure very large periods for all generated sequences.

In addition, other techniques also can be found in the existing literature. A new form of the power-exponential chaotic structure for encryption purpose was presented in [93]. It can integrate 1D chaotic maps to achieve good chaotic behavior, but needs a considerable computational consumption. In paper [124], authors proposed a new PCNG scheme based on coupled map lattice with time-varying delay and used it to achieve a simple image encryption that could resist the differential attack. Y.Zhang divided the AES S-box into four zones to form a 3D S-box. Two pseudo-random key streams could be generated based on this cubic S-box depending on the two different binary orders in each integer value of a piece-wise linear chaotic sequence. The key streams passed the randomness test and applied into two image encryption schemes [125,126]. Based on the logistic map, Garcia-Bosque et al. proposed a bitwise PCNG that changed the parameters dynamically and could pass the NIST test [127]. In the encryption scheme in [128], quantum chaotic map was utilized to be the random source of the key stream. A generalized fractional order chaotic systems based on logistic map and Chen map were designed as PCNG for secure stream ciphers [129,130]. Based on the ISAAC (indirection, shift, accumulate, add, and count) cipher and XOR shift

generators, authors in [131] proposed a fast PCNG which used the chaotic iterations to combine the above components.

Notice that, PCNG is first and foremost a pseudo-random number generator (PRNG). In addition to being useful in cryptography field, PCNG also can be used in many PRNG needed situations. PRNG is widely acknowledged as a vital component for a plethora of applications that involve diverse fields, such as numerical simulations, communication systems, sampling, entertainment, decision making, numerical analysis, control theory, etc [11]. Some of the most commonly used PRNGs are based on numerical methods, for instance, linear congruential generator (LGG), mid-square method generator, lagged Fibonacci generator, and linear feedback shift registers-based generator (LFSR) . However, many of these systems have been proven to be insecure and biased owing to their correlations or short periods. What's worse, their heavy computational requirements make them hardware unfriendly and thus they are not a good choice to many applications [132,133]. By contrast, due to the ease of implementation and nonlinear complex behavior, PCNG is more efficient than the numerical PRNG. Therefore, the significance of studying PCNG is not only that it is a vital part of the cryptography, but also that it can be used as a PRNG to play an important role in various fields.

2.3.3 Existing problems and solutions

Although many chaos-based image cryptosystems have been proposed, some of them do not possess the high security as they claimed and they have been proven to be vulnerable to certain kinds of attack.

F.Mousa et al. [75] analyzed the security of a chaos-based image cryptosystem [74] which used the logistic map to perform the dependent diffusion and demonstrated its diffusion effect can be removed because its argument is exposed in the ciphered image. As a result, key space has been reduced and permuted version of the ciphered image could be recovered, which made the brute-force attack and chosen plaintext attack possible. But if the encryption process is iterated twice (two rounds), the system [74] can be considered to be secure. Actually, multiple rounds of an encryption scheme can increase the encryption complexity and increase the security to some extent, but consequently, it will cause low efficiency [134]. However, there also exists evidence that has proven multiple rounds of an encryption scheme can not ensure absolute security. Authors of [135] cracked an encryption scheme [136] by differential attack even if it has the multi-round encryption strategy. The problem of [136] existed in its encryption scheme whose security merely depended on

its permutation key instead of all of the keys, which made the key space greatly reduced. Thus, beside the low efficiency shortcoming, multiple rounds cannot ensure a high security.

In a positive turn of events, an increasing number of papers aim to design efficient and secure cryptosystems using only one-round encryption. But the existing problems cannot be ignored. In [137], the secret key has been divided into two groups for chaotic system and rectangular transformation permutation. However, [138] has indicated that the rectangular transformation does not work for all pixels, and [139] has proven that the secret key for permutation can be recovered by using square test images and this scheme can be cracked by brute-force attack and chosen-plaintext attack. Paper [140] has pointed out the weakness of [141] : a parameter depends purely on the average intensity of a plain image, and then [140] has broken the image of [141] effectively by a collision-based inference algorithm. Authors of [142] has been able to obtain an equivalent secret key of [143] and has cracked [143] using the chosen-plaintext attack. [144] has demonstrated that [145, 146] have design defects in confusion and diffusion, and the avalanche effect are not complex enough which allows the attacker to reveal the key stream and break the system by the chosen-plaintext attack. Paper [147] has broken the scheme in [148] using differential attack, since [148] can be degraded to a diffusion-only algorithm and permutation-only algorithm. In addition to this, owing to incomprehensive consideration in security, cryptosystems proposed in [149–152] have been proved not resistant to chosen-plaintext attack by papers [153–156] correspondingly.

Taking a deeper look in these insecure cryptosystems, we can find that they have the following primary problems : (1) insufficient confusion and diffusion requires multiple rounds leading to low efficiency, which hinders these schemes to be applied in real-time applications [74, 75, 136] ; (2) insecure and not complex enough confusion and diffusion may leak the information of the key stream or even the secret key [137–143] and the effect of confusion or diffusion can be removed by cryptologist leading to the diffusion-only or confusion-only scheme that can be easily cracked [140, 141, 144–148] ; (3) key stream without cryptographic features can expose the secret key [137–143]. The above three problems call for effective solutions : a secure and complex confusion and diffusion strategy, and a cryptographic key stream that can protect the secret key. As for the latter, a PCNG that can generate pseudo-chaotic key stream with good randomness and chaotic properties is an excellent approach. Many PCNGs with larger Lyapunov exponent have been proposed, but not all of them can be applied to encryption applications because some of them lack cryptographic analysis [11].

Other than the above discussed problems and solutions, there exists a crucial issue regarding to all the chaos-based image cryptosystems : dynamical degradation encountered in chaotic systems over finite precision implementation platforms.

A great majority of the well-known chaotic maps are defined using real numbers. Based on these chaotic maps, most of the proposed PCNGs work in continuous-space domain. However, chaotic orbits produced by finite precision platforms will not exhibit the ideal infinite chaotic behavior due to the quantization in the digital devices, as a result, it is inevitable that the dynamical degradation will occur [11]. What's worse, due to the quantization, truncations or round-offs in digital implementations, the adopted chaotic maps using real numbers may lose chaotic features, even may drop into periods or fixed points. As a result, the PCNG has a high risk of losing randomness, which damages the reliability of the PCNG and leads to a security breach of a chaos-based cryptosystem. In addition to this drawback, from the hardware perspective, the computation of floating-point numbers (especially the double precision notation) has the disadvantages of slow data transfer and inefficient resource utilization when compared to the fixed-point numbers and integer numbers [133].

To solve these problems, a digital chaotic system with finite precision has been proposed in [157]. Also, fixed-point solutions have been investigated in [133, 158]. [133] has examined the finite precision effect of the skew tent map using the fixed-point notation and has proposed a binary PCNG based on a crossed-coupled skew tent map scheme that works using 40 bits with 32 bits of fraction length. [158] has introduced a fixed-point hardware realization (FPGA) of a PCNG based on the logistic map using 45 bits bus size. Due to the arithmetic operations of fixed-point numbers are same as integer arithmetic, from the hardware implementation perspective, fixed-point numbers and integers have the advantages of higher data transfer and more efficient resource utilization when compared to the floating-point numbers. S.El Assad has proposed number of works in chaos-based cryptography including efficient PCNGs, secure stream ciphers and block ciphers, based on multiple low-dimensional chaotic maps that are reformulated over a positive integer field with 32 bits precision [44, 58, 123, 159]. Also, H.Li et al. proposed a PCNG based on the logistic map, PWLCM and skew tent map using 32-bits positive integers [119].

2.4 Conclusion

In this chapter, the basis of the chaos-based cryptosystem has been introduced. We focus on the symmetric-key encryption algorithm, present the chaos-based confusion-diffusion

encryption scheme and give the common cryptographic attacks. From the literature analysis we made in this chapter, many effective techniques have been proposed for chaos-based cryptosystems and PCNG designs. However, the existing problems cannot be ignored. Low efficiency and insecurity are caused by the insufficient and not complex confusion-diffusion operations, and not well-used PCNGs. Besides, a crucial issue concerning the reliability of PCNG and security of a chaos-based cryptosystems is how to overcome the dynamical degradation of chaotic maps encountered in the finite precision implementations.

The good performance of a new chaos-based cryptosystem is not only dependent on one component. A secure and efficient encryption scheme is a result of the synergy between each parts (PCNG, confusion-diffusion scheme, encryption algorithm). Thus, designers devoted to chaos-based image cryptosystems cannot neglect the importance of every component. To solve the existing problems and design secure chaos-based cryptosystem, we first redefine four well-known 1D chaotic maps over an integer field in Chapter 3 since using integers is a good solution to eliminate the security breach caused by the quantization, round-off errors over finite platforms and it is more hardware friendly and efficient than floating-point numbers and fixed-point numbers. Then, a new PCNG with simple structure will be designed for a chaotic stream cipher in Chapter 4. It can overcome the dynamical degradation and achieve good cryptographic properties (large key space, high sensitivity to the secret key and pseudo-randomness). After that, a novel secure chaos-based cryptosystem including an inner block cipher will be proposed in Chapter 5. There is no doubt that PCNG is a crucial component in a chaos-based cryptosystem. A PCNG is also a PRNG that plays an important role in various fields and applications. To explore a new coupling method to design PRNG over an integer field, a new smart coupling will be developed in Chapter 6. Besides, based on the new coupling scheme, a family of PRNGs will be evaluated.

CHAPITRE 3

ONE-DIMENSIONAL CHAOTIC MAPS OVER A FINITE INTEGER FIELD

3.1 Introduction

Image encryption algorithms are defined on finite set of integers, while the chaotic maps are defined using real numbers. L.Kocarev has pointed out that this is an important difference between chaotic dynamics and image encryption [57]. Thus, the PCNG based on integers will be more appropriate for image encryption.

In this chapter, 1D chaotic maps include logistic map, skew tent map, PWLCM, and Chebyshev 3rd order chaotic map will be reformulated over an N-bit (N=32) finite integer field in Section 3.2. It will overcome the quantization and round-off errors which arise when the chaotic maps using real numbers are numerically implemented. Thus, deviation caused by finite precision of digital devices is eliminated in the produced chaotic numbers. Consequently, the PCNGs based on these maps have a high reliability to be applied over different platforms regardless of the finite precision. In addition, compared to the floating-point and fixed-point notations, integer definitions have the advantages of reduced resource utilization, higher data transfer and ease of implementation, which are much more efficient and hardware friendly.

However, dynamical degradation is inevitable in the finite precision implementation. In the literature, some works used integer chaotic maps [44, 102, 160, 161], but they did not analyze the dynamical degradation of the redefined maps. From the cryptographic perspective, this chapter gives a more complete analysis of the reformulated chaotic maps. Effect of finite precision will be discussed in Section 3.3. Furthermore, key space of cryptosystems depends on the precision of the used chaotic maps. For the reformulated chaotic maps, the finite precision determines the key space when they are used for encryption purposes. Hence, the key space contribution of the reformulated chaotic maps will be analyzed in Section 3.4.

3.2 Reformulated chaotic maps over an integer field

3.2.1 Logistic map

The logistic map (1.13) for $\mu = 4$ redefined over the N-bit finite field is given as below :

$$X(n+1) = \begin{cases} \lfloor \dfrac{X(n) \times \left(2^N - X(n)\right)}{2^{N-2}} \rfloor, & if\ X(n) \neq \dfrac{3}{4} \times 2^N\ and\ 2^N \\ 2^N - 1, & if\ X(n) = \dfrac{3}{4} \times 2^N\ or\ 2^N \end{cases} \tag{3.1}$$

where X is the generated chaotic sequence ; $X(n)$ is the $n-$th number in X and $1 \leqslant X(n) \leqslant 2^{\mathrm{N}} - 1$; $N = 32$; $\lfloor \cdot \rfloor$ means the nearest integer that is not bigger than the element in it.

The reformulated logistic map has been shown in Figure 3.1, where there is one fixed point shown in the region of $[1, 2^N - 1]$, that is $\frac{3}{4} \times 2^N$ (marked with a small red circle). Equation (3.1) already avoids the fixed point and also gets around the problem of fixed point preimages (explained in Chapter 1). This can prevent the orbits from reaching undesirable states (fixed point or its preimages) if the latter have been accidentally (randomly) selected as initial conditions, and will ensure pseudo-chaotic properties.

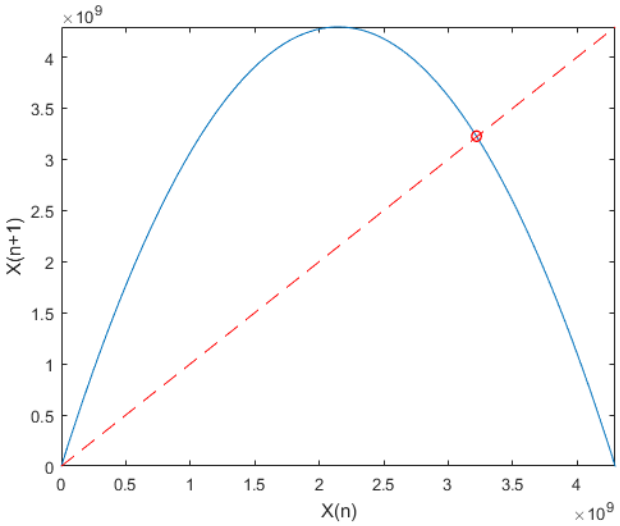


FIGURE 3.1 – Reformulated logistic map

3.2.2 Skew tent map

The reformulated skew tent map is defined as follows :

$$X(n+1) = \begin{cases} \lfloor 2^N \times \dfrac{X(n)}{P} \rfloor, & if\ 0 < X(n) < P \\ \lfloor 2^N \times \dfrac{2^N - X(n)}{2^N - P} \rfloor, & if\ P < X(n) < 2^N \\ 2^N - 1, & otherwise \end{cases} \tag{3.2}$$

where the notations are similar to those in the logistic maps ; P is the control parameter ranging in $[1, 2^N - 1]$.

The reformulated skew tent map can be seen in Figure 3.2, where there is one unstable fixed point shown in the small red circle. The value of this point is related to the control parameter P. To avoid this value, Equation (3.2) can be modified by :

$$X(n+1) = X(n+1) - 1,\ if X(n+1) = X(n)$$

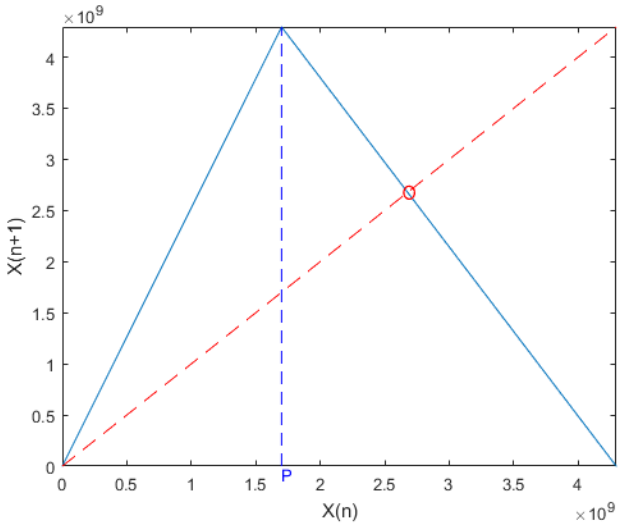


FIGURE 3.2 – Reformulated skew tent map

3.2.3 Piece-wise linear chaotic map (PWLCM)

Reformulating the piece-wise linear chaotic map (PWLCM) in the N-bit finite field is :

$$X(n+1) = \begin{cases} \lfloor 2^N \times \dfrac{X(n)}{P} \rfloor, & if\ 0 < X(n) < P \\ \lfloor 2^N \times \dfrac{X(n) - P}{2^{N-1} - P} \rfloor, & if\ P < X(n) < 2^{N-1} \\ \lfloor 2^N \times \dfrac{2^N - P - X(n)}{2^{N-1} - P} \rfloor, & if\ 2^{N-1} < X(n) < 2^N - P \\ \lfloor 2^N \times \dfrac{2^N - X(n)}{P} \rfloor, & if\ 2^N - P < X(n) < 2^N \\ 2^N - 1, & otherwise \end{cases} \tag{3.3}$$

where the notations are similar to those in the logistic map ; $P \in [1, 2^{N-1} - 1]$ is the control parameter of PWLCM.

The function of PWLCM can be seen in Figure 3.3, where three unstable fixed points have been identified. To avoid the fixed point, Equation (3.3) can include :

$$X(n+1) = X(n+1) - 1, if X(n+1) = X(n)$$

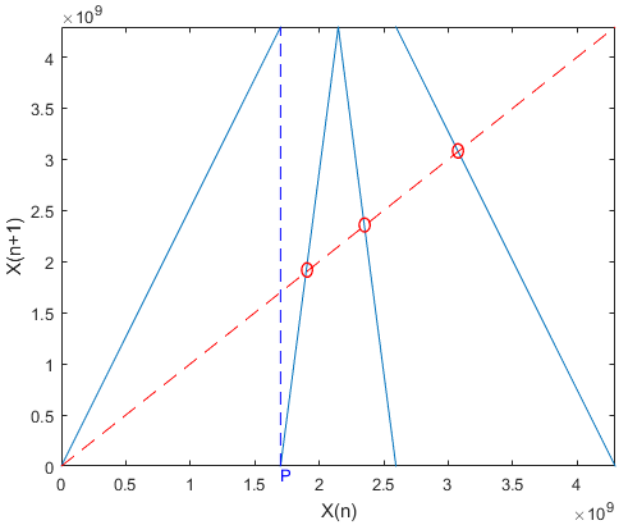


FIGURE 3.3 – Reformulated PWLCM

3.2.4 Chebyshev chaotic map

Here below is the Chebyshev 3rd order chaotic map reformulated over the N-bit finite field :

$$X(n+1) = \begin{cases} 2^N - 1, & if\ X(n) = 0\ or\ \frac{1}{2} \times 2^N\ or\ 2^N \\ \lfloor 2^{-2N+2} \left[4 \times \left(X(n) - 2^{N-1} \right)^3 - 3 \times 2^{2N-2} \times \left(X(n) - 2^{N-1} \right) \right] + 2^{N-1} \rfloor, & otherwise \end{cases} \tag{3.4}$$

where the notations are similar to the logistic map.

The delayed phase space of this map is shown in Figure 3.4, where there exists one fixed point : $\frac{1}{2} \times 2^N$ that has been avoided by Equation (3.4).

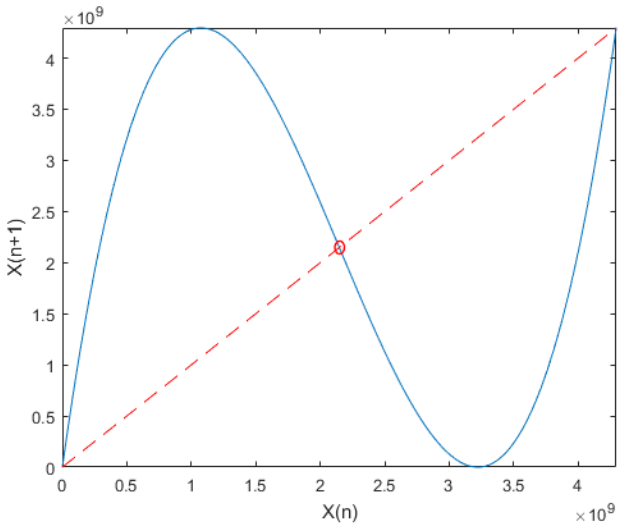


FIGURE 3.4 – Reformulated Chebyshev 3rd order chaotic map

3.3 Effect of finite precision

Chaotic systems exhibit infinite period orbits in analog communication or ideal infinite precision situations. However, in reality, digital device with finite precision will not support the infinite feature of chaos. When chaotic systems are applied in digital implementation, effect of finite precision is inevitable. It leads to the dynamical degradation in chaotic sys-

tems : the orbits become periodic or even locked into fixed points ; their distribution and correlation property will be deteriorated.

The period of cycle thus obtained is usually greatly smaller than the total number of states of the finite notation. Figure 3.5 shows a typical orbit that falls into a cycle in digital chaotic system.

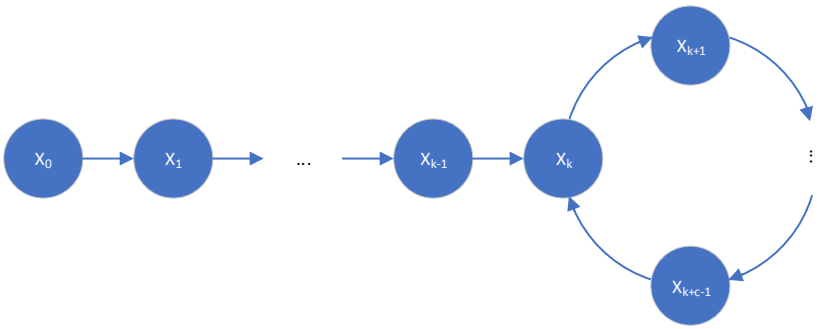


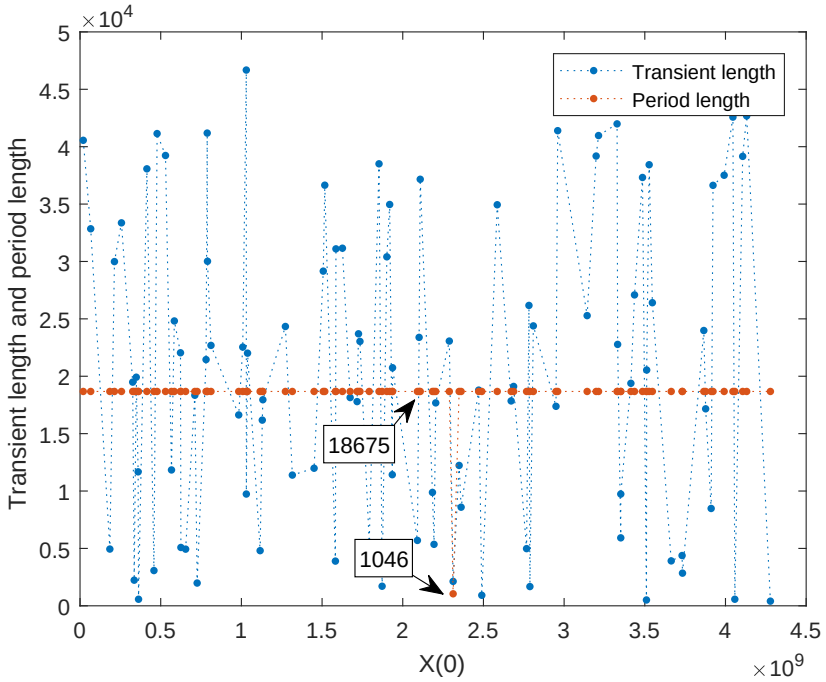
FIGURE 3.5 – Orbit of a chaotic system with finite precision

— The orbit is : $X_0, X_1, ..., X_{k-1}, X_k, X_{k+1}, ..., X_{k+c-1}$. The length of the orbit is $k+c$.
— Transient part of the orbit is formed by : $X_0, X_1, ...X_{k-1}$. The transient length is k ;
— Cycle part of the orbit is formed by : $X_k, X_{k+1}, ...X_{k+c-1}$. The period length is c.

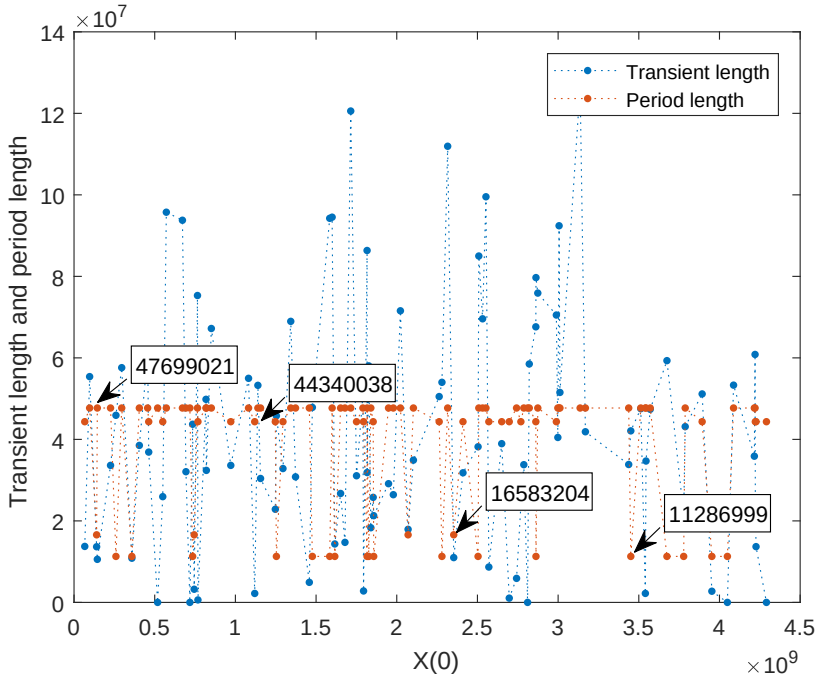
If a chaotic map is defined over an integer field with N bits and its states vary between 1 and $2^N - 1$, the theoretical maximum length of the orbit is $2^N - 1$. But it is improbable to get this number.

3.3.1 Period analysis in different precision N

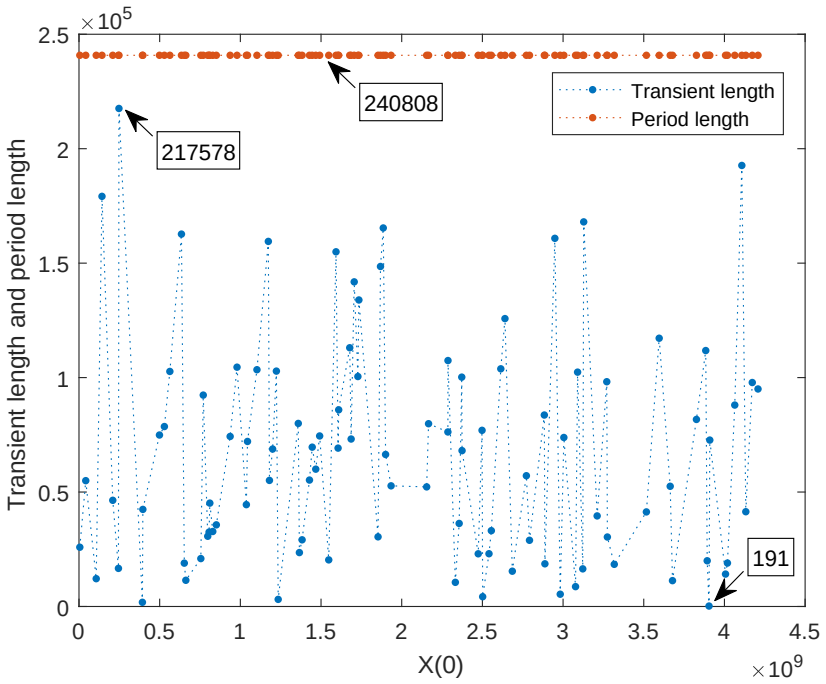
There is no doubt that a trajectory of a chaotic system with finite precision will fall into a cycle. If the length of the cycle is 1, it means the trajectory is locked to a fixed point. In other words, the period of the orbit is 1. To analyze the periods of the above four reformulated chaotic maps, for each map, 100 different initial conditions $(X(0))$ have been randomly created by MATLAB. For each initial condition, their transient lengths and period lengths have been calculated and recorded in Figure 3.6.



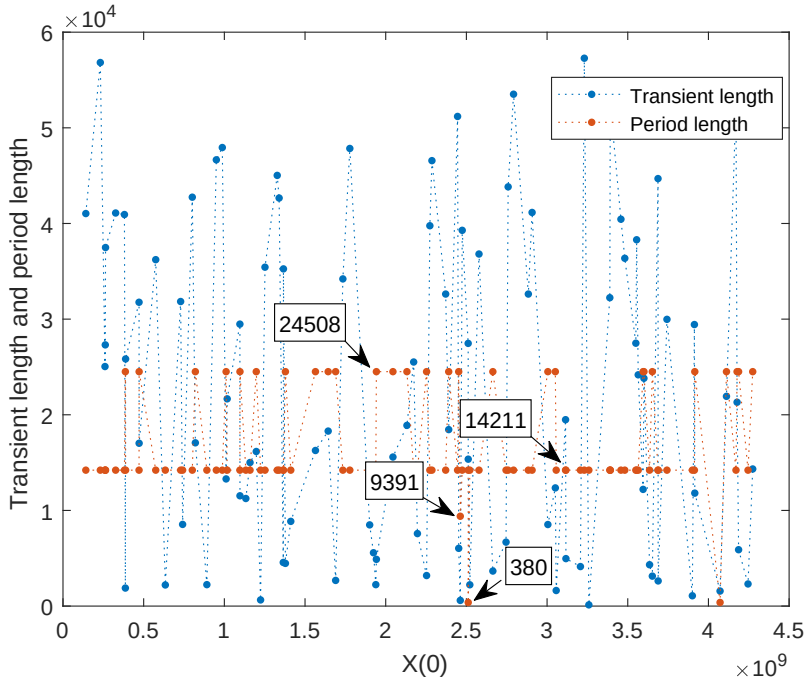
(a) Logistic map



(b) Skew tent map



(c) PWLCM



(d) Chebyshev 3rd order chaotic map

FIGURE 3.6 – Transient length and period length tested in the above reformulated integer chaotic maps ($N = 32$)

With the $N = 32$ bit finite precision, all the test sequences have shown the periodicity. According to Figure 3.6, the detected period of PWLCM i.e. 240808, is almost 10 times longer than the maximum period of logistic map, i.e. 18675, and Chebyshev 3rd order chaotic map, i.e. 24508. The detected minimum period of skew tent map, i.e. 11286999, is almost 100 times longer than the period of PWLCM. The detected transient lengths of skew tent map are also much larger than the others'. Therefore, we can observe that the skew tent has relatively long transient length and period. This is more consistent with the characteristic requirements of random numbers.

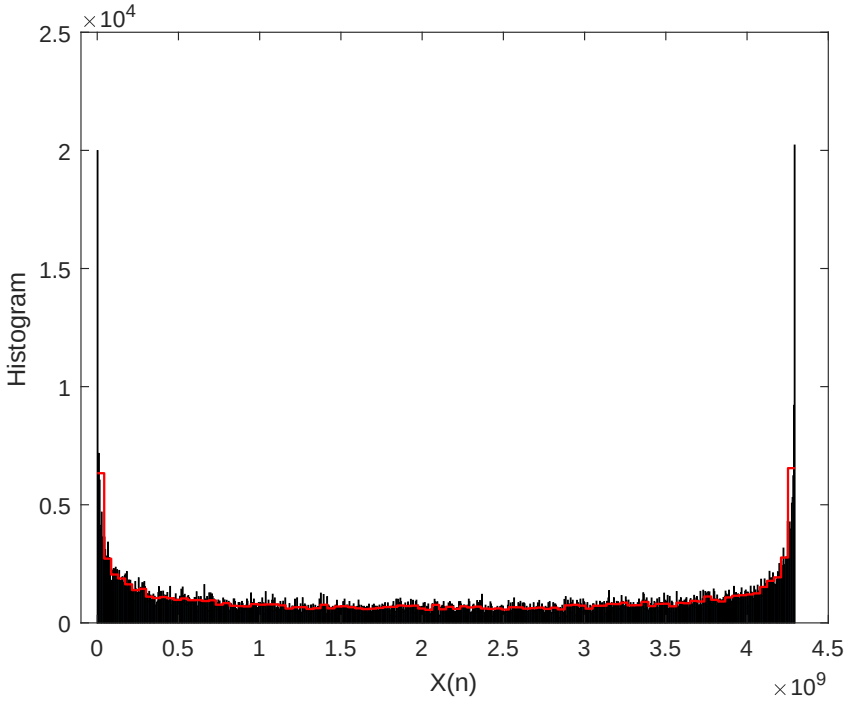
3.3.2 Histogram

Histograms shown in Figure 3.7 reveal the distribution properties of each sequence generated by each chaotic map. For each sequence, 2×10^6 values are produced but the first 10^6 are discarded as transient and the rest 10^6 are plotted in 1000 classes in the histograms, where the red curves are the average values in each 10 classes.

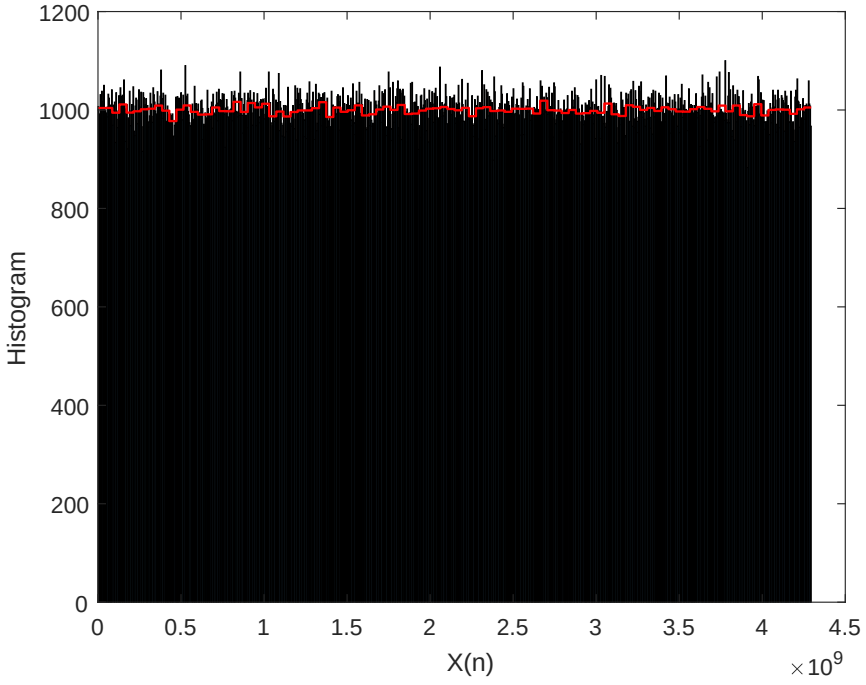
According to Figure 3.7, we can observe that the piece wise linear maps, including skew tent map and PWLCM, show much better uniform distribution than the logistic map and Chebyshev 3rd order chaotic map. Furthermore, skew tent map has the best uniformity than the other maps.

In addition, it appears that these histograms have similar distribution properties with those of the original chaotic maps defined using reals (Figure 1.18, 1.23, 1.28, 1.33). There seems no distinct different distribution caused by the finite precision. However, if the precision decreases to $N = 16$ bits, the effect of finite precision becomes more obvious.

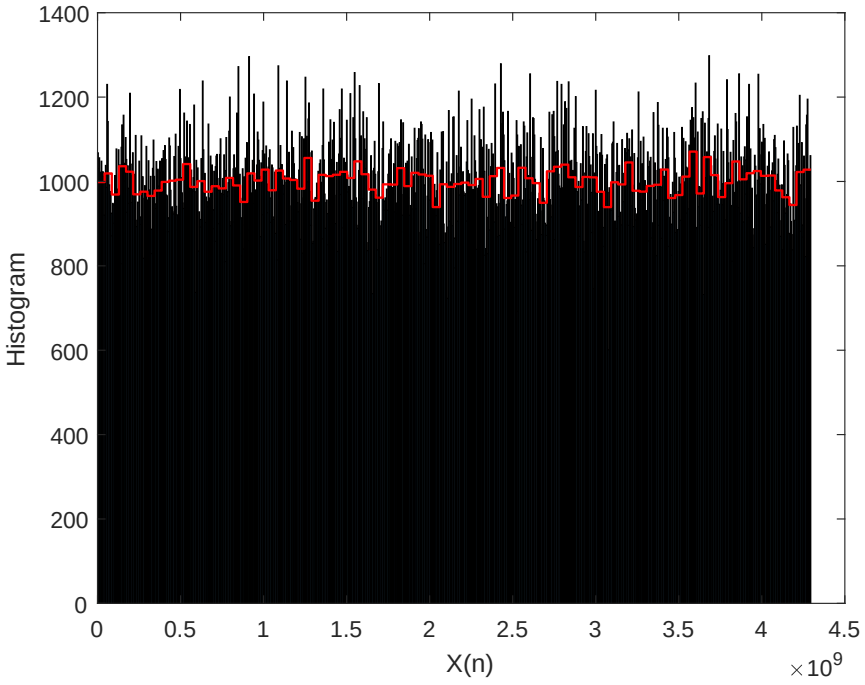
When $N = 16$ bits, a chaotic sequence is generated by the logistic map (3.1) with the length of 10^6. Its histogram plotted in 1000 classes has been shown in Figure 3.8. The length of the orbit is 149 which is quite smaller than 2^{16}. Due to the dynamical degradation caused by finite precision, the numbers generate by logistic map only distributed discretely in the histogram instead of covering all the statistical intervals. This result correspond to the period analysis in Section 3.3.1. This effect can be reduced by increasing the finite precision (e.g. in Figure 3.7(a), the distribution with $32-$bit precision seems more dense than Figure 3.8). But the bad effect of finite precision can not be completely eliminated. Figure 3.6(a) has indicated that even the trajectory produced with $32-$bit precision, it will still fall into a cycle eventually.



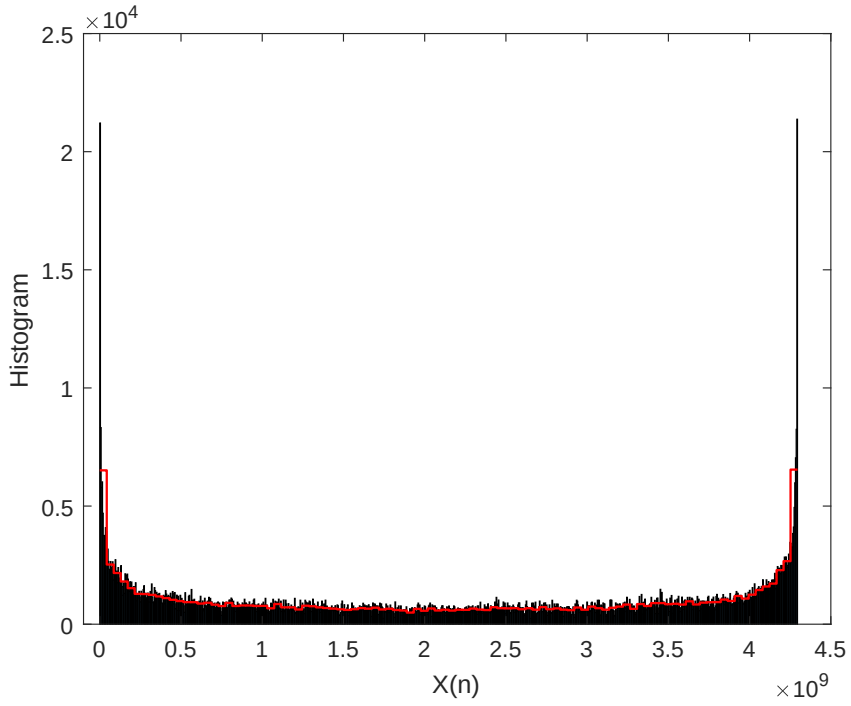
(a) Logistic map



(b) Skew tent map



(c) PWLCM



(d) Chebyshev 3rd order chaotic map

FIGURE 3.7 – Histograms of the above reformulated integer chaotic maps (red curve in the figure represents the averages of each 100 classes)

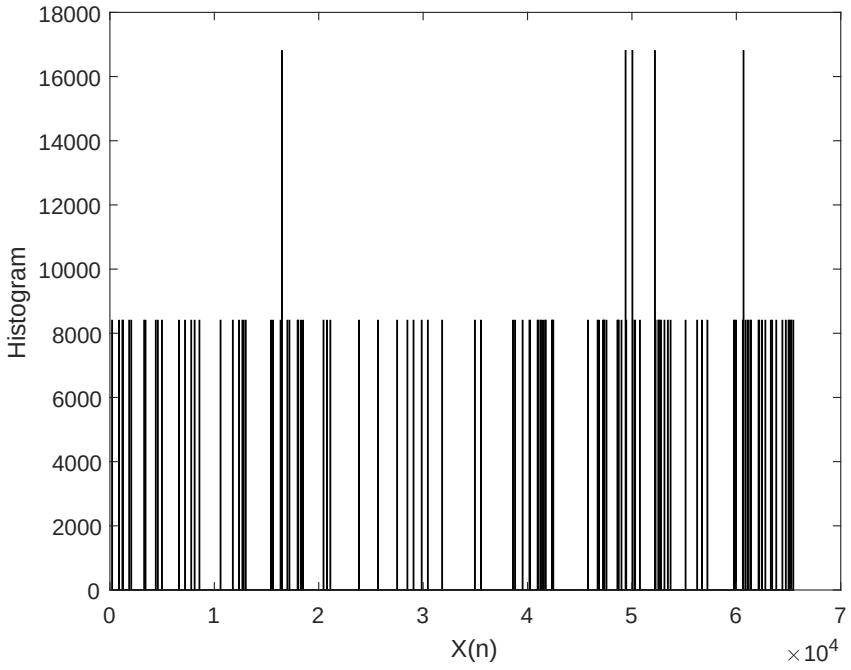


FIGURE 3.8 – Histogram of a sequence generated by logistic map with $N = 16$ bits finite precision (Initial condition $X(0) = 8323$ is created randomly)

3.4 Key space contribution

The key space of an encryption system should be large enough to resist the brute-force attack. According to the existing literature, the key space of a cryptosystem should be equal or bigger than 2^{128} [7].

Unlike the statistical and security performances, which only can be tested after completing the design of a PCNG, key space needs to be taken into account when we are conceiving a new PCNG scheme for cryptosystems.

Initial conditions and parameters of a chaotic map constitute the key space. The precision of the chaotic maps directly affects the key space. For logistic map and Chebyshev 3rd order chaotic map, only N bits initial conditions can serve as key space, while for the skew tent map and PWLCM, other than their N bits initial conditions, N bits and $N - 1$ bits control parameters can be counted into key space as well. Thus, skew tent map and PWLCM can provide $2N$ and $2N - 1$ for the key space, which are almost twice that of the logistic map and Chebyshev 3rd order chaotic map.

3.5 Conclusion

In this chapter, we have introduced the reformulated functions of logistic map, skew tent map, PWLCM and Chebyshev 3rd order chaotic map over the $N-$bit ($N = 32$) finite integer field. The original chaotic maps have been historically defined over a real domain using real numbers. If they are adopted for encryption purposes, initial conditions should be set carefully to avoid preimages of the fixed points since these initial conditions will make the evolving chaotic orbits fall into fixed points eventually. In contrast, initial conditions of the reformulated chaotic functions can be randomly selected, since they are defined over a finite integer field using discrete values. We have avoided the fixed points in the reformulated chaotic map definition and therefore, have overcome the problem caused by their preimages.

Finite precision will give rise to dynamical degradation and thus the produced sequence by the chaotic maps with finite precision will fall into a period/cycle. What a good key stream demands is a very long period and a uniform distribution of the output pseudo-chaotic sequence. Thus, the effect of finite precision has been analyzed in terms of period and histogram aspects. According to the test results, it can be seen that the skew tent map has longest periods and the best uniform distribution performance among the four chaotic maps. Followed by the skew tent map, it is the PWLCM that shows the similar property with skew tent map, but from periodicity and distribution perspective, it is slightly less prominent than the skew tent map.

The chaotic maps that will be used in a design of a cryptosystem. The precision of the chaotic maps determines the key space. Key space should be large enough to resist the brute-force attack. The key space contributions of the logistic map, skew tent map, PWLCM and Chebyshev 3rd order chaotic map are N, $2N$, $2N-1$ and N respectively.

In the following chapters, we will use these finite integer field redefined 1D chaotic maps to design secure and robust encryption algorithms and PCNGs.

CHAPITRE 4

PROPOSED CHAOS-BASED STREAM CIPHER

4.1 Introduction

PCNG using parallel structure can increase the key space. In this chapter, we will propose a new simple and efficient PCNG in parallel structure and then apply it to the design of a secure stream cipher. The PCNG works over the 32 bit finite field and it is based on three discrete chaotic maps, that is, PWLCM (3.3), skew tent map (3.2) and logistic map (3.1). Only four XOR operators are adopted in this scheme to mix these 1D chaotic maps to form the intermediate chaotic outputs as well as the decision samples which operate cooperatively under a dynamic output control mechanism to generate the final pseudo-chaotic sequence. The produced pseudo-chaotic sequence is the key stream for the stream cipher.

In the following, the proposed PCNG and the stream cipher are described in Section 4.2 ; in Section 4.3, performance analyses of the PCNG in terms of computational performance and statistical analysis are given in Section 4.3.1 ; Section 4.3.2 presents the cryptanalytic analysis results of the stream cipher including key space analysis, uniformity test, entropy test, correlation analysis and key sensitivity analysis. Finally, we draw the conclusion in Section 4.4.

4.2 Proposed stream cipher

The proposed stream cipher is achieved by using XOR operation to mask the plaintext with the key stream provided by the PCNG. The core of the stream cipher is the new designed PCNG.

The scheme of the proposed PCNG is presented in Figure 4.1. It is based on three classical discrete chaotic maps : $Fp[Xp(n-1)]$, $Fs[Xs(n-1)]$ and $Fl[Xl(n-1)]$,

namely PWCLM (3.3), skew tent map (3.2) and logistic map (3.1) with $N = 32$ bits. They operate in parallel to produce chaotic numbers, and then these numbers are processed by XOR operators (denoted by $\oplus$) and a dynamic output control mechanism to form the final output sequence that is the key stream for the stream cipher. Chapter 3 has demonstrated that all these original maps are chaotic but exhibit poor dynamic properties for encryption purposes when taken alone.

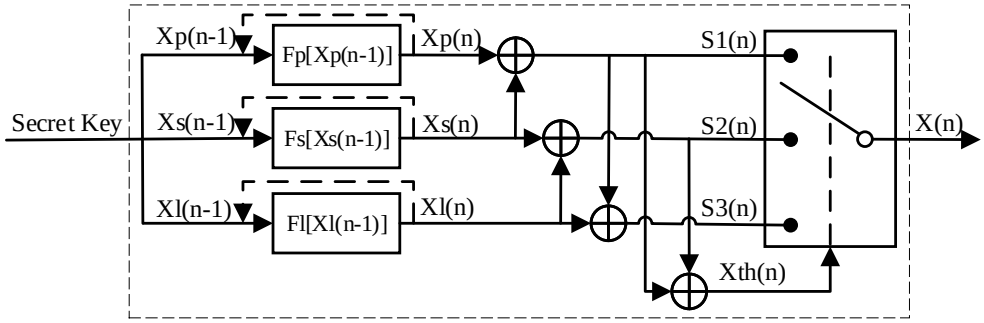


FIGURE 4.1 – The proposed PCNG scheme for the stream cipher

The secret key of the PCNG contains the initial conditions of the PWLCM, skew tent map and logistic map that are $Xp(0)$, $Xs(0)$, $Xl(0)$ respectively and the parameters of PWLCM and skew tent map that are Pp and Ps. Notice that, $Xp(0)$, $Xs(0)$, $Xl(0)$, Ps are integers in the the range of $[1, 2^N-1]$ while Pp is integer in the range of $[1, 2^{N-1}-1]$. $S1(n)$, $S2(n)$, $S3(n)$ are three intermediate outputs that come from the following expressions :

$$\begin{aligned} S1\,(n) &= Xp\,(n) \oplus Xs\,(n) \\ S2\,(n) &= Xs\,(n) \oplus Xl\,(n) \\ S3\,(n) &= Xp\,(n) \oplus Xs\,(n) \oplus Xl\,(n) \end{aligned} \tag{4.1}$$

The usage of the convertible XOR operators can improve the chaotic characteristics effectively in comparison with the single original chaotic maps. The final output $X(n)$ is controlled by the a decision sample $Xth(n)$ with two thresholds $Th1$ and $Th2$, where $Xth(n)$ can be considered as a dynamic parameter to switch between $S1(n)$, $S2(n)$, $S3(n)$:

$$X\,(n) = \begin{cases} S1\,(n)\,,\ if\ 0 < Xth\,(n) < Th1 \\ S2\,(n)\,,\ if\ Th1 < Xth\,(n) < Th2 \\ S3\,(n)\,,\ otherwise \end{cases} \tag{4.2}$$

where $Xth = S1\,(n) \oplus S2\,(n) = Xp\,(n) \oplus Xl\,(n)$ and $Th1 = 0.8 \times 2^N$, $Th2 = 0.9 \times 2^N$.

This kind of dynamic output control is designed to increase the scheme complexity and enhance the randomness

4.3 Performance analysis

In this section, we will discuss the performance of the proposed stream cipher. All simulations are conducted in MATLAB (R2017b) on a computer of Intel Core i-7-3770 CPU in Windows 7 Professional, 64-bit operating system with 3.4GHz processor, 8 GB RAM.

4.3.1 Performance analysis of the proposed PCNG

Firstly, performance of the proposed PCNG is evaluated in terms of computational performance and statistical analysis. Histogram, χ^2 test and NIST test have been adopted to analyze the statistical properties. All these tests are used to explore and verify the cryptographic and randomness performances of the proposed PCNG.

Computational performance

The execution time of an algorithm not only depends on the complexity of an algorithm, but is affected significantly by the programming language, operating environment, code optimization, etc. It will cause biased result if we compare two algorithms that operate using different programming language in different operating environments. Thus, here, for evaluating the computational performance, we give below the results in terms of average bit rate (Mbps) and average NCpB (Number of needed Cycles to generate one Byte) which can provide relatively fair results. For that, we generate 100 chaotic sequences with length of 31250 samples in each sequence using 100 different secret keys. Then the average generation time of these 100 sequences is calculated.

The bit rate and NCpB are given by the following relations :

$$\begin{aligned} Bit\ Rate\ \ (Mbps) &= \frac{Generated\ data\ size\ \ (Mbits)}{Average\ genertion\ time\ \ (s)} \\ NCpB &= \frac{CPU\ \ speed\ \ (Hz)}{Bit\ \ Rate\ \ (Byte/s)} \end{aligned} \tag{4.3}$$

The obtained results of the proposed PCNG and other PCNGs simulated in the similar environment are shown in Table 4.1, from which we can find our PCNG has achieved a higher speed than the others.

TABLE 4.1 – Time consuming results

PCNG	Bit Rate (Mbps)	NCpB
Proposed PCNG	17.679	1539
Ref. [10]	1.7	9411
Ref. [162]	0.49	45714

Actually, if analyzing the proposed PCNG, from the perspective of computational complexity, the major time consuming component is existed in the iterations of three chaotic maps (PWLCM, skew tent map and logistic map). However, the iterations of chaotic maps are indispensable parts in any PCNG designs. In other words, it is a common method to choose three chaotic maps to design PCNGs, and thus, roughly speaking, these PCNGs cost equivalent execution time. Thus, the remaining components of a PCNG determine its computational performance. In our PCNG scheme, except for the chaotic maps, only four basic and low-cost XOR operators and a simple and easily implemented dynamic output control mechanism are used. They can enhance the complexity of PCNG effectively but not spend lots of time. Hence, the proposed PCNG scheme is considered to be efficient.

Furthermore, the proposed PCNG operates in 32-bit, while most of the PCNGs in literature use double precision notation which is in 64-bit. Thus, our PCNG occupies reduced resources and are more hardware efficient for computation, which is also beneficial to achieving a good computational performance.

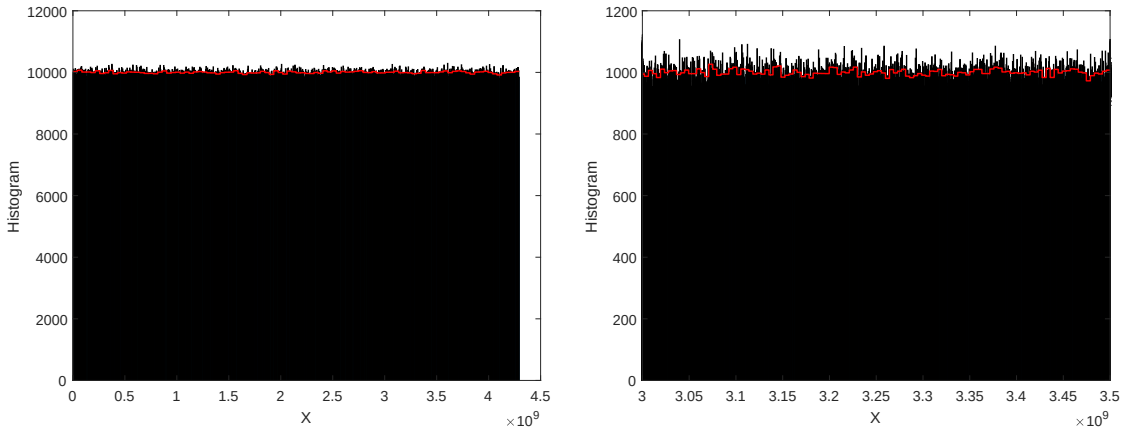
Statistical analysis

The PCNG is responsible for providing key stream for the stream cipher. The key stream must exhibit randomness to ensure that the attackers cannot find the rule of the key stream and never be able to derive the secret key. Thus, firstly, the basic rule of PCNG in statistical analysis is that the generated chaotic sequences should have a uniform distribution. And, then the chaotic sequences should pass the randomness test.

(1) Histogram and χ^2 test

As can be seen from Figure 4.2(a), the generated chaotic sequence is uniformly distributed by its histogram, where 10^7 chaotic samples X have been plotted in 1000 statistical

classes and the red curve in the figure shows the average values in every 10 classes (an interval). When we zoom in a part of Figure 4.2(a), for instance, the range of $[3\times10^9, 3.5\times10^9]$, and then plot its histogram in Figure 4.2(b), we can find that the partial histogram is qualitatively similar to the whole histogram of Figure 4.2(a). Note that, in Figure 4.2(b), to reveal the partial histogram more clearly, we divide each class of Figure 4.2(a) into 10 classes, which is equivalent to the original sequence in Figure 4.2(a) being drawn in the histogram of 10000 classes, and then a part of it has been magnified.



(a) Histogram (b) Enlarged histogram

FIGURE 4.2 – Histogram of the produced key stream

Furthermore, to verify whether the output variable X follows the uniform law, we evaluate the probability density as follows.

Suppose there is a sequence (x) with a large number of values $x(1), x(2), ..., x(i), ..., x(n)$ taken by a given variable X. An approximate representation of the distribution law that X follows can be obtained by a histogram of the sequence x in 10 classes. For this, using MATLAB, we execute the following operations :

(a) using function "$[nelements, centers] = hist(X)$" to determine the $centers$ of the classes obtained by diving the interval $[min(x), max(x)]$ into a given number of classes, for instance, 10 classes, with the same length (l), where the notation $min(x)$ and $max(x)$ mean the minimal value or the maximal value of the sequence x and $l = \frac{max(x)-min(x)}{10}$, and the number of elements ($nelements$) in each class.

(b) the heights ($heights$) of the rectangles of the histogram are obtained by

$$heights = (nelements/n)/l.$$

(c) the histogram can be drawn by the function $bar(centers, heights)$.

The areas of the rectangles of the histogram give the approximations of the probability $P(X \in I)$, where I is one of the classes. The heights of the rectangles mean the approximations of the probability density law followed by the variable X.

If the variable X follows the uniform law, i.e. $U(min(X), max(X)) = U(1, 2^{32} - 1)$, the probability density should be $\frac{1}{max(X)-min(X)} = \frac{1}{2^{32}-2} \approx 2.3283 \times 10^{-10}$, so the heights should be 2.3283×10^{-10}.

After applying the operations described above on the produced key stream, the approximation of the probability density of the output variable X has been shown in Figure 4.3, which has confirmed that the produced key stream follows the uniform law.

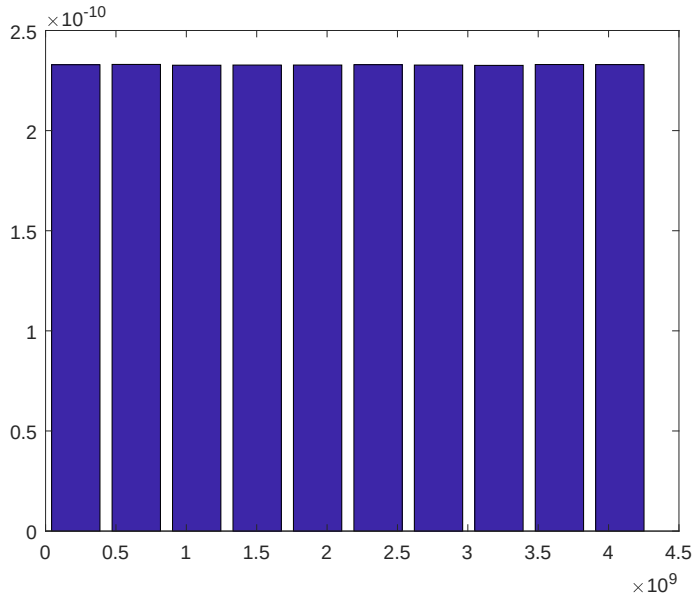


FIGURE 4.3 – The approximation of the probability density of the key stream X

In addition, χ^2 test has been used to assert its uniformity more precisely. The experimental value of χ^2 test is calculated as below :

$$\chi^2_{exp} = \sum_{i=0}^{N_c-1} \frac{(O_i - E_i)^2}{E_i} \tag{4.4}$$

where N_c is the number of classes chosen (here $N_c = 1000$), O_i is the number of observed samples in the $i - th$ class and E_i is the expected number of samples in a uniform distribution. Here, we generate 3125000 chaotic samples, hence $E_i = 3125000/1000$. The

experimental value χ^2_{exp} equals to 961.0874 which is smaller than the theoretical value $\chi^2_{th}(N_c - 1, \alpha) = 1073.6427$ obtained for a threshold $\alpha = 0.05$ of χ^2 distribution. This has confirmed the uniformity of the generated chaotic sequence.

(2) Uniformity test in binary level

In addition, the calculation of the number of bit 0 and bit 1 in the binary conversion of the output sequence X provides the binary perspective to analyze its randomness. Convert the sequence X from decimal integers to binary elements first, then separate it into 100 bit streams. So, each bit stream contains $3125000 \times 32/100 = 10^6$ bits. After that, we calculate the number of 0 and 1 in each bit stream. The result shown in Figure 4.4 has indicated that the proportions of bit 0 and bit 1 are symmetrically distributed around the optimal value 50%. Meanwhile, the mean value of 100 proportions of bit 0 and bit 1 among all bit streams are 49.993% and 50.007% respectively.

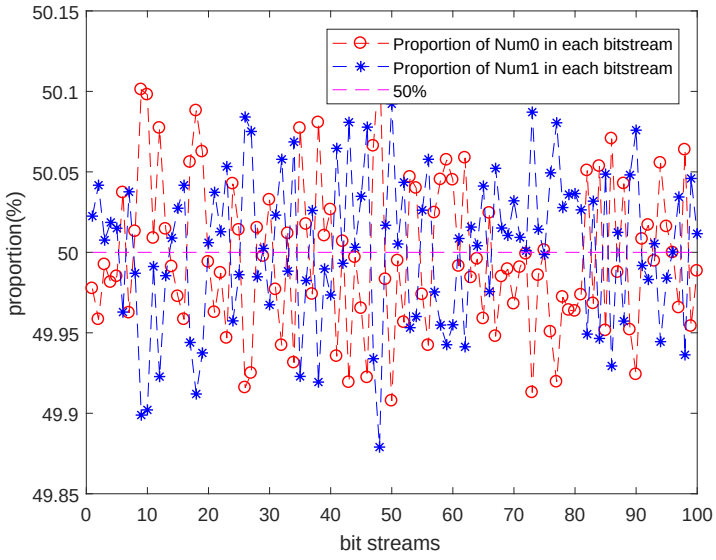


FIGURE 4.4 – Proportion of bit 0 and 1 in binary bit stream

Hence, the proposed PCNG can pass the statistical analysis not only in decimal level, but also in binary level. It shows highly similar properties with random numbers.

This test corresponds to the first test in NIST randomness test. Applying the following NIST test depends on the passing of this test.

(3) NIST test

NIST (National Institute of Standard and Technology) test suite is a standard to assess randomness of sequences. It contains 15 independent statistical tests for revealing various

deviations from random behavior [115].

In the NIST test results report, P-value greater than a predefined significance level α means the sequence pass the test. P-value is equal to 1 meaning the sequence has a perfect randomness, and it is equal to 0 meaning the test sequence is completely non-random. In the NIST standard, $\alpha = 0.01$ is suggested. P-value$\geqslant 0.01$ means the sequence would be considered to be random with a confidence of 99%. Otherwise, the sequence is non-random with a confidence of 99%.

The range of accepted proportion is determined using the confidence interval defined as follows :

$$\widehat{p} \pm 3\sqrt{\frac{\widehat{p}\,(1-\widehat{p})}{n}}$$

where $\widehat{p} = 1 - \alpha$ and n is the sample size (the number of tested sub-sequences) [115].

Here, we apply the NIST test on the produced sequence (3125000×32bits$= 100$ sub-sequences $\times 10^6$ bits), that is $n = 100$. Thus, proportions should be in the acceptable interval $[96.00\%, 102.00\%]$.

The results in Table 4.2 have demonstrated that the chaotic sequence has passed the NIST test successfully.

TABLE 4.2 – P-value and Proportion results of NIST test

Test	P-value	Proportion(%)	Result
Frequency	0.936	100.000	Pass
Block-frequency	0.817	99.000	Pass
Cumulative-sums	0.117	99.500	Pass
Runs	0.350	99.000	Pass
Longest-run	0.163	97.000	Pass
Rank	0.475	100.000	Pass
FFT	0.554	99.000	Pass
Non-overlapping template	0.511	98.845	Pass
Overlapping template	0.637	99.000	Pass
Universal	0.335	98.000	Pass
Approximate entropy	0.063	99.000	Pass
Random-excursions	0.411	98.790	Pass
Random-excursions-variant	0.371	99.283	Pass
Serial	0.232	99.000	Pass
Linear-complexity	0.740	100.000	Pass

4.3.2 Security analysis of the proposed stream cipher

Key space analysis

A large secret key space of a cryptosystem is necessary to resist the brute-force attack and it is considered to be secure if the key space is equal or greater than 2^{128} [7].

The secret key of this stream cipher depends on the input values of the proposed PCNG which contains first the initial conditions for the three chaotic maps : $Xp(0)$, $Xs(0)$, $Xl(0)$ and then the control parameters Pp and Ps for PWLCM and skew tent map. Thus, the key size is :

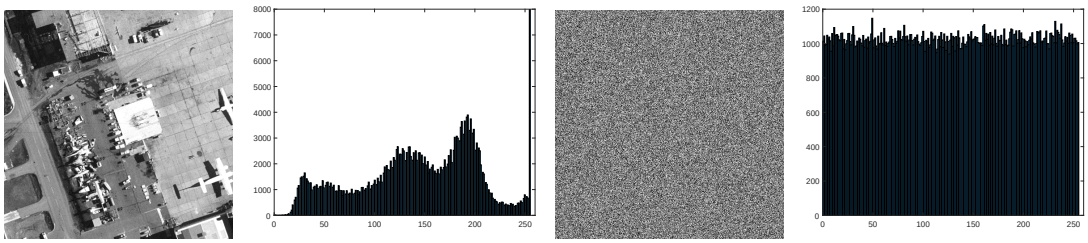
$$|K| = |Xp\,(0)| + |Xs\,(0)| + |Xl\,(0)| + |Pp| + |Ps| = 159 \;\; bits$$

where $|Xp\,(0)| = |Xs\,(0)| = |Xl\,(0)| = |Ps| = 32$ bits, $|Pp| = 31$ bits.

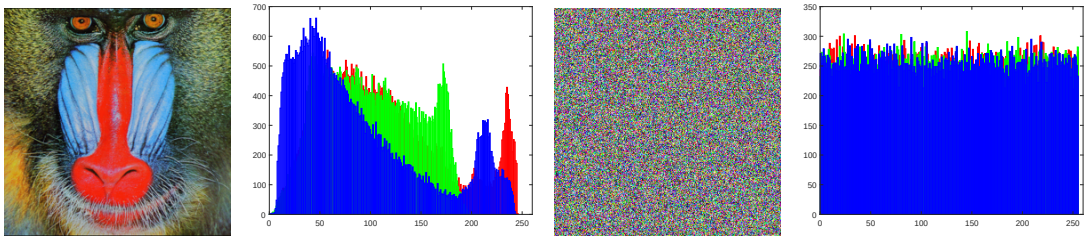
Therefore, the key space of the proposed stream cipher is 2^{159}, which is large enough to resist the brute-force attack.

Histogram and χ^2 test

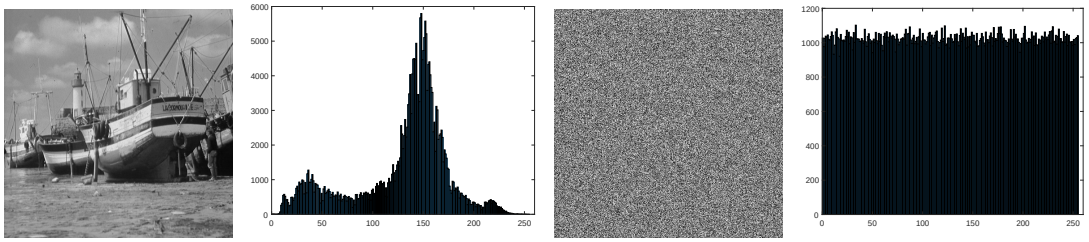
We tested 5 images (Airfield, Baboon, Boat, Lena, Pepper) with different sizes and features (the sizes of images can be found in Table 4.3). The ciphered images should be uniformly distributed to resist the statistical attack. We analyze the distribution of plain and ciphered image in Figure 4.5, where the plain images are shown in Figure 4.5(a), 4.5(e), 4.5(i), 4.5(m), 4.5(q) and their corresponding histograms in gray or RGB color plane are displayed in Figure 4.5(b), 4.5(f), 4.5(j), 4.5(n), 4.5(r). Their ciphered images (Figure 4.5(c), 4.5(g), 4.5(k), 4.5(o), 4.5(s)) are uniformly distributed in every color plane, which are shown in Figure 4.5(d), 4.5(h), 4.5(l), 4.5(p), 4.5(t).



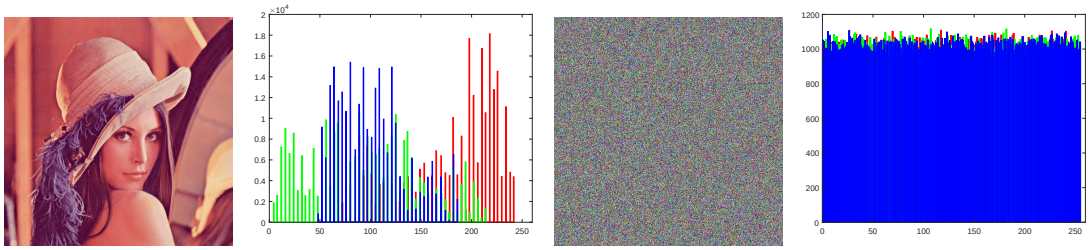
(a) Airfield (b) Histogram (c) Ciphered image (d) Histogram of ciphered image



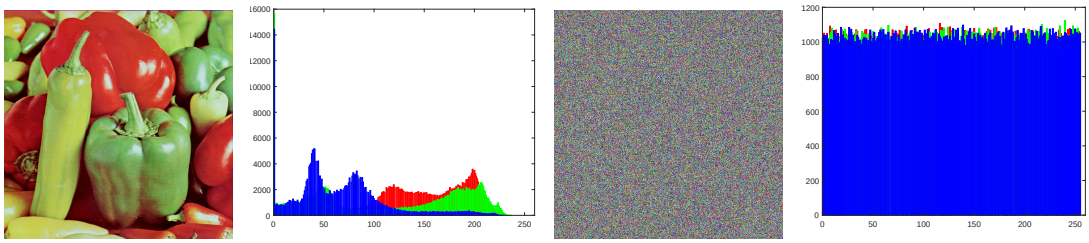
(e) Baboon (f) Histogram (g) Ciphered image (h) Histogram of ciphered image



(i) Boat (j) Histogram (k) Ciphered image (l) Histogram of ciphered image



(m) Lena (n) Histogram (o) Ciphered image (p) Histogram of ciphered image



(q) Pepper (r) Histogram (s) Ciphered image (t) Histogram of ciphered image

FIGURE 4.5 – Plain and ciphered images and their histograms

In addition, the χ^2 test is applied using (4.4) to assert the uniformity of the ciphered

images but with different parameters : $Nc = 256$, $E_i = imagesize/Nc$, $\alpha = 0.05$, which give the theoretical value $\chi^2_{th}(255, 0.05) = 293.2478$. For each image, 100 different secret keys have been applied to repeat this test. Table 4.3 has displayed the average experimental χ^2_{exp} test results, which are all smaller than $\chi^2_{th}(255, 0.05)$, and thus the results have confirmed the uniformity of the ciphered images.

TABLE 4.3 – Results of the χ^2 test and entropy test

Image	Size	χ^2_{exp}	Entropy :H(P)	Entropy :H(C)
Airfield	$512 \times 512 \times 1$	255.7314	7.1206	7.9993
Baboon	$256 \times 256 \times 3$	258.1894	7.7073	7.9991
Boat	$512 \times 512 \times 1$	255.0322	7.1914	7.9993
Lena	$512 \times 512 \times 3$	256.0950	5.6822	7.9998
Pepper	$512 \times 512 \times 3$	252.3005	7.6698	7.9998

Entropy test

The information entropy is used to evaluate uncertainty and randomness properties in a message. The image pixel values are in the range of $[0, 255]$. In a robust cipher algorithm, the occurrence probability of any pixel value should be the same or almost the same. The random behavior of the ciphered image can be evaluated using the information entropy given by :

$$H(C) = \sum_{i=0}^{Q-1} Pro(c_i) \times log_2 \frac{1}{Pro(c_i)} \tag{4.5}$$

where $H(C)$ is the entropy of the ciphered image C, $Pro(c_i)$ is the occurrence number of c_i in each level (i=0,1,2...255), and $Q = 256 = 2^8$ is the number of levels.

Therefore, ideally, each level should have equal occurrence probability $Pro(c_i) = 1/Q = 2^{-8}$. In this case, the information entropy is maximal :

$$H_{ideal}(C) = \sum_{i=0}^{255} 2^{-8} \times log_2 256 = 8.$$

We have calculated the information entropy for each plain image ($H(P)$) and the average entropy for the ciphered image ($H(C)$) over 100 entropy results accomplished by 100 secret keys. From the obtained results shown in Table 4.3, we remark that all average information entropy of the ciphered images is close to the above mentioned optimal value.

Correlation analysis

Image has an intrinsic feature that is the high correlation between pixels. A secure cryptosystem should break this relationship. To test the correlation between two adjacent pixel, 8000 pairs of adjacent pixels have been selected randomly in horizontal (H), vertical (V) and diagonal (D) directions respectively from the plain image and its corresponding ciphered image. Then the correlation coefficient (ρ_{xy}) of each pair is calculated by Equation (4.6).

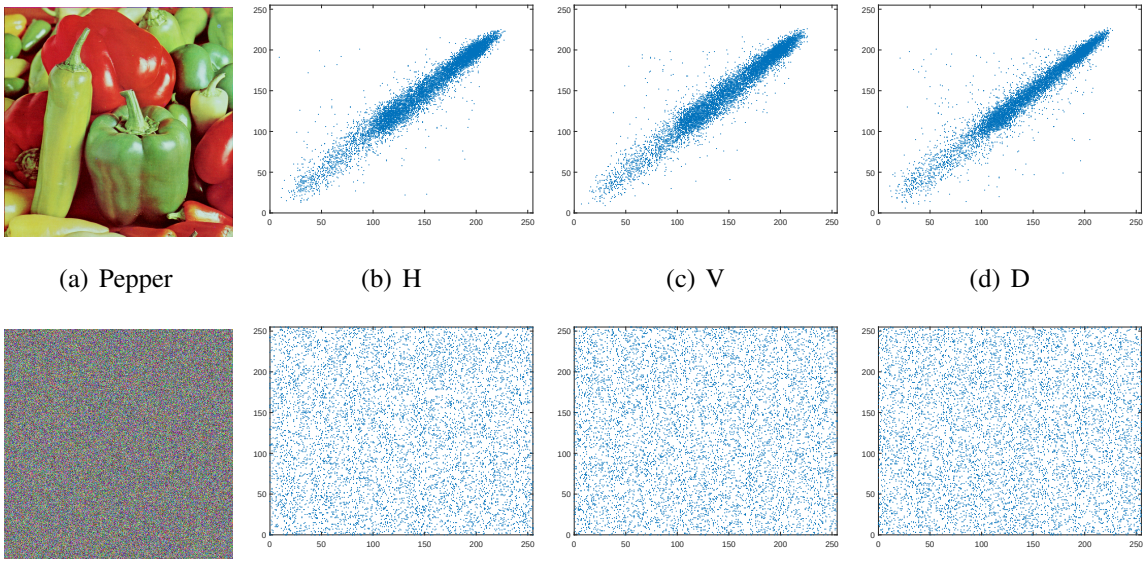
$$\rho_{xy} = \frac{\sum_{i=1}^{Np} \left[(x_i - \overline{x}) \, (y_i - \overline{y}) \right]}{\sqrt{\sum_{i=1}^{Np} (x_i - \overline{x})^2} \sqrt{\sum_{i=1}^{Np} (y_i - \overline{y})^2}} \tag{4.6}$$

where $N_p = 8000$ is the number of the randomly selected pairs of adjacent pixels ; x_i, y_i are pixel values of $i - th$ pair, and $\overline{x}$, $\overline{y}$ are the mathematical expectations.

Correlation coefficients ρ_{xy} of each plain image have been calculated in each direction (H, V, D). For each test image, 100 different secret keys are created to encrypt the plain image into 100 ciphered images, and then we calculate the correlation coefficients in each ciphered image and find the average value to represent the correlation coefficient of ciphered image. Table 4.6 has shown the results obtained in each direction H, V, D in plain and ciphered images. In addition, Figure 4.6 gives the correlation diagram of image $Pepper$ in H, V, D directions of the plain and ciphered images separately. Table 4.4 and Figure 4.6 have revealed that the adjacent pixels are highly correlated to each other in the plain image and the stream cipher can break this correlation effectively.

TABLE 4.4 – Correlation coefficient results

Image	Plain image			Ciphered image		
	H	V	D	H	V	D
Airfield	0.9396	0.9422	0.9052	0.0041	-0.0029	0.0032
Baboon	0.9540	0.9348	0.9177	-0.0020	-0.0028	0.0013
Boat	0.9384	0.9711	0.9215	-0.0005	-0.0036	0.0010
Lena	0.9753	0.9854	0.9648	0.0009	0.0013	0.0026
Pepper	0.9622	0.9654	0.9542	0.0033	0.0008	-0.0001



(a) Pepper (b) H (c) V (d) D

(e) Ciphered image (f) H (g) V (h) D

FIGURE 4.6 – Correlation between adjacent pixels of $Pepper$ in horizontal (H), vertical (V) and diagonal (D) directions in plain and ciphered image

Key sensitivity analysis

A robust stream cipher should have high sensitivity to the secret key. This property can be measured by calculating the Hamming distance (D_H) (4.7) between two ciphered images $C1$ and $C2$ which have been encrypted from the similar plain images but their secret keys are only one bit different from each other.

$$D_H\left(C_1, C_2\right) = \frac{1}{|lb|} \times \sum_{k=1}^{|lb|} \left(C_1\left[k\right] \oplus C_2\left[k\right]\right) \tag{4.7}$$

where $|lb|$ is the bit length of the image under processing.

For each test image, C_1, C_2 are encrypted by one bit different (the position of the different bit is randomly selected) secret keys. 100 different secret keys are used to repeat this experiment and the average D_H over 100 D_Hs are shown in Table 4.5. As we can see, the obtained D_Hs are close to the optimal value 50% indicating that the probability of bit changes between each pairs of ciphered images is 50%.

We also adopted two common methods to measure the cryptosystem's sensitivity to the secret key : the number of pixels change rate (NPCR) and the unified average changing

intensity (UACI), which are defined by Equation (4.8), (4.9).

$$\begin{aligned} NPCR &= \frac{1}{M_1 \times M_2 \times M_3} \times \sum_{u=1}^{M_1} \sum_{v=1}^{M_2} \sum_{w=1}^{M_3} D\left[u,v,w\right] \times 100\% \\ D\left[u,v,w\right] &= \begin{cases} 0, \ if \ C_1\left[u,v,w\right] = C_2\left[u,v,w\right] \\ 1, \ if \ C_1\left[u,v,w\right] \neq C_2\left[u,v,w\right] \end{cases} \end{aligned} \tag{4.8}$$

$$UACI = \frac{1}{M_1 \times M_2 \times M_3 \times 255} \times \sum_{u=1}^{M_1} \sum_{v=1}^{M_2} \sum_{w=1}^{M_3} |C_1 - C_2| \times 100\% \tag{4.9}$$

where C_1 and C_2 are the same as defined in Equation (4.7). The test image size is $M_1 \times M_2 \times M_3$. u, v, w indicate the pixel $C_1[u,v,w]$ or $C_2[u,v,w]$ is at the position of $u-th$ row, $v-th$ column and $w-th$ plane.

The average results of NPCR and UACI over 100 different secret keys given in Table 4.5 are close to the optimal values of NPCR and UACI that are 99.6094% and 33.4635% respectively, which has demonstrated that the cryptosystem is sensitive to its secret key.

TABLE 4.5 – Hamming distance and NPCR/UACI results

Image	$D_H(\%)$	NPCR(%)	UACI(%)
Airfield	49.9902	99.5983	33.4537
Baboon	49.9902	99.5976	33.4505
Boat	49.9902	99.5983	33.4335
Lena	49.9939	99.5981	33.4599
Pepper	49.9939	99.5981	33.4666

4.4 Conclusion

In this chapter, we developed, implemented and evaluated a novel efficient stream cipher based on a new proposed secure PCNG. The PCNG is built on three discrete chaotic maps, namely, PWLCM, skew tent map and logistic map, using XOR operators and a dynamic output control mechanism. The XOR operators and the dynamic output control mechanism can increase the complexity and enhance the randomness of the PCNG effectively. The proposed PCNG works over a 32-bit finite integer field which uses reduced hardware resources and can operate more efficiently with high reliability when compared to the PCNGs defined using 64-bit double precision real numbers.

The obtained experimental results have proven that the PCNG can generate chaotic numbers with excellent randomness characteristics. The stream cipher based on this PCNG has shown very good cryptographic properties. The proposed PCNG can be used not only in any design of new stream ciphers, block ciphers or other cryptosystems, but also in any other pseudo-random generator required applications.

Notice that, our proposed stream cipher is based on the combination of three different chaotic maps. Besides, we have also tested other combinations but they could not pass the statistical tests. For instance, if the PCNG is based on three skew tent maps (different initial conditions and parameters), even if the skew tent map has the best uniformity distribution, longest period, and largest key space among all the maps that we have analyzed in Chapter 3, the produced key stream shows special patterns in the phase space, which means the relation between $X(n) - X(n+1)$ (X means the key stream) is not completely concealed. Also, this combination cannot pass the NIST test ("block frequency test", i.e, numbers of bit 0 and bit 1 are not equal in test block in the NIST test). If the PCNG uses two skew tent maps and one PWLCM, the produced key stream shows the similar problems when three skew tent maps are adopted. If the PCNG is based on three logistic maps, its key space is too small (2^{96}) and the produced key stream is not uniformly distributed. Since the adopted discrete chaotic maps have their own shortcomings, such as short period, non-uniformity, the specific relation between $x(n) - x(n+1)$ (x denotes the original chaotic sequence), etc, if the same maps are used in the PCNG, they exhibit similar dynamics and show correlation between each other, and their own shortcomings cannot be greatly overcome by chaotic dynamics generated by other maps. Hence, using same maps are strongly not recommended. The proposed PCNG has chosen the most appropriate combination among the four reformulated chaotic maps in Chapter 3.

CHAPITRE 5

PROPOSED SECURE AND ROBUST CHAOS-BASED IMAGE CRYPTOSYSTEM

5.1 Introduction

In this chapter, we design, realize and evaluate a new secure cryptosystem based on a new proposed PCNG, a global diffusion and a block cipher in cipher block chaining(CBC) mode. The proposed PCNG, defined over a finite field, is based on the discrete Chebyshev 3rd order chaotic map (Equation (3.4)) coupled with a pseudo-random number generator (PRNG) and a discrete skew tent map (Equation (3.2)). It can remove a hidden danger of deteriorated security caused by the dynamical degradation encountered in numerical implementation of chaotic maps defined on real numbers. The global diffusion uses a horizontal addition diffusion (HAD) and a vertical addition diffusion (VAD) followed by a modified 2D cat map. The block cipher in CBC mode is based on a confusion layer using the AES S-Box, followed by a diffusion layer built on the modified 2D cat map and a key addition operation. The global diffusion enhances the diffusion process of the block cipher.

In the following sections, Section 5.2 describes the proposed cryptosystem, and the performance analyses are given in Section 5.3. Finally, we draw the conclusion in Section 5.4.

5.2 Proposed cryptosystem scheme

5.2.1 Encryption process

The encryption process of the proposed chaos-based cryptosystem is shown in Figure 5.1. The new proposed PCNG, controlled by the secret key, provides pseudo-chaotic samples as the key stream for the encryption process that contains a global diffusion operation and a block cipher.

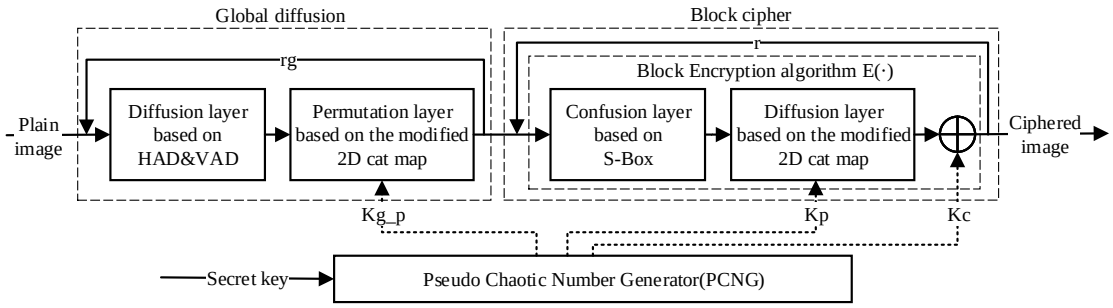


FIGURE 5.1 – Encryption process

The global diffusion is carried out to enhance the diffusion properties. Firstly, the whole input plain image is processed by the global diffusion operation which includes a diffusion layer based on a horizontal addition diffusion (HAD) followed by a vertical addition diffusion (VAD) and a permutation layer based on a modified 2D cat map. In this process, the parameters (K_{g_p}) required by the modified 2D cat map are provided by the PCNG. The global diffusion can be repeated rg times. After that, the output image of global diffusion is split into blocks with 16 bytes (4×4 bytes) size per block. Then, the block cipher in CBC mode is applied to each block consecutively. The kernel of the block cipher is the block encryption algorithm E(.) which contains a confusion layer based on the AES (Advanced Encryption Standard) S-Box [163], a diffusion layer based on a modified 2D cat map and a key addition operation (XOR). The parameters (K_p, K_c) required by the modified 2D cat map and XOR operator are fed by the PCNG. The block cipher operation can be repeated r times to obtain the final ciphered image.

5.2.2 Proposed PCNG

The new proposed PCNG is described in Figure 5.2. It produces the required pseudo-chaotic samples, i.e. key stream, for confusion-diffusion process and it works in a fixed finite precision of N bits $(N = 32)$. It consists of two discrete chaotic maps, i.e. the Chebyshev 3rd order chaotic map Fc and the skew tent map Fs, and a Pseudo-Random Number Generator (PRNG) which is used to expand the period of Fc and enhance its uniformity. The PRNG uses a parameter "Seed" to control the produced numbers.

Recalling the equations of Chebyshev 3rd order chaotic map (Fc) defined by Equation (3.4) and the skew tent map (Fs) defined by Equation (3.2) in Chapter 3, the secret key in

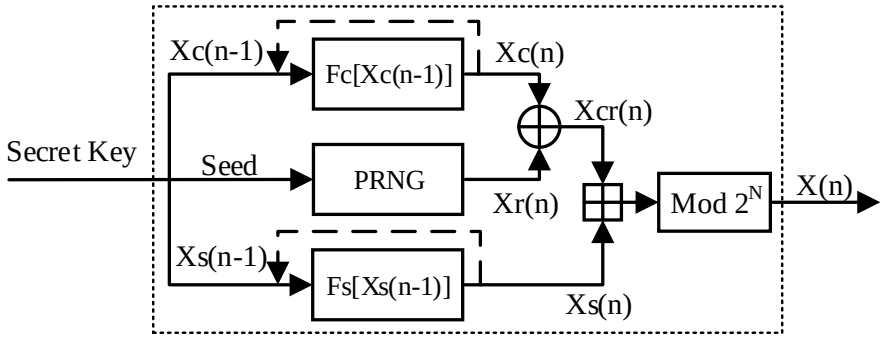


FIGURE 5.2 – Pseudo-chaotic number generator (PCNG)

Figure 5.2 is formed by two initial values of Fc and Fs : $Xc(0)$ and $Xs(0)$, and two control parameters : P and $Seed$. Note that the first 100 iterations of the PCNG are discarded to reach randomness.

Hence, the key size ($|K|$) is $|K| = |Xc(0)| + |Xs(0)| + |P| + |Seed| = 128$ bits with $|Xc(0)| = |Xs(0)| = 32$, $|P| = 32$ and $|Seed| = 32$. Therefore, the key space is 2^{128}, which is large enough to make brute-force attack infeasible.

5.2.3 Global diffusion

Global diffusion works on the whole image aiming at enhancing the diffusion properties of the cryptosystem. In this section, firstly, we will describe the diffusion layer based on the HAD and VAD, and secondly, we will present the permutation layer based on the modified 2D cat map.

Diffusion layer based on HAD and VAD

The diffusion layer, introduced by Tasnime O. et al. [164], operates on a horizontal addition diffusion (HAD) followed by a vertical addition diffusion (VAD). The HAD and VAD operations are described by Figure 5.3 and Equations (5.1) and (5.2). In these equations, I represents the input plain image of size $S_r \times S_c$ (S_r : number of rows, S_c : number of column) and L is the bits number of a pixel.

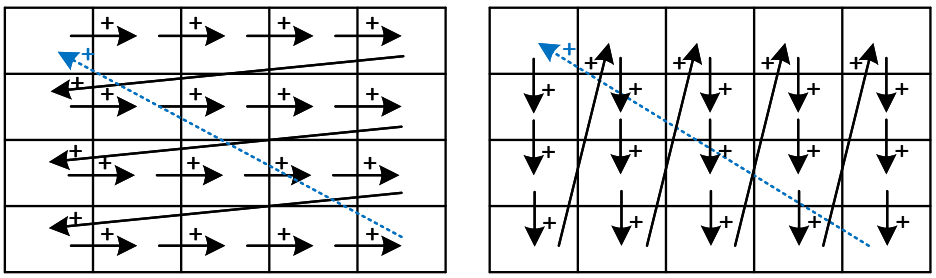


FIGURE 5.3 – Horizontal addition diffusion (HAD) and vertical addition diffusion (VAD)

$$HAD\left[I\left(i,j\right)\right]=\begin{cases} I\left(i,j\right)+I\left(i,j-1\right)\ mod\ 2^{L} & \text{for } 1\leq i\leq S_r \text{ and } 2\leq j\leq S_c \\ I\left(i,j\right)+I\left(i-1,S_c\right)\ mod\ 2^{L} & \text{for } 2\leq i\leq S_r \text{ and } j=1 \\ I\left(i,j\right)+I\left(S_r,S_c\right)\ mod\ 2^{L} & \text{for } i=j=1 \end{cases} \tag{5.1}$$

$$VAD\left[I\left(i,j\right)\right]=\begin{cases} I\left(i,j\right)+I\left(i-1,j\right)\ mod\ 2^{L} & \text{for } 2\leq i\leq S_r \text{ and } 1\leq j\leq S_c \\ I\left(i,j\right)+I\left(S_r,j-1\right)\ mod\ 2^{L} & \text{for } i=1 \text{ and } 2\leq j\leq S_c \\ I\left(i,j\right)+I\left(S_r,S_c\right)\ mod\ 2^{L} & \text{for } i=j=1 \end{cases} \tag{5.2}$$

Notice that if the image to be processed has three color planes, such as an RGB color image, three planes are laid out from left to right horizontally as a matrix described by Figure 5.4 and this matrix is processed by HAD and VAD. This operation will enhance the diffusion property among the different color planes.

Permutation layer based on the modified 2D cat map

The permutation layer is based on a modified 2D cat map, which rearranges the pixels' positions on the image processed after HAD and VAD. The applied modified 2D cat map is derived from the Arnold's cat map and it is defined by the following equations [44] :

$$\begin{bmatrix} x_{new} \\ y_{new} \end{bmatrix} = \mathrm{mod}\left(\mathbf{A}_0 \times \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} rl+rc \\ rc \end{bmatrix}, \begin{bmatrix} M \\ M \end{bmatrix}\right) + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{5.3}$$

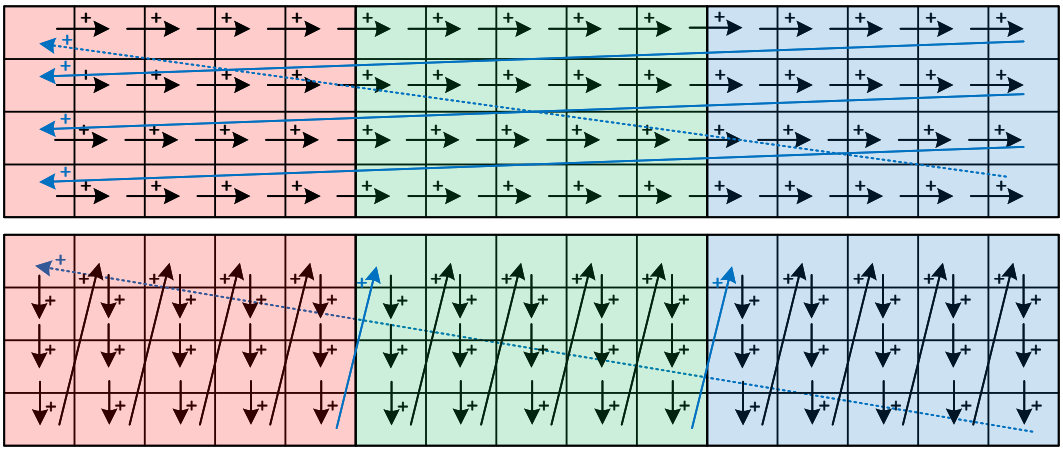


FIGURE 5.4 – HAD and VAD for processing an image with three color planes

The cat map matrix $\mathbf{A}_0$ is defined as :

$$\mathbf{A}_0 = \begin{bmatrix} 1 & u \\ v & 1 + u \times v \end{bmatrix} \tag{5.4}$$

The determinant of $\mathbf{A}_0$ is 1, indicating each original position (x, y) in the image of size $M \times M$ is permuted to another position (x_{new}, y_{new}) uniquely. The parameters u,v,rl and rc, in the range of $[0, M-1]$, form the dynamic key (K_{g_p}). rl,rc are added to overcome the fixed-point problem of Arnold's cat map. $[\ 1 \quad 1\ ]^T$ is to ensure the subscript indices in MATLAB implementation start from 1.

Now, to speed up the calculus, Equation (5.3) is written as follows [44] :

$$\begin{aligned} \mathbf{Mr}_{new} &= mod(\mathbf{Mr} + u \times \mathbf{Mc} + \mathbf{Rl} + \mathbf{Rc}, M) + \mathbf{J}_M \\ \mathbf{Mc}_{new} &= mod(v \times \mathbf{Mc} + (1 + u \times v) \times \mathbf{Mc} + \mathbf{Rc}, M) + \mathbf{J}_M \end{aligned} \tag{5.5}$$

where $\mathbf{Mr}_{new}$, $\mathbf{Mc}_{new}$ are the new row and column indices of permuted pixel positions while **Mr** and **Mc** are the original row and column indices with the following form :

$$\mathbf{Mr} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2 & \cdots & 2 \\ \vdots & \vdots & \ddots & \vdots \\ M & M & \cdots & M \end{bmatrix}; \mathbf{Mc} = \begin{bmatrix} 1 & 2 & \cdots & M \\ 1 & 2 & \cdots & M \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & \cdots & M \end{bmatrix} \tag{5.6}$$

$\mathbf{J}_M$ is a square matrix of size $M \times M$ and its elements are all 1 ; **Rl** $= rl \times \mathbf{J}_M$, **Rc** $= rc \times \mathbf{J}_M$.

The dynamic parameters u,v,rl,rc are fed by the PCNG and their values change for each encryption round. We consider here one sample by parameter, thus, for rg rounds, the global diffusion needs $4 \times rg$ PCNG samples in total.

In order to determine the optimal value of rg, we measure the diffusion performance by calculating Hamming distance (D_H) between two ciphered images (C_1, C_2) which have been encrypted from two plain images (I_1, I_2) that are just the LSB (Least Significant Bit) different.

$$D_H(C_1, C_2) = \frac{1}{|lb|} \sum_{k=1}^{|lb|} \left(C_1\left[k\right] \oplus C_2\left[k\right]\right) \tag{5.7}$$

where $|lb|$ is the bit length of the image : $|lb| = M \times M \times Plane \times L$. "$Plane$" is the number of color planes of an image (for a gray image, $Plane = 1$; for an RGB color image, $Plane = 3$).

We have tested 8 gray and color images with different sizes and features as shown in Figure 5.5. For each plain image (I_1), 24 altered pixel positions are selected in the similar manner as in the work done by Tasnime O. et al. [164] to change the LSB (I_2). After rg rounds of global diffusion, 24 pairs of C_1 and C_2 are obtained. Then, 24 D_Hs have been calculated by Equation (5.7) and the average D_Hs for each image versus rg have been given in Figure 5.6 and Table 5.1. We observe that, for $rg \geq 2$, D_H is very close to 50% (the probability of a bit change) which is the optimal value meaning the best diffusion level for one bit change in the plain image.

(a) Airfield (b) Baboon (c) Boat (d) Goldhill (e) Lena (f) Pepper (g) White (h) Black

FIGURE 5.5 – Eight test images with different sizes and features

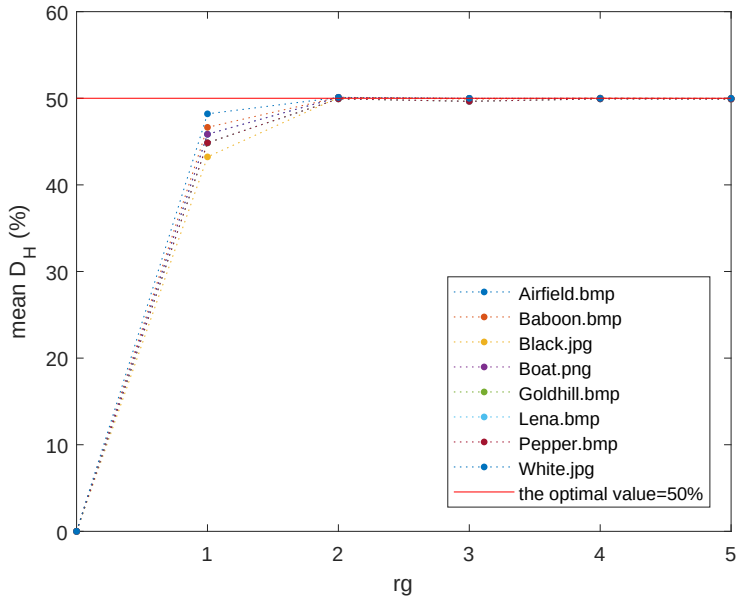


FIGURE 5.6 – Mean D_H versus the round times rg in global diffusion$(\%)$

TABLE 5.1 – D_H versus the round times rg in global diffusion$(\%)$

Image	Size	rg=1	2	3	4	5
Airfield	$512 \times 512 \times 1$	45.8481	50.1021	49.9879	49.9999	49.9902
Baboon	$256 \times 256 \times 3$	46.6437	50.1096	49.9041	50.0074	49.9766
Boat	$512 \times 512 \times 1$	45.8429	50.1051	49.9842	49.9996	49.9768
Goldhill	$512 \times 512 \times 3$	44.8466	49.9274	49.6480	49.9336	49.8998
Lena	$512 \times 512 \times 3$	44.8565	49.9304	49.6417	49.9277	49.9010
Pepper	$512 \times 512 \times 3$	44.8582	49.9305	49.6470	49.9280	49.8978
White	$512 \times 512 \times 1$	48.2026	50.0967	49.9925	49.9854	49.9853
Black	$512 \times 512 \times 1$	43.2300	50.0813	49.9846	50.0007	49.9924

5.2.4 Block cipher

After the global diffusion, the diffused image is split into blocks of size 4×4 bytes each. And each block is processed by the block encryption algorithm $E(.)$ in CBC mode as shown in Figure 5.7(a). The ciphering process can be repeated r times to obtain the best security performances.

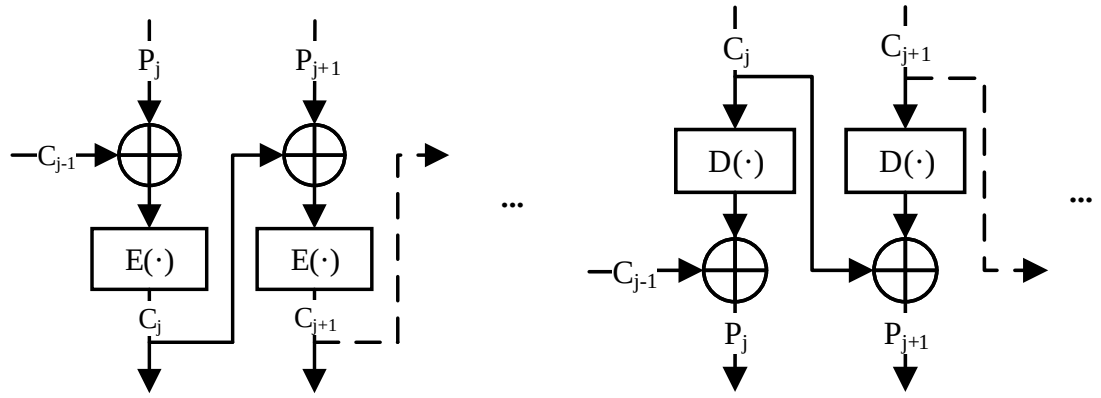
In terms of the CBC mode, P_j,C_j are the $j-th$ input plain block and its corresponding output ciphered block. In the encryption process shown in Figure 5.7(a), it operates as follows,

$$C_j = E(P_j \oplus C_{j-1})$$

which means, C_j is formed by applying encryption algorithm $E(\cdot)$ on the result of an XOR operation between P_j and its former ciphered block C_{j-1}, where $j = 1, 2..., N_b$, and N_b is the number of blocks of the processed image. If $r = 1$, after N_b plain blocks have been successively processed by $E(\cdot)$ in CBC mode, all C_j ($j = 1, 2, ..., N_b$) blocks constitute the final ciphered images. If $r = 2$, C_j ($j = 1, 2, ..., N_b$) is regarded as the plain block P_j and repeat the CBC mode for the second round. Similar working mode when $r = 3, 4, ...$ It should be noticed that, for the first block, when $r = 1$, $C_0 = IV$, where IV (Initialization Vector) is a predefined pseudo-random sequence in the length of 16 bytes. The decryption process of CBC mode is shown in Figure 5.7(b). Each plain block can be recovered by

$$P_j = C_{j-1} \oplus D(C_j)$$

where the decryption algorithm $D(\cdot)$ is the reverse of the encryption process $E(\cdot)$.



(a) encryption process (b) decryption process

FIGURE 5.7 – CBC mode

In $E(\cdot)$, the first component is AES S-Box, the "SubBytes" step in the AES encryption algorithm, which consists of two mathematical transformations : a multiplicative inverse g

in the Finite Galois Field **GF**(2^8) and an invertible affine transformation f [163]. It is a byte nonlinear transformation : $S(p\_old) = f(g(p\_old)) : p\_old \rightarrow p\_new$, by which each old byte p_old can be replaced by a new substitution byte p_new. In our program, we apply the functions g and f to each number in the range of $[0x00, 0xff]$ to obtain the S-box mapping (S) between each value in $[0x00, 0xff]$. So, in our block cipher, each input pixel p_old of the S-box can be easily and immediately transformed to its corresponding output pixel p_new by the S-box mapping.

Then, the modified 2D cat map (Equation (5.5)) is used to permute the pixels' positions aiming to reinforce the diffusion effect. Here, each parameter u, v, rl, rc of the dynamic key K_p is in the range of $[0, 3]$ (2 bits for each parameter, 8 bits for K_p). Finally, XOR operator is applied between pixels of the output block from the modified 2D cat map and a dynamical key K_c to fulfill a masking task. K_p and K_c are fed by the PCNG and their values are changed for each block and for each round r. In one round, for each block, K_p needs 8 bits taking up $1/4$ of the PCNG sample ($X(n)$) and K_c requires 16 bytes taking up 4 PCNG samples, so each encrypted block needs $(1/4 + 4)$ PCNG samples. Thus, the block cipher requires in total $\lceil (1/4+4) \times r \times N_b \rceil$ PCNG samples, where N_b is the number of blocks of the processed image.

To sum up, in $E(\cdot)$, S-box and the modified 2D cat map changes and relocates all pixels and their positions in block. Besides, the application of XOR masking operator reinforces the confusion level, leading to almost no original input block information retained after $E(\cdot)$. Furthermore, each ciphered block is affected by its plain block and its former ciphered block, which makes that even the identical input plain blocks can be encrypted into different ciphered blocks. In this method, it is impossible for attackers to attempt block replay and to build a code book. Therefore, this architecture is expected to have excellent security performances.

5.2.5 Decryption process

The operations done in the decryption process are the inverse of those carried out in the encryption process as described in Figure 5.8. The only difference with the encryption process is that here we need to produce all the required PCNG samples before deciphering.

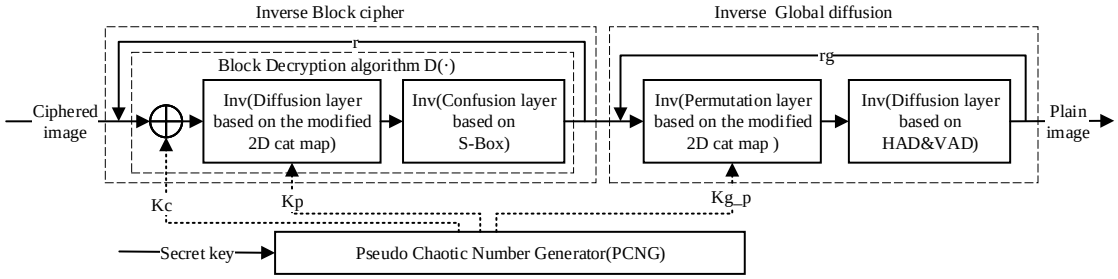


FIGURE 5.8 – Decryption process

5.3 Performance analysis

Hereafter, we quantify the performance of the proposed cryptosystem. First, we evaluate its performances against the statistical attacks, and then, we analyze its security from the perspectives of confusion and diffusion properties, the robustness and computation time performances. All the simulations have been implemented in MATLAB(2017b) on a standard computer of Intel Core i7-3770 CPU in Win 7, 64-bit operating system with 3.4 GHz processor 8GB RAM.

5.3.1 Statistical analysis of the PCNG

Histogram and χ^2 test

The generated pseudo-chaotic samples should have an uniform distribution. To test this feature, we have generated 3125000 PCNG samples and then the corresponding histogram (using 1000 classes) has been drawn in Figure 5.9, where the red curve shows the average values in every 10 classes. We can find that the PCNG produced sequence seems uniformly distributed in the definition region.

In addition, we have plotted the approximation of the probability density of the produced key stream in Figure 5.10 as we have done in "Section 4.3.1-Statistical analysis-(1) Histogram and χ^2 test", which has demonstrated that the key stream follows the uniform law.

To assert the uniformity, we recall Equation (4.4) in Chapter 4 for the χ^2 test. The obtained experimental value (χ^2_{exp}) is equal to 999.44 which is smaller than the theoretical

value $\chi^2_{th}\left(N_c - 1, \alpha\right) = 1073.64$ obtained for a threshold $\alpha = 0.05$, which can confirm the uniformity of the generated chaotic sequence.

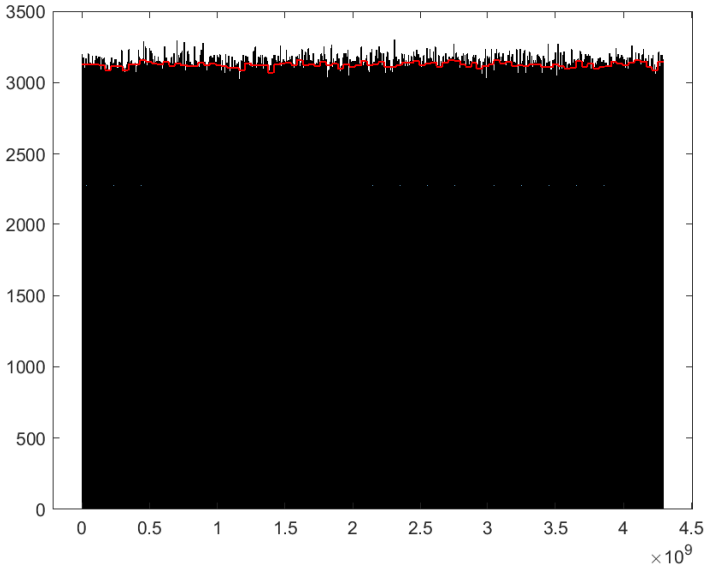


FIGURE 5.9 – Histogram of the produced key stream

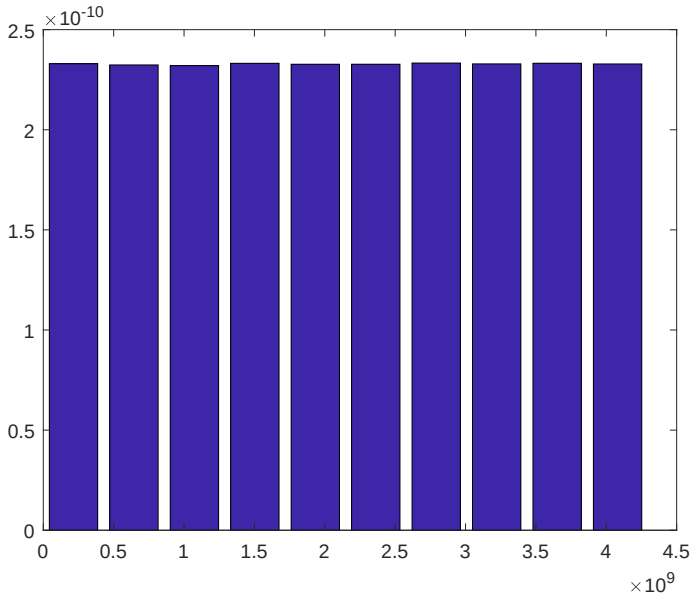


FIGURE 5.10 – The approximation of the probability density of the key stream

Uniformity test in binary level

In addition, we divide the produced sequence into 100 binary sub-sequences in which we calculate the proportion of bits 0 and 1. The obtained results are shown in Figure 5.11. As we can see, the distributions of bits 0 and 1 are close to the optimal value 50%.

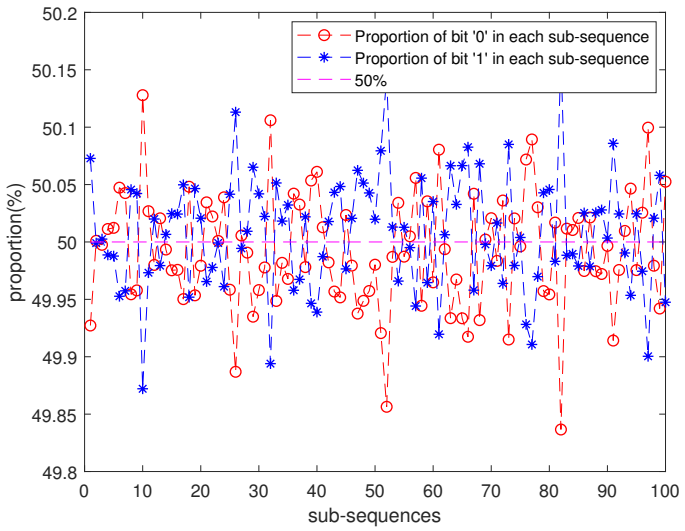


FIGURE 5.11 – Proportion of numbers of bit $'0'$ and $'1'$

NIST test

We apply NIST test on the previous produced sequence (3125000×32 bits $= 100$ bit streams $\times 10^6$ bits). The obtained results in Table 5.2 have shown that the generated chaotic numbers have passed the NIST test successfully.

All the obtained results up to now have demonstrated that the proposed PCNG can produce pseudo-random numbers efficiently, thus it is able to resist statistical attacks.

5.3.2 Security analysis of the cryptosystem

In the proposed encryption scheme, the global diffusion enhances the diffusion effect by HAD and VAD algorithm which spread the pixels' influence in the plain image, and the modified 2D cat map reinforces this property by relocating the pixels. From Figure 5.6 and Table 5.1, we have observed that for rounds $rg \geq 2$, the achieved diffusion level on the whole image is very good. In addition, the block cipher in CBC mode improves the diffusion effect. The confusion effect of the cryptosystem is achieved here by the AES S-Box

TABLE 5.2 – P-values and Proportion results of NIST test

Test	P-value	Proportion	result
Frequency test	0.494	98.000	passed
Block-frequency test	0.720	99.000	passed
Cumulative-sums test	0.491	98.000	passed
Runs test	0.679	99.000	passed
Longest-run test	0.924	99.000	passed
Rank test	0.911	100.000	passed
FFT test	0.883	100.000	passed
Nonperiodic-templates	0.566	99.115	passed
Overlapping-templates	0.225	99.000	passed
Universal	0.554	96.000	passed
Approximty entropie	0.046	98.000	passed
Random-excursions	0.446	98.904	passed
Random-excursions-variant	0.164	99.513	passed
Serial test	0.339	98.500	passed
Linear-complexity	0.419	100.000	passed

which is a robust nonlinear function. Moreover, each plain block is encrypted under different parameters and thus even identical plain blocks will be encrypted into different ones, which increases the encryption keys' space substantially and also enhances the security.

Key space has been analyzed in section 5.2.2. In the following, we analyze the confusion and diffusion properties of the proposed cryptosysteme of Figure 5.1 for rg=1, r=1.

Confusion property

Good confusion demands a high sensitivity of the ciphered image to the secret key, and makes the statistical relation among the secret key, the plain image and the ciphered image so complex that it is hard for the attacker to recover the secret key even though he has obtained plenty of plain-ciphered images pairs.

In the following, we conduct the experiments based on 8 plain images I_i ($i = 1, 2, ..., 8$ represents the indices of images) of Figure 5.5. For each image, 100 different secret keys produced randomly are used to generate 100 ciphered image $C_{i,j}$, where $i = 1, 2, ..., 8$ represents the indices of images and $j = 1, 2, ..., 100$ indicates the indices of secret keys.

(1) Hamming distance

Hamming distance is given by Equation (5.8).

$$D_H(I,C) = \frac{1}{|lb|}\sum_{k=1}^{|lb|}\left(I\left[k\right] \oplus C\left[k\right]\right) \tag{5.8}$$

where I is the plain image ; C is the ciphered image ; $|lb|$ is the number of bit in the test image.

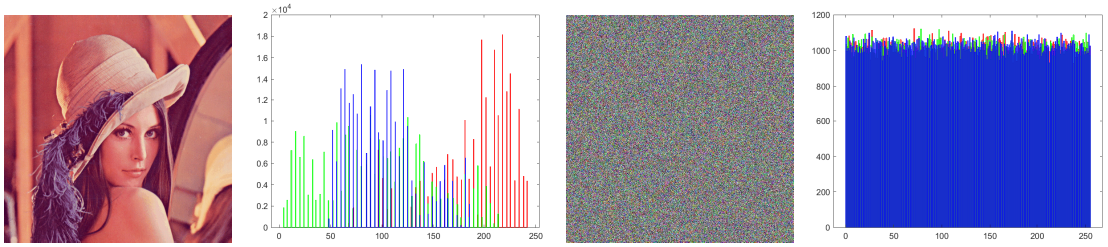
Here, for each plain image I_i ($i = 1, 2, ..., 8$), 100 D_Hs has been calculated between I_i and $C_{i,j}(j = 1, 2, .., 100)$ and then the average D_H has been obtained. The D_H results for each test image have been shown in Table 5.3. They are very close to the optimal value 50%, which indicates that the probability of bit changes between each ciphered image and its plain image is 50%. Thus, the complexity between secret key, plain image and ciphered image is achieved.

TABLE 5.3 – Statistic test results

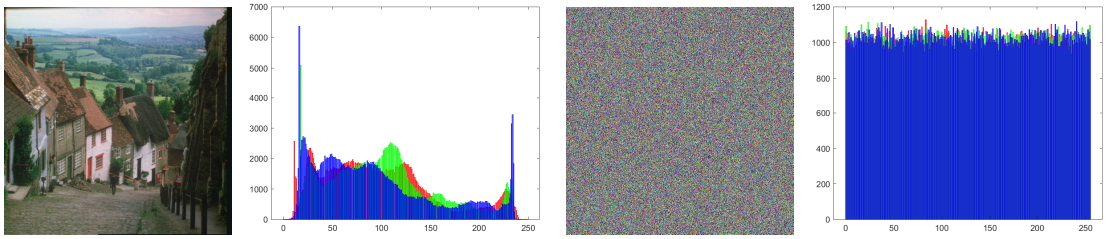
Image	Size	$D_H(\%)$	χ^2_{exp}	Entropy :H(P)	Entropy :H(C)
Airfield	$512 \times 512 \times 1$	49.9975	254.8931	7.1206	7.9993
Baboon	$256 \times 256 \times 3$	50.0046	252.1045	7.7073	7.9991
Boat	$512 \times 512 \times 1$	49.9976	255.4712	7.1914	7.9993
Goldhill	$512 \times 512 \times 3$	50.0032	252.7116	7.6220	7.9998
Lena	$512 \times 512 \times 3$	49.9978	258.0559	5.6822	7.9998
Pepper	$512 \times 512 \times 3$	50.0006	257.2954	7.6698	7.9998
White	$512 \times 512 \times 1$	50.0012	255.4313	0	7.9993
Black	$512 \times 512 \times 1$	49.9949	253.2374	0	7.9993

(2) Histogram and χ^2 test

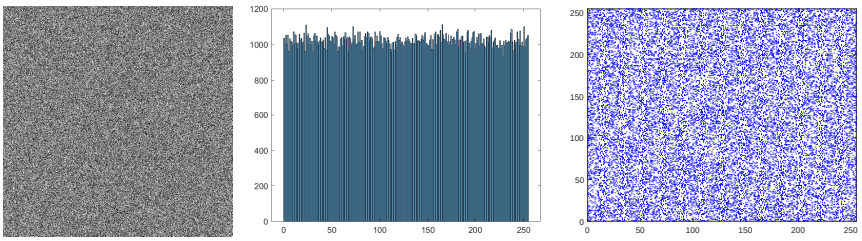
The uniform distribution of a ciphered image is a basic condition to resist statistical attacks. Figure 5.12(a), 5.12(e) represent the plain images of Lena and Goldhill. Their histograms in RGB color plane are shown in Figure 5.12(b), 5.12(f), which reflects their color compositions. The corresponding ciphered images Figure 5.12(c), 5.12(g) are uniformly distributed in each color plane as shown in Figure 5.12(d), 5.12(h). We can observe that even for White and Black images Figure 5.12(i), 5.12(m), their ciphered ones shown in Figure 5.12(j), 5.12(n) appear to be random and their corresponding histograms shown in Figure 5.12(k), 5.12(o) have uniform distribution.



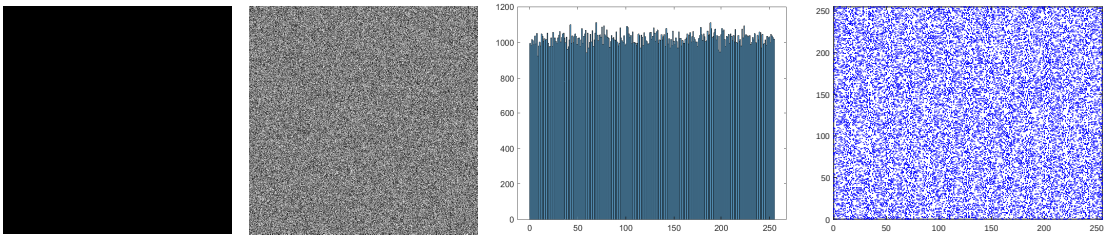
(a) Lena (b) Histogram (c) Ciphered image (d) Histogram of ciphered image



(e) Goldhill (f) Histogram (g) Ciphered image (h) Histogram of ciphered image



(i) White (j) Ciphered image (k) Histogram of ciphered image (l) Correlation in ciphered image



(m) Black (n) Ciphered image (o) Histogram of ciphered image (p) Correlation in ciphered image

FIGURE 5.12 – Plain and ciphered $Lena/Goldhill/White/Black$ images and their histograms

To assess their uniformity accurately, the χ^2 test is applied using Equation (4.4) with

different parameters : $N_c = 256$, $E_i = (M \times M \times Plane)/K$, $\alpha = 0.05$. Thus,the theoretical value is $\chi^2_{th}(255, 0.05) = 293.2478$. The values shown in Table 5.3 are the average experimental values χ^2_{exp} calculated based on 100 ciphered images ($C_{i,1}, C_{i,2}, ..., C_{i,100}$), which has confirmed the uniformity of the ciphered images.

(3) Information entropy test

Information entropy test is adopted here to evaluate uncertainty and randomness properties in the ciphered images. According to Equation (4.5) in Section 4.3.2. We have calculated the information entropy for each plain image ($H(P)$) and the average entropy ($H(C)$) values based on 100 ciphered image ($C_{i,1}, C_{i,2}, ..., C_{i,100}$). From the obtained results shown in Table 5.3, we remark that the information entropy values of the ciphered images are close to the ideal value, i.e. 8.

(4) Correlation analysis

In order to test the correlation between two adjacent pixels, 8000 pairs of adjacent pixels have been selected randomly in horizontal (H), vertical (V) and diagonal (D) directions respectively from the plain image and its corresponding ciphered image. Then the correlation coefficient (ρ_{xy}) of each pair is calculated by Equation (4.6).

The correlation coefficient of each plain image (I_i) of Figure 5.5 and the average correlation coefficient of its corresponding ciphered images ($C_{i,1}, C_{i,2}, .., C_{i,100}$) have been calculated. In Table 5.4, we give the results obtained for R,G,B color planes in each direction (H, V and D). We also show the correlation of image $Pepper$ in three directions of the plain and ciphered images separately in Figure 5.13. For White and Black images, their correlation in H, V, D directions of the ciphered image are presented in Figure 5.12(l) and Figure 5.12(p). Table 5.4 and Figure 5.13 have demonstrated the adjacent pixels are highly correlated to each other in the plain image but appear uncorrelated in the ciphered image.

Diffusion property : against the chosen-plaintext attack

In the chosen plaintext attack (differential attack), difference analyses are applied between ciphered images which are encrypted by a certain number of plain images (just 1 bit difference from each other). To resist these attacks, a high plaintext sensitivity is required. This is the diffusion property which assesses how a small change in the plain text affects the corresponding ciphered one. In addition, similar cryptanalysis approach can be applied to secret keys in order to derive the derive the secret key and crack the cryptosystem. Thus, a secure cryptosystem should be highly sensitive to even one bit change in the plain image or in the secret key.

TABLE 5.4 – Correlation coefficient values

Image	Size		Plain image			Ciphered image		
			H	V	D	H	V	D
Airfield	$512 \times 512 \times 1$		0.93994	0.94185	0.90514	0.00146	0.00025	0.00039
		R	0.95387	0.93427	0.91779	0.00022	0.00073	0.00141
Baboon	$256 \times 256 \times 3$	G	0.88427	0.85596	0.81150	0.00102	-0.00125	0.00003
		B	0.92882	0.92848	0.89313	0.00021	-0.00153	0.00032
Boat	$512 \times 512 \times 1$		0.93748	0.97129	0.92198	0.00047	-0.00252	0.00124
		R	0.97764	0.97647	0.95983	-0.00059	0.00031	-0.00133
Goldhill	$512 \times 512 \times 3$	G	0.98196	0.98501	0.97002	-0.00089	-0.00171	0.00052
		B	0.98444	0.98646	0.97345	-0.00089	0.00003	-0.00157
		R	0.97524	0.98533	0.96489	-0.00028	0.00229	-0.00107
Lena	$512 \times 512 \times 3$	G	0.96666	0.98009	0.95345	-0.00184	-0.00069	0.00190
		B	0.93391	0.95554	0.91848	0.00160	-0.00181	-0.00105
		R	0.96236	0.96537	0.95416	0.00023	-0.00006	0.00046
Pepper	$512 \times 512 \times 3$	G	0.97951	0.97945	0.96490	0.00099	0.00040	0.00037
		B	0.96577	0.96333	0.94436	0.00011	-0.00256	-0.00039
White	$512 \times 512 \times 1$		-	-	-	-0.00105	-0.00146	0.00152
Black	$512 \times 512 \times 1$		-	-	-	0.00017	-0.00176	-0.00203

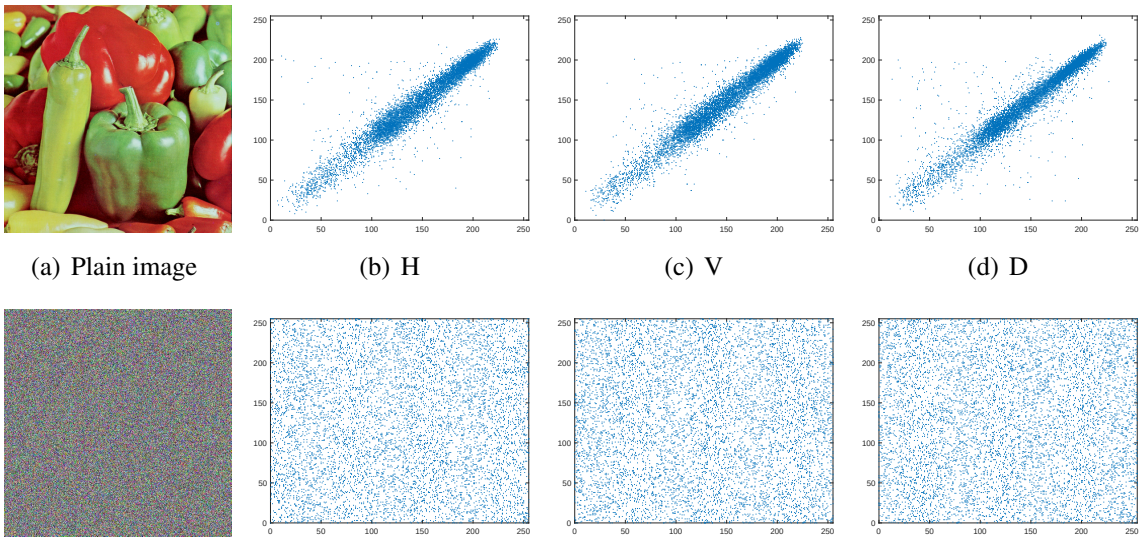
(1) Hamming distance

Plaintext sensitivity can be measured using Hamming distance (see Equation (5.7)) between two ciphered images C_1 and C_2 which are encrypted from two plain images with only one bit difference.

For each image of Figure 5.5, the pixels at 21 positions have been chosen in turn to change their LSBs, and then after the encryption process, 21 D_H values have been computed by Equation (5.7). For each position, the D_Hs of the eight test images (blue points) and their average values (red line) are shown in Figure 5.14. We observe that for each position, the average D_H over images is close to the optimal value 50%. Moreover, the maximum D_H is equal to 50.145% and the minimum one is equal to 49.8598% which are near to the theoretical optimal value. In Figure 5.15, we compare the diffusion property of the proposed cyptosystem with the AES-CBC algorithm. As we can see, the obtained diffusion results are excellent compared to the AES-CBC one.

(2) NPCR and UACI tests

We also use two parameters to measure the cryptosystem's sensitivity on the plaintext and the secret key : the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), which are commonly used by researchers and defined by Equation (4.8) and Equation (4.9).



(a) Plain image (b) H (c) V (d) D

(e) Ciphered image (f) H (g) V (h) D

FIGURE 5.13 – Correlation between adjacent pixels of $Pepper$ in three directions (H, V, D) in plain and ciphered image

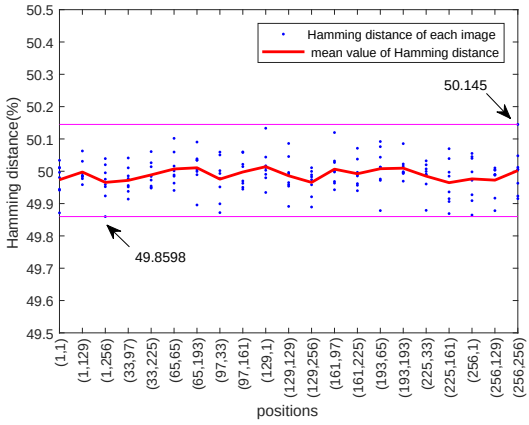


FIGURE 5.14 – Hamming distance

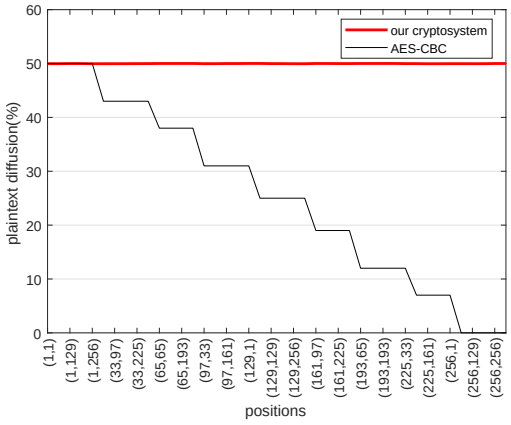


FIGURE 5.15 – Comparison with AES-CBC

For each test image, the plain image has been encrypted into the ciphered one C_1. The pixels at 21 different positions have been changed their LSBs in turn and 21 ciphered images C_2 have been obtained after the cryptosystem. The average values of NPCR, UACI for plaintext sensitivity analysis have been calculated in Table 5.5. To analyze the secret key sensitivity property, we have changed the LSB of each inner secret key ($Xc(0)$, $Xs(0)$, P, $Seed$) in turn to obtain the ciphered image C_2. The average NPCR and UACI results over each inner secret key have been given in Table 5.5. The test results in Table 5.5 are all

close to the optimal values of NPCR and UACI that are 99.6094% and 33.4635%.

TABLE 5.5 – NPCR and UACI results

Image	Size	Plaintext sensitivity		Secret key sensitivity	
		NPCR(%)	UACI(%)	NPCR(%)	UACI(%)
Airfield	$512 \times 512 \times 1$	99.6088	33.4770	99.6169	33.4505
Baboon	$256 \times 256 \times 3$	99.6109	33.4493	99.6044	33.5260
Boat	$512 \times 512 \times 1$	99.6119	33.4680	99.6150	33.4143
Goldhill	$512 \times 512 \times 3$	99.6102	33.4808	99.6097	33.4764
Lena	$512 \times 512 \times 3$	99.6097	33.4573	99.6062	33.4672
Pepper	$512 \times 512 \times 3$	99.6071	33.4543	99.6076	33.4601
White	$512 \times 512 \times 1$	99.6097	33.4707	99.6150	33.4323
Black	$512 \times 512 \times 1$	99.6113	33.4676	99.6106	33.4162

Here, we also compare the security of our proposed cryptosystem with other benchmarks from the literature in terms of the confusion and diffusion properties, see Table 5.6, 5.7. It can be observed that our cryptosystem has achieved similar results compared to other benchmark cryptosystems.

TABLE 5.6 – Comparison on confusion property

Cryptosystem	Confusion	χ^2 test	Entropy	Correlation coefficient in ciphered image			
	$D_H(\%)$	χ^2_{exp}	H(C)		H	V	D
Proposed scheme (Lena in RGB)	49.9978	258.0559	7.9998	R	-0.00028	0.00229	-0.00107
				G	-0.00184	-0.00069	0.00190
				B	0.00160	-0.00181	-0.00105
Proposed scheme (Lena in gray)	49.9999	253.6835	7.9993		0.00176	-0.00093	0.00167
Lena in Ref. [165]	-	-	7.9993	R	-0.0131	0.0142	-0.0044
			7.9994	G	-0.0007	-0.0167	-0.0145
			7.9993	B	0.0036	0.0083	-0.0214
Lena in Ref. [108]	-	-	7.9976		0.0018	0.0040	-0.0006
Lena in Ref. [113]			7.9993		0.0019	-0.0024	0.0011
test image in Ref. [166]	-	-	7.9973		-0.00048	0.00277	0.00096
Lena in Ref. [167]	-	-	7.9987		-0.0115	-0.0032	0.0047
test image in Ref. [168]	-	-	7.9983		-0.0056	0.0044	0.0089

TABLE 5.7 – Comparison on diffusion property

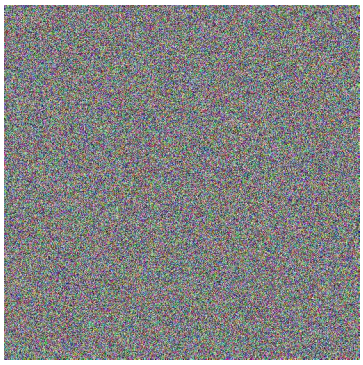
Cryptosystem	Diffusion		Plaintext sensitivity		Key sensitivity	
	$D_H(\%)$		NPCR(%)	UACI(%)	NPCR(%)	UACI(%)
Proposed scheme (Lena in RGB)	49.9944		99.6097	33.4573	99.6062	33.4672
Proposed scheme (Lena in gray)	50.0079		99.6080	33.4925	99.6100	33.4763
		R	99.5941	33.471	-	-
Lena in Ref. [93]	-	G	99.614	33.4784	-	-
		B	99.6383	33.4211	-	-
		R	99.6091	33.4678	99.6089	33.4589
Lena in Ref. [98]	-	G	99.6099	33.4577	99.6089	33.4598
		B	99.6090	33.4608	99.6085	33.4624
Lena in Ref. [108]	-		99.6086	33.4507	99.5972	30.7214
Lena in Ref. [113]	-		99.6113	33.4682		
		R	99.79	33.56	-	-
Lena in Ref. [167]	-	G	99.85	35.64	-	-
		B	99.86	36.06	-	-
test image in Ref. [168]	-		99.4566	33.1561	-	-

5.3.3 Robustness analysis

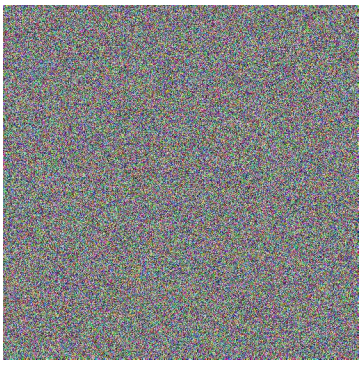
Since the ciphered image may suffer from noise interference and data loss during transmission, the image cryptosystem should be robust against noise attacks and corrupted data. Here, we analyze its robustness in terms of the ability to resist salt and pepper noise perturbation and occlusion attack.

The ciphered Lena image has been added the salt and pepper noise in three intensities of 0.01, 0.05 and 0.1 that are shown in Figure 5.16(a),5.16(b),5.16(c), and their corresponding recovered images are given in Figure 5.16(d),5.16(e),5.16(f). We can observe that the quality of the recovered image decreases with the increase of noise intensity. However, the recovered image can still be identified, which shows that the proposed image cryptosystem has a good robustness for resisting noise attack.

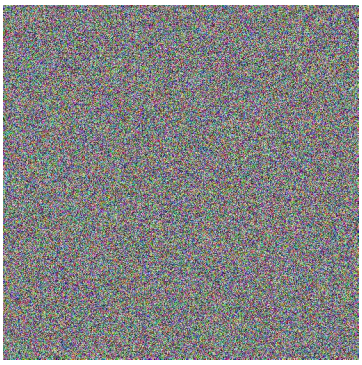
What's more, the cryptosystem should be capable of resisting the occlusion attack. To evaluate this property, the ciphered Lena image has been submitted to the occlusion attack from different positions in the image with different data loss size. The test results can be found in Figure 5.17.



(a) Intensity of 0.01

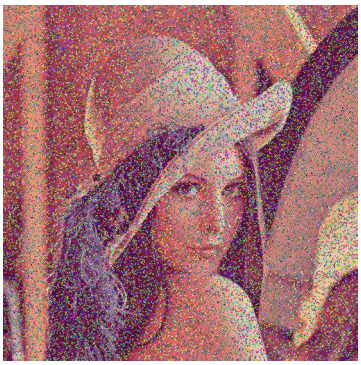


(b) Intensity of 0.05

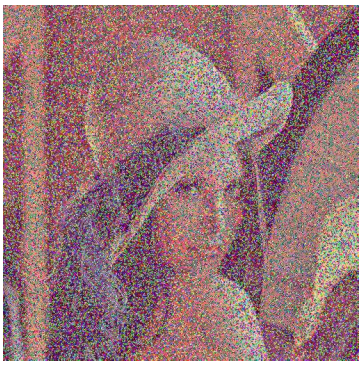


(c) Intensity of 0.1

(d) Recovered image

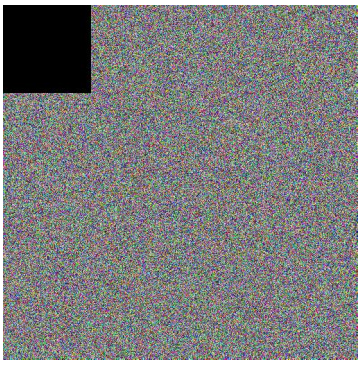


(e) Recovered image

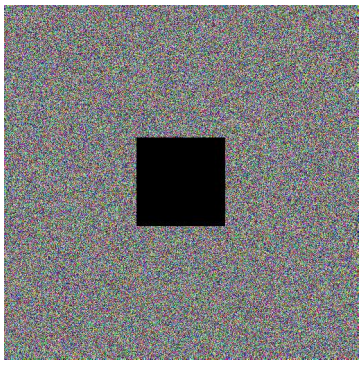


(f) Recovered image

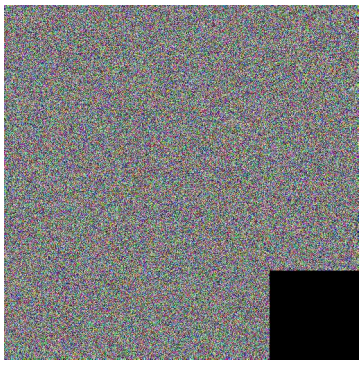
FIGURE 5.16 – Robustness against salt and pepper noise



(a) $1/16$ data loss at upper left corner

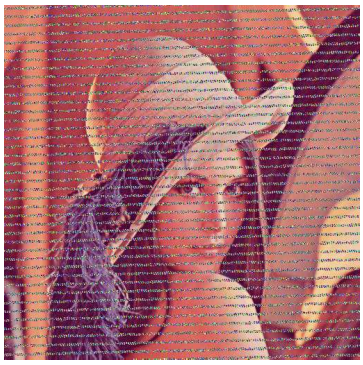


(b) $1/16$ data loss at middle

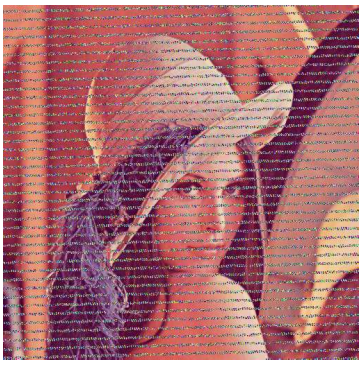


(c) $1/16$ data loss at lower right corner

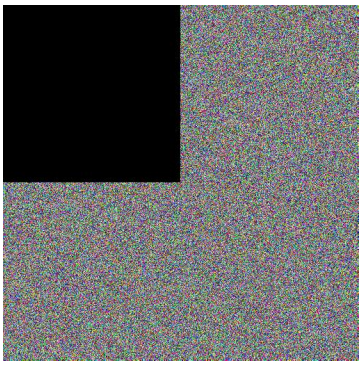
(d) Recovered image from above



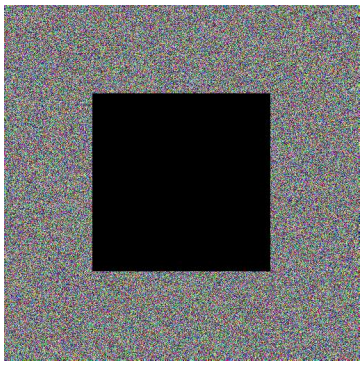
(e) Recovered image from above



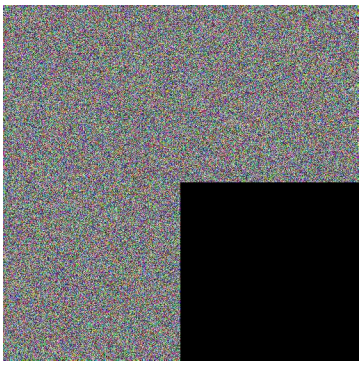
(f) Recovered image from above



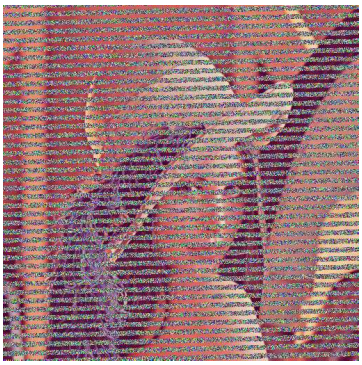
(g) $1/4$ data loss at upper left corner



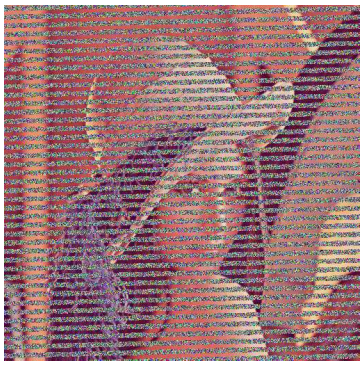
(h) $1/4$ data loss at middle



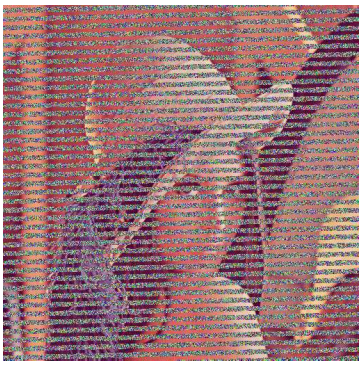
(i) $1/4$ data loss at lower right corner



(j) Recovered from above



(k) Recovered from above



(l) Recovered from above

FIGURE 5.17 – Robustness against occlusion attack

As shown in Figure 5.17, Figure 5.17(a), 5.17(b), 5.17(c) represent the ciphered Lena image with $1/16$ (128×128) pixels loss in the upper left corner, middle, lower right corner. The recovered image are given in Figure 5.17(d), 5.17(e), 5.17(f). Also, the ciphered image

with $1/4$ (256×256) data loss are displayed in Figure 5.17(g), 5.17(h), 5.17(i), and their corresponding recovered images are shown in Figure 5.17(j), 5.17(k), 5.17(l), respectively. It can be seen that the recovered images can be recognized even if a quarter of the ciphered image is lost, which demonstrates the high robustness of the proposed image cryptosystem.

5.3.4 Computation time analysis

The encryption time of an image cryptosystem is influenced by many factors, such as programming language, operating environment, code optimization, etc. Thus, it is impossible to obtain an explicit comparison results from different algorithms running in different environments. For these reasons, Encryption Throughput (ET) and Number of needed Cycles per Byte (NCpB) defined by Equation (5.9) and (5.10) have been adopted to evaluate the encryption speed of the proposed cryptosystem. For that, the encryption time in Equation (5.9) is calculated by averaging 100 encryption times using 100 different secret keys. Table 5.8 shows the ET and NCpB of the proposed cryptosystem compared to other encryption systems running in similar environments.

$$ET = \frac{Image_{size}(Byte)}{Encryption_{Time}(second)} \tag{5.9}$$

$$NCpB = \frac{CPUSpeed(Hertz)}{ET(Byte/s)} \tag{5.10}$$

TABLE 5.8 – ET and NCpB results

Cryptosystem	ET(MBps)	NCpB
Proposed	0.045	77385.32
Ref. [169]	0.035	95367.43
Ref. [94]	0.213	15641.21

According to [96, 99], the computation time of an image cryptosystem mainly consists in the iterations of chaotic maps and the real number arithmetics and quantization. The proposed cryptosystem does not cost time in quantization since the proposed PCNG has been defined over a finite field. However, the iterations are still the most time consuming operation. This can be observed from Figure 5.18 which displays the encryption time percentage of each component of the proposed cryptosystem for Lena image with size 512×512.

Because of the repetitions of 2D cat map for each block in the block cipher and the iterations of PCNG, the 2D cat map in the block cipher accounted for almost a half of the total computing time, followed by the PCNG which takes another 20%.

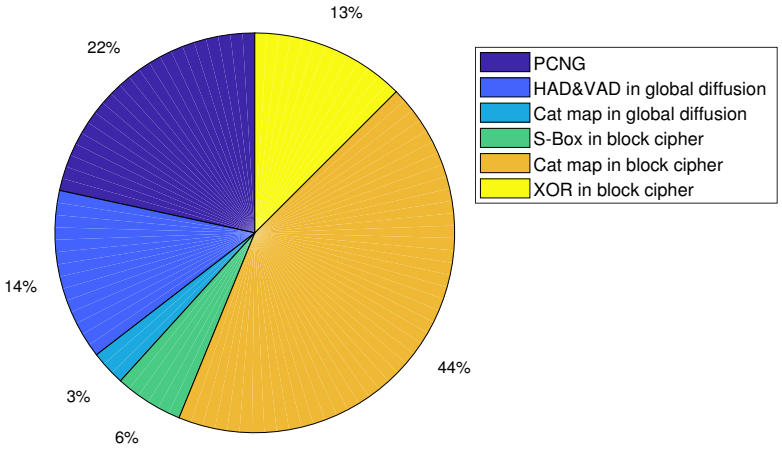


FIGURE 5.18 – Encryption time percentage of each component of the proposed cryptosystem for $Lena$ image with size 512×512

5.4 Conclusion

In this chapter, a secure robust cryptosystem based on chaotic components and the AES S-Box is proposed, which contains an efficient PCNG, a global diffusion and a block cipher. The PCNG defined over a finite integer field eliminates the risk of deteriorated security resulting from the dynamical degradation when chaotic maps defined on real numbers are numerically implemented. The HAD and VAD with the modified 2D cat map in global diffusion increase effectively the diffusion properties among the pixels of an image. The block cipher composed of the AES S-Box, the modified 2D cat map and an XOR masking operator works in CBC mode, which reinforces the confusion and diffusion performances. The security analyses of the experimental results have demonstrated that the proposed image encryption system can resist successfully the main known attacks in the literature and it is suitable for practical implementations.

CHAPITRE 6

EXPLORING A SMART COUPLING OF CHAOTIC MAPS FOR NEW PSEUDO-RANDOM NUMBER GENERATORS (PRNGS)

6.1 Introduction

As can bee seen from Chapter 4 and Chapter 5, PCNG plays a significant role in the security of a cryptosystem. Basically, a PCNG in a chaos-based cryptosystem is first and foremost a pseudo-random number generator (PRNG), but apart from the randomness, these PRNGs should meet the security requirements, such as a large secret key space and the high sensitivity to the secret key (seed of a PRNG). Besides the encryption field, PRNG is also a vital component for a plethora of applications. In this chapter, for highlighting the pseudo-randomness of the generated numbers, we use a more common and familiar term "PRNG" to describe the "PCNG" appeared in the previous chapters.

PCNGs designed in Chapter 4 and Chapter 5 used specific chaotic maps to produce randomness. This chapter will propose a chaos-based PRNG design framework based on a smart chaotic maps coupling and output control structures. This PRNG framework can employ different 1D chaotic maps to produce a huge number of pseudo-random sequences with good cryptographic properties.

In the proposed PRNGs, the coupling model, defined over the integer field, aims at breaking the original orbits (that exhibit short periods) generated by single chaotic maps and thus lengthen the periods, boost the dynamic behavior and improve the randomness. Two types of chaotic generator output control approaches, i.e. alternate output control and dynamic output control, following the coupling model are designed to enhance the ran-

domness and unpredictability of the PRNGs. In addition, to improve their cryptographic property to resist the brute-force attack, a key space expandable strategy will be presented in this chapter.

In the following sections, we will introduce the chaotic maps coupling model in two dimensions and three dimensions, and analyze the coupling performance in Section 6.2 and Section 6.3. Then, PRNG schemes based on the coupling model and two types of output control methods will be introduced and evaluated in Section 6.4. After that, Section 6.5 will give the key space expandable scheme and its performance analysis.

The kernel of the PRNGs is the chaotic coupling model that is inspired by the idea of ultra-weak coupling over a real number domain in the work of Professor René Lozi [120].

Firstly, we recall the model of ultra-weak coupling in [120]. It works on the continuous field using floating-point and fixed-point notations according to the ordinary (IEEE-754) precision standard. Using an example of a symmetric tent map which is noted as

$$f : x_{n+1} = 1 - 2\,|x_n| \tag{6.1}$$

where the $n-$th iterate x_n is in the range of $[-1, 1]$. Using the ultra-weak coupling scheme to couple two tent maps, it can be described as follows :

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \mathrm{A} \cdot \begin{bmatrix} f\,(x_n) \\ f\,(y_n) \end{bmatrix} \tag{6.2}$$

where **A** is the coupling matrix :

$$\mathbf{A} = \begin{bmatrix} 1-\varepsilon_1 & \varepsilon_1 \\ \varepsilon_2 & 1-\varepsilon_2 \end{bmatrix}$$

The coupling constant $\varepsilon = (\varepsilon_1, \varepsilon_2)$ varies from $(0, 0)$ to $(1, 1)$, and the coupling coefficients sum per line is 1. If $\varepsilon = (0, 0)$, the maps are completely decoupled ; $\varepsilon = (1, 1)$ means the maps are fully cross coupled. In the Lozi's study in [120], constant ratio between ε_1 and ε_2 is fixed to 2, that is : $\varepsilon_2 = 2\varepsilon_1$.

The parameters ε_1 and ε_2 are very small ($\varepsilon_1 = 10^{-7}$ for floating-point numbers or $\varepsilon_1 = 10^{-14}$ for double precision numbers) but the authors aimed to verify that even ultra small coupling parameter can render the chaotic map a very long period one and thus they offered a good technique for PRNG design.

An example of the implementation of this ultra-weak coupling is based on four-dimensional

(4D) coupling :

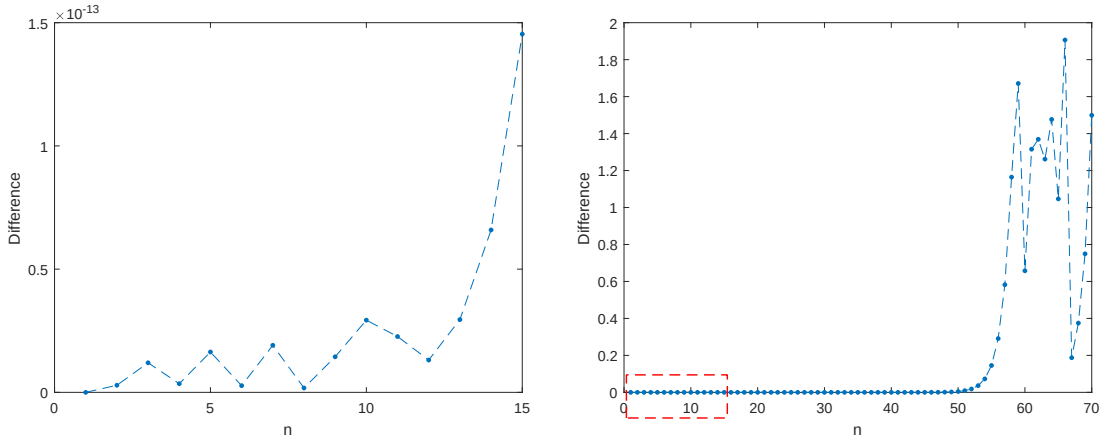
$$\begin{bmatrix} x_{n+1}^1 \\ x_{n+1}^2 \\ x_{n+1}^3 \\ x_{n+1}^4 \end{bmatrix} = \mathbf{A} \cdot \begin{bmatrix} f\left(x_n^1\right) \\ f\left(x_n^2\right) \\ f\left(x_n^3\right) \\ f\left(x_n^4\right) \end{bmatrix} \tag{6.3}$$

where the coupling matrix $\mathbf{A}$ is :

$$\mathbf{A} = \begin{bmatrix} 1-3\varepsilon_1 & \varepsilon_1 & \varepsilon_1 & \varepsilon_1 \\ \varepsilon_2 & 1-3\varepsilon_2 & \varepsilon_2 & \varepsilon_2 \\ \varepsilon_3 & \varepsilon_3 & 1-3\varepsilon_3 & \varepsilon_3 \\ \varepsilon_4 & \varepsilon_4 & \varepsilon_4 & 1-3\varepsilon_4 \end{bmatrix}$$

and $\varepsilon_1 = 10^{-14}, \varepsilon_2 = 2\varepsilon_1, \varepsilon_3 = 3\varepsilon_1, \varepsilon_4 = 4\varepsilon_1$.

This is an ultra weak coupling, since the parameter $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ is very small. For the generated sequence $x^l, (l = 1, 2, 3, 4)$, its orbit exhibits an gradually accumulated perturbation when compared to the original chaotic orbit created by the tent map (Equation (6.1)). The difference (absolute values) of two orbits can be observed by Figure 6.1, which indicates the coupling works even if the parameter ε is extremely small.



(a) $n = 0, 1, 2, ..., 15$ (enlarged red rectangular area of (b))

(b) $n = 0, 1, 2, ..., 70$

FIGURE 6.1 – Difference between the orbit x^1 produced by the coupling scheme (6.3) and the original chaotic orbit produced by the tent map (6.1). n is the number of iterations ; the same initial conditions as in the Lozi's work : $x_0^1 = 0.330, x_0^2 = 0.3387564,\ x_0^3 = 0.50492331,\ x_0^4 = 0.0$

However, because of this tiny difference, if we plot sequence x^1 in the phase space (x_n^1, x_{n+1}^1) in Figure 6.2, the function of tent map still can be recognized. This is not a big problem to PRNG design if it is not used for encryption purposes, but it is indeed a drawback for encryption purposes because the information leakage of the chaotic function will be very helpful for attackers to crack a cryptosystem.

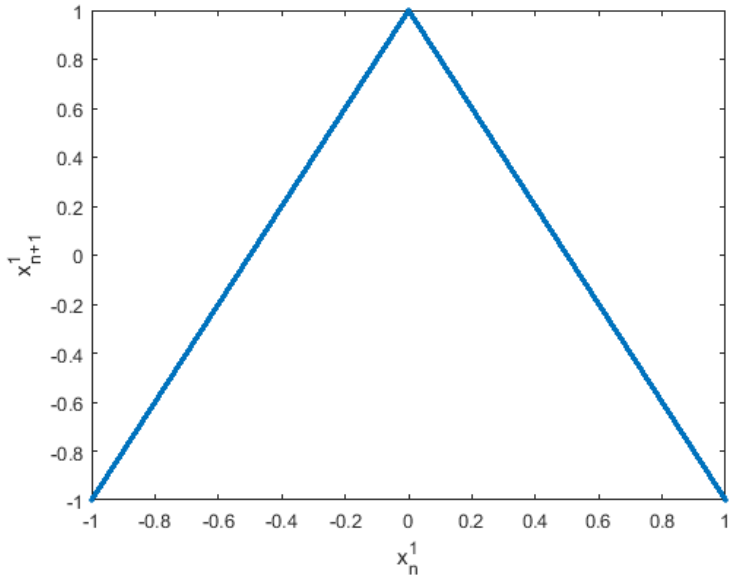


FIGURE 6.2 – x^1 in the phase space (x_n^1, x_{n+1}^1)

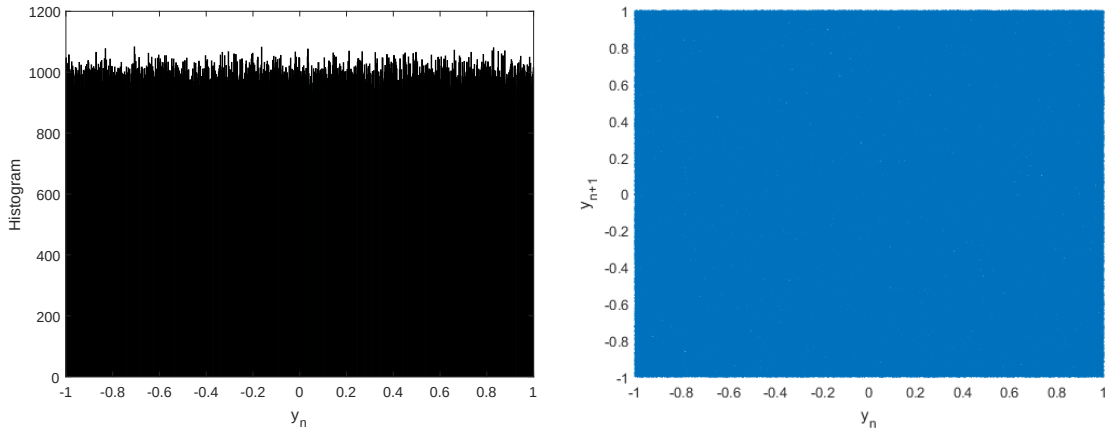
To hide the function and increase the unpredictability, a sampling strategy has been proposed in his work [120] to control the output y_q $(q = 1, 2, 3, ...)$:

$$y_q = \begin{cases} x_n^1, & if\ x_n^4 \in [T_1, T_2] \\ x_n^2, & if\ x_n^4 \in [T_2, T_3] \\ x_n^3, & if\ x_n^4 \in [T_3, 1] \end{cases} \tag{6.4}$$

with $T_1 = 0.998, T_2 = 0.9987, T_3 = 0.9994$.

In this condition, approximately 1000 iterates of x^1, x^2, x^3 and x^4 can output one chaotic number y_q. The histogram diagram of a produced sequence y distributed in 1000 intervals is shown in Figure 6.3(a), which indicates y has a uniform distribution. Besides, according to Figure 6.3(b) which displays the produced sequence y in the phase space (x_n^1, x_{n+1}^1), we can find that Equation (6.4) is able to conceal the function of the chaotic map effectively.

In summary, Lozi's ultra-weak coupling is able to couple chaotic maps for PRNG de-



(a) Histogram

(b) Phase space (y_n^1, y_{n+1}^1)

FIGURE 6.3 – Performance of the output sequence y (length of y is 998930 which is produced by 10^9 iterations of x^1, x^2, x^3, x^4 ; the initial condition is : $x_0^1 = 0.330, x_0^2 = 0.3387564,\ x_0^3 = 0.50492331,\ x_0^4 = 0.0$.)

sign. But it is necessary to combine with a sampling strategy to generate pseudo-random numbers. However, the disadvantage of ultra-weak coupling is that the function of chaotic map is exposed in the phase space, which is insecure for encryption purposes. The sampling strategy also has a drawback of low productivity, because for the 4D scheme, each chaotic map $x^l, (l = 1, 2, 3, 4)$ has to iterate approximately 10^3 times to produce only one pseudo-random number.

In Lozi's ultra-weak coupling scheme, the coupling parameter is extremely small if compared to the chaotic numbers that vary in real domain $[-1, 1]$. Thus, the coupling is ultra-weak. However, if using this idea in the 32-bit integer finite field, even a very small coupling parameter will lead to a big difference in the produced sequence. Hence, the coupling is no longer "ultra-weak". This will be presented in the following sections.

6.2 Two-dimensional coupling

Hereafter, a new coupling matrix defined over the 32-bits integer field will be proposed. The overall dynamics is a combined effect of each parameter in the coupling matrix. We will get started with the two-dimensional (2D) coupling.

The 2D coupling structure is shown in Figure 6.4.

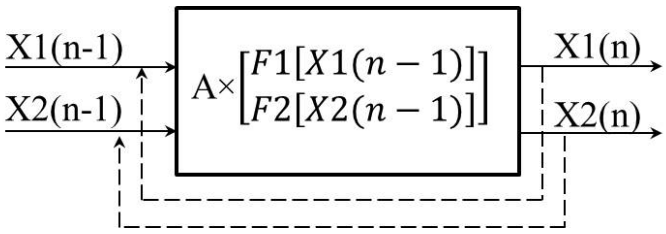


FIGURE 6.4 – 2D coupling structure

The coupling process can be described as

$$\begin{bmatrix} X1\,(n) \\ X2\,(n) \end{bmatrix} = \mathbf{A} \times \begin{bmatrix} F1\,[X1\,(n-1)] \\ F2\,[X2\,(n-1)] \end{bmatrix} \tag{6.5}$$

where $F1$ and $F2$ are 1D chaotic functions ; $X1(n)$, $X2(n)$ represent the states of the system in chaotic regime ; the current states $X1(n)$ and $X2(n)$ are the coupled results of the previous states $X1(n-1)$, $X2(n-1)$; $X1, X2$ stands for the produced sequence.

A general coupling matrix **A** is given as below :

$$\mathbf{A} = \begin{bmatrix} e1 & e2 \\ e3 & e4 \end{bmatrix} \tag{6.6}$$

where the coupling parameters $e1$, $e2$, $e3$, $e4$ are N_e-bit integers in the range of $\left[1, 2^{N_e} - 1\right]$. Here, $N_e = 5$.

Since the coupling scheme aims to increase the randomness features of the produced sequence $X1$ and $X2$, the basic condition of randomness is the uniform distribution property of $X1$ and $X2$. χ^2 test can be used to evaluate the uniformity (see Equation (4.4)). Thus, hereafter, we use the χ^2 experimental values $\chi^2_{\exp}$ to evaluate the uniformity of $X1$ and $X2$.

Generally, if $e1, e2, e3, e4$ are randomly created plenty of times to form different coupling matrix **A**, most of the formed **A** can make the output sequences $X1$ and $X2$ possess uniformity. However, in a few of particular relations between $e1, e2, e3, e4$, $X1$ and $X2$ are not uniformly distributed and they exhibit some special patterns.

To find an effective coupling matrix, we analyze the relation among the coupling parameters.

(1) First test form of A

Firstly, we consider a particular case, that is $e1 = e2 = e3 = e4$. In this case, $X1$ and

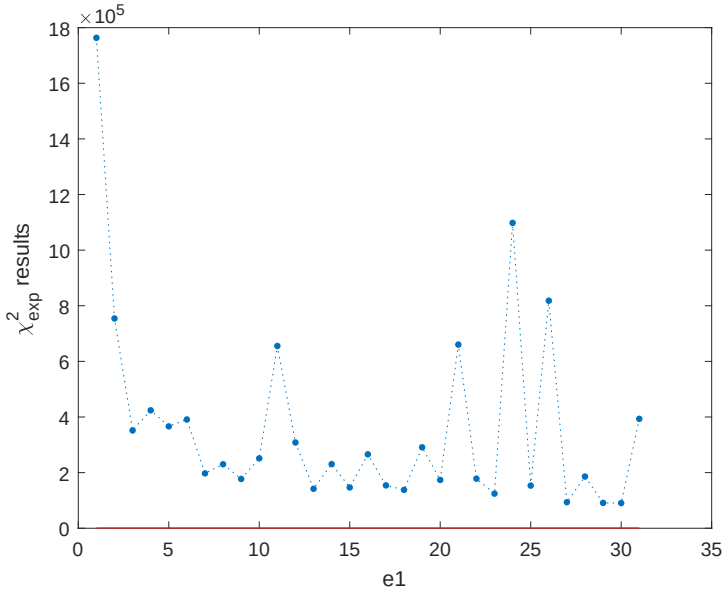
$X2$ are same sequences.

The most widely-used logistic map and skew tent map are chosen to serve as $F1$ and $F2$ to analyze the coupling. The output sequences $X1$ and $X2$ are in the length of 2×10^6, but the the first 10^6 values are considered as transient and removed. The analysis of the design steps will be explained hereafter.

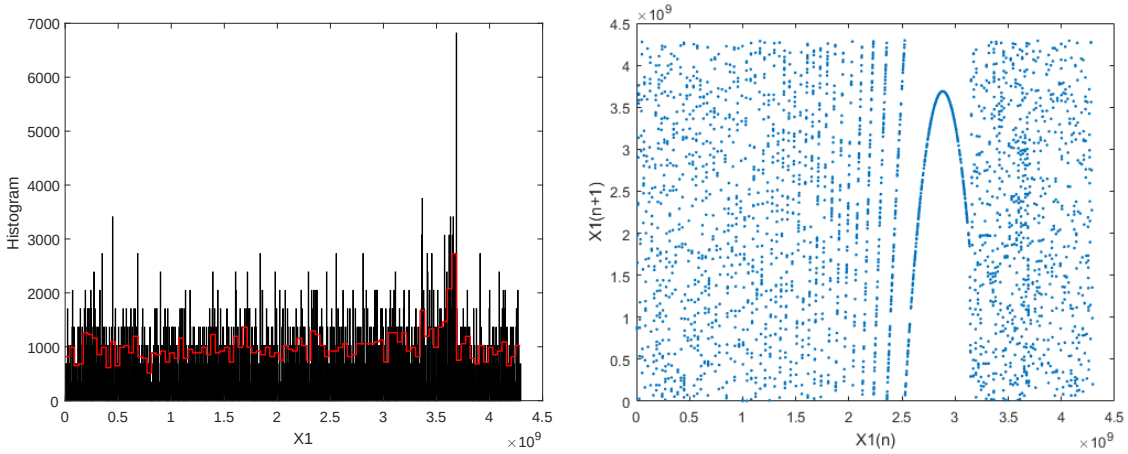
Figure 6.5(a) shows the χ^2_{exp} results (calculated using Equation (4.4)) versus $e1$, from which we can find out that no matter what $e1$ is, $X1$ cannot pass the χ^2 test. This finding also can be demonstrated by the histogram and the phase space diagram (when $e1 = 2^{Ne} - 1$) shown in Figure 6.5(b) and Figure 6.5(c) : the generated sequences in these coupling parameters are not uniformly distributed and they can display special patterns related to the generating functions (original chaotic maps) in the phase space $(X1(n), X1(n+1))$.

Furthermore, all the generated sequences have short periods, which can be seen in Table 6.1. Thus, the combination of the coupling parameters when $e1 = e2 = e3 = e4$ is not suitable for randomness purposes.

Therefore, this type of A using the coupling parameters $e1 = e2 = e3 = e4$ is not suitable to be applied to PRNG design for the following reasons : (1) it cannot ensure the uniformity of $X1, X2$; (2) it causes special patterns in the phase space $(X1(n), X1(n+1))$; (3) the period of $X1$ is too short, which has indicated that it cannot overcome the dynamical degradation caused by the finite precision.



(a) χ^2_{exp} results versus different coupling parameters $e1$



(b) Histogram ($e1 = 31$) (c) Phase space ($X1(n), X1(n+1)$) of X1 ($e1 = 31$)

FIGURE 6.5 – Performance of the output sequence $X1$ [1]

TABLE 6.1 – Periods of $X1$ when $e1 = e2 = e3 = e4$ (using the same conditions with Figure 6.5)

e1	period	e1	period	e1	period	e1	period	e1	period
1	20810	8	16340	15	22452	22	12513	29	23266
2	25997	9	36113	16	7868	23	22349	30	41103
3	47777	10	19774	17	13276	24	919	31	2934
4	16119	11	2540	18	17519	25	11003		
5	8215	12	5842	19	4239	26	1348		
6	9751	13	24918	20	12531	27	27749		
7	46672	14	7467	21	1840	28	6819		

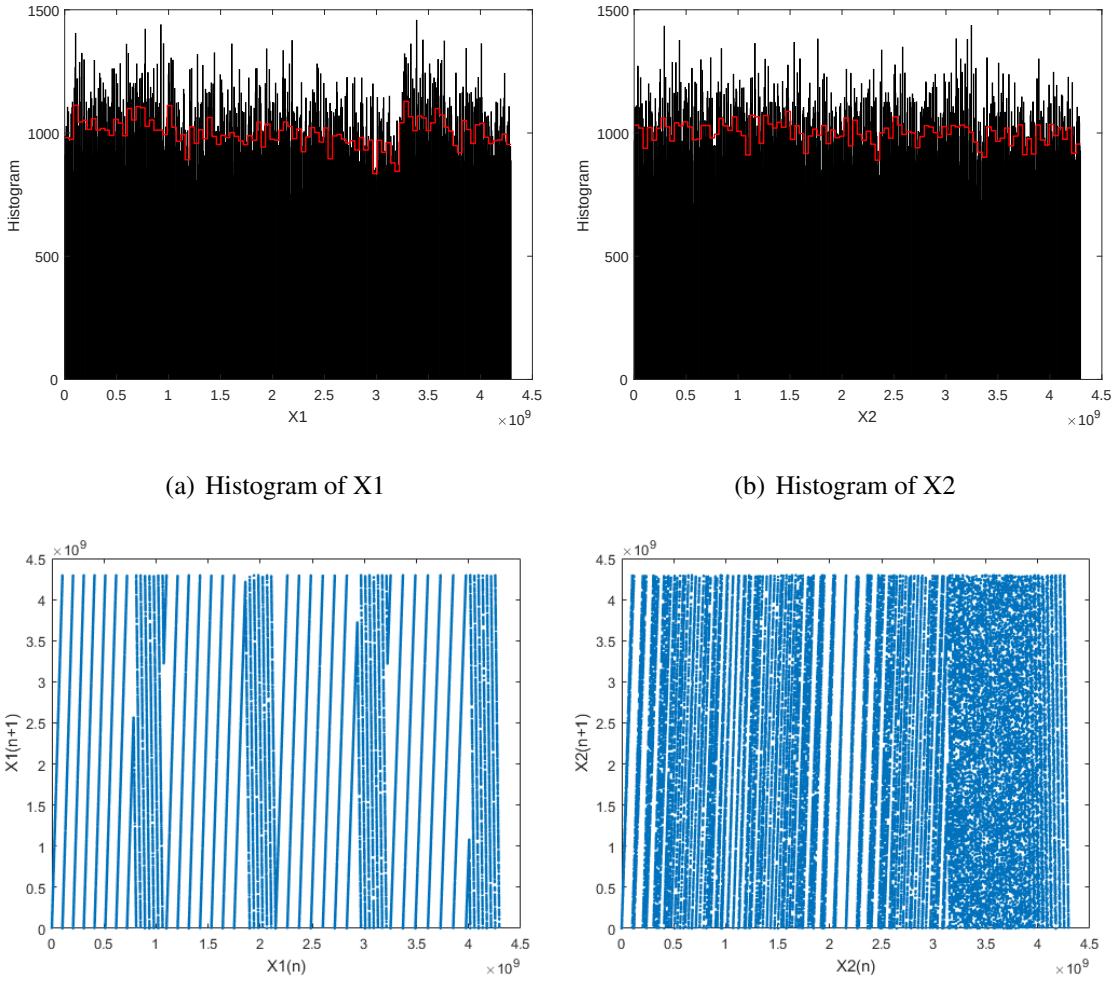
(2) Second test form of A

If the coupling parameters have the relation : $\frac{e2}{e1} = \frac{e4}{e3}$, the coupling performance is still unsatisfactory. As an example, when $A = \begin{bmatrix} 1 & 7 \\ 4 & 28 \end{bmatrix}$, histogram diagrams and the phase space portraits of $X1$, $X2$ are shown in Figure 6.6.

According to Figure 6.6(a) and Figure 6.6(b), sequences $X1$, $X2$ do not exhibit uniformity. More precisely, their corresponding χ^2 test experimental values χ^2_{exp} are 2.1092×10^4 and 1.9052×10^4 which are much larger than the theoretical value $\chi^2_{theo} = 1.073 \times 10^3$. In

1. The initial conditions and parameters are generated randomly in MATLAB. Initial condition for logistic map is 1139372832, and the initial condition and parameter for skew tent map are 3540669105 and 3136394681 respectively.

addition, particular patterns shown in the phase space portraits (see Figure 6.6(c), Figure 6.6(d)) have indicated that the produced $X1$, $X2$ do not possess randomness property after the coupling scheme. Furthermore, we have detected that the period of $X1, X2$ is 50759 which is too short to be a pseudo-random sequence.



(a) Histogram of X1

(b) Histogram of X2

(c) Phase space of X1

(d) Phase space of X2

FIGURE 6.6 – Performance of the output sequence $X1$, $X2$ [2]

If the coupling parameters are in other ratios that satisfy the equation $\frac{e2}{e1} = \frac{e4}{e3}$, $X1, X2$ have the similar performance to those shown in Figure 6.6. Obviously, the relation of $\frac{e2}{e1} =$

2. The length of $X1, X2$ is 2×10^6 but the first 10^6 is regarded as transient and removed ; initial conditions and parameters for chaotic maps are chosen randomly ; initial condition for logistic map is 1139372832 ; the initial condition and parameter for skew tent map are 3540669105 and 3136394681 respectively.

$\frac{e4}{e3}$ includes the case of $e1 = e2 = e3 = e4$. To sum up, if the coupling is linear dependent, i.e. $det(\mathbf{A}) = 0$, the coupling matrix **A** cannot increase the randomness of $X1, X2$.

(3) the final form of A

To avoid the linear dependent coupling and enhance the sensitivity of $X1, X2$ to the parameter in coupling matrix **A**, the final form of **A** using only one parameter (e) is given as below :

$$\mathbf{A} = \begin{bmatrix} (2^{Ne}+1)-e & e \\ 2e & (2(2^{Ne}-1)+1)-2e \end{bmatrix} \tag{6.7}$$

where te coupling parameter $e \in [1, 2^{Ne}-1]$; $Ne = 5$; the constants $(2^{Ne}+1)$ and $(2(2^{Ne-1})+1)$ are the smallest values to make sure all parameters in **A** are positive integers ; notice that, $(2^{Ne}+1)$ (odd number) instead of $(2^{Ne}-1+1)$ (even number) set here is to avoid appearing both even values ($(2^{Ne}-1+1)$ and e) in the first row of **A**. Because from the binary multiplication perspective, for any multiplicand, an even multiplier leads to supplemental zeros added to the end of the significant bits, which will increase the ratio of bit 0 to bit 1. For example, if the multiplier is 2 ("10" in binary), the product is the multiplicand that is left shifted by one bit, and if the multiplier is 16 ("10000" in binary), the product is the multiplicand that is left shifted by four bit. If the coupling matrix **A** is fixed and the first row of **A** is $[16, 16]$ ($e = 16$, and $(2^{Ne}-1+1)$ instead of $(2^{Ne}+1)$ in **A**), the output value $X1(n+1)$ is the low N bits of the sum of $X1(n)$ left-shifted 4 bits and $X2(n)$ left-shifted 4 bits. Thus, the least 4 significant bits all are 0, which has bad effect on the randomness of $X1$. The bad effect can be accumulated as the length of $X1$ increases. Thus, this process will make redundant bits 0 added in the coupling output data, which does not serve the purpose of increasing the randomness of the coupling scheme's output. Using constant $(2^{Ne}+1)$ is able to minimize this drawback.

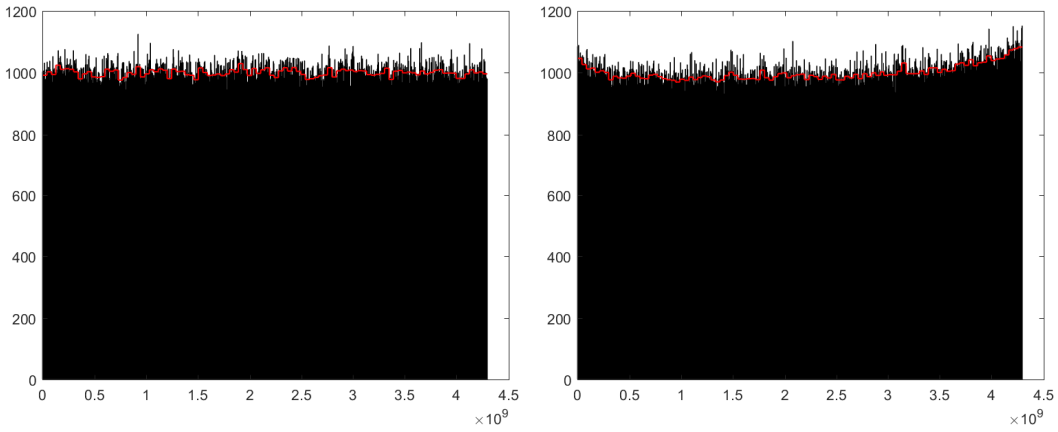
Coupling performance in terms of histogram, χ^2 test, phase portrait and period detection based on the different combinations $(F1, F2)$ have been evaluated and the results have been summarized in Table 6.2.

Firstly, let us consider the uniformity of the produced sequences $X1$ and $X2$. The histogram results shown in Table 6.2 have indicated that almost all coupling combinations render the distribution of X1, X2 uniform except for the couplings of "LL" and "LC" (the notations of "LL" and "LC" are shown in Table 6.2). Visually, histogram of $X1$ produced by the coupling "LS" has been shown in Figure 6.7(a), which has roughly demonstrated the uniform distribution. Other couplings that have passed the histogram test have the si-

milar diagrams. While, the histogram of $X1$ that is produced by the coupling "LC" has been shown in Figure 6.7(b), which reveals this coupling can increase the uniformity of the sequence generated by the original chaotic map but can not ensure a uniform distribution of the coupled outputs $X1, X2$. The histogram of coupling "LL" has similar diagram.

TABLE 6.2 – Coupling performance [3]

Couplings	F1	F2	Histogram and χ^2 test		Phase space		Period detection	
			X1	X2	X1	X2	X1	X2
LL	Logistic	Logistic	×	×	✓	✓	no period detected	
LS	Logistic	Skew tent	✓	✓	✓	✓	no period detected	
LP	Logistic	PWLCM	✓	✓	✓	✓	no period detected	
LC	Logistic	Chebyshev 3rd order	×	×	✓	✓	no period detected	
SL	Skew tent	Logistic	✓	✓	✓	✓	no period detected	
SC	Skew tent	Chebyshev 3rd order	✓	✓	✓	✓	no period detected	
SP	Skew tent	PWLCM	✓	✓	✓	✓	no period detected	
SS	Skew tent	Skew tent	✓	✓	✓	✓	no period detected	



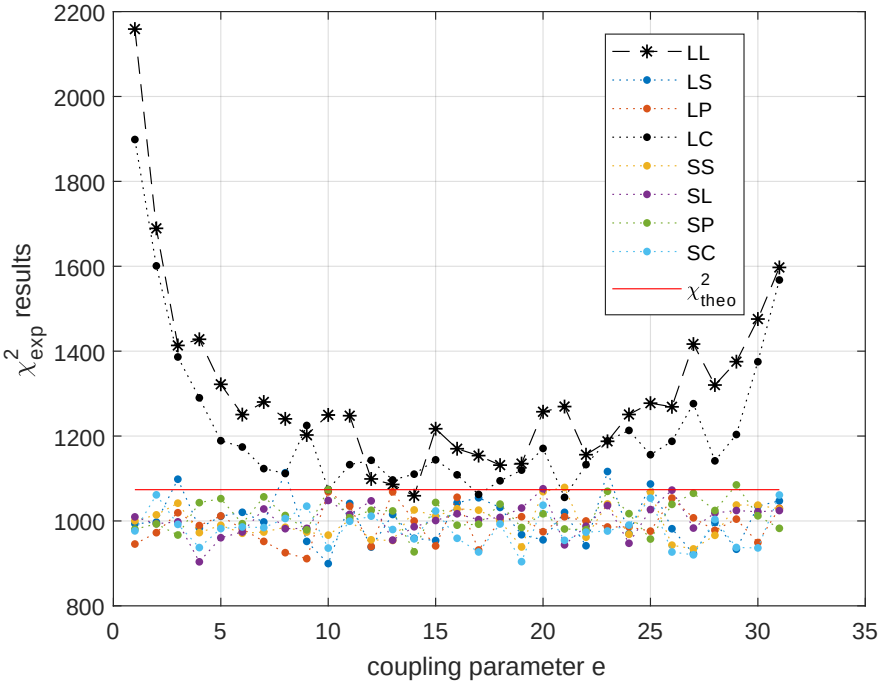
(a) Histogram of $X1$ of the coupling "LS" (b) Histogram of $X1$ of the coupling "LC"

FIGURE 6.7 – Histogram

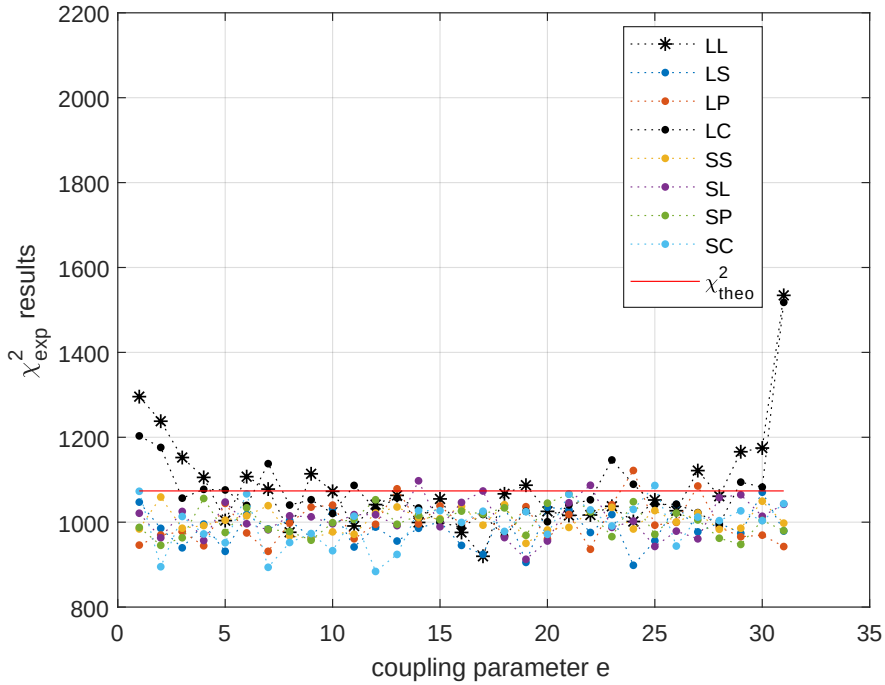
3. The initial conditions (IC) and parameters are chosen randomly (Ps, Pp is the parameter of skew tent map and PWLCM respectively) for the chaotic maps are : (1) logistic : IC1=1139372832, IC2=809731856 ; (2) skew tent map : IC1=3540669105, Ps1=3136394681, IC2=3543597725, PS2=4148523159 ; (3) PWLCM : IC=2067014358, Pp=1875378875 ; (4) Che3 : IC=893224612. The length of $X1, X2$ is 10^6.
For the test of period detection, the length of X1, X2 is 10^8.
Marker "✓" (or "×") means the produced sequences pass (or do not pass) the corresponding test in the table.

More precisely, to test the performance of uniform distribution, χ^2_{exp} test results of different coupling combinations versus parameter e have been displayed in Figure 6.8, from which we can observe that most of the combinations have shown good uniformity because their χ^2_{exp} values are smaller than the χ^2_{theo} value (i.e. 1073.64 shown in red curve), except for the coupling of "LL" and that of "LC". Most of the χ^2_{exp} values of coupling "LL" and coupling "LC" are bigger than the χ^2_{theo} value. Besides, we can also find that the χ^2_{exp} values of couplings "LL" and that of "LC" calculated in $X2$ are smaller than those in $X1$. That is because, in the coupling matrix **A**, the multipliers that produce $X2$ are bigger than those to produce $X1$. Bigger multipliers lead to a more complex multiplication operation, which can make the products more complex and thus have better uniformity (random-like) behavior.

Secondly, the coupling must "hide" the function of the original chaotic functions in the phase space. The sequences $X1$ generated by the representative couplings "LS" and "LC" have been plotted in the phase space in Figure.6.9(a) and Figure.6.9(b) respectively. Figure 6.9 has verified that, regardless of the different coupling combinations of the original chaotic maps, the coupling method using matrix **A** shown in Equation (6.5) and (6.7), is able to hide the generating function effectively.

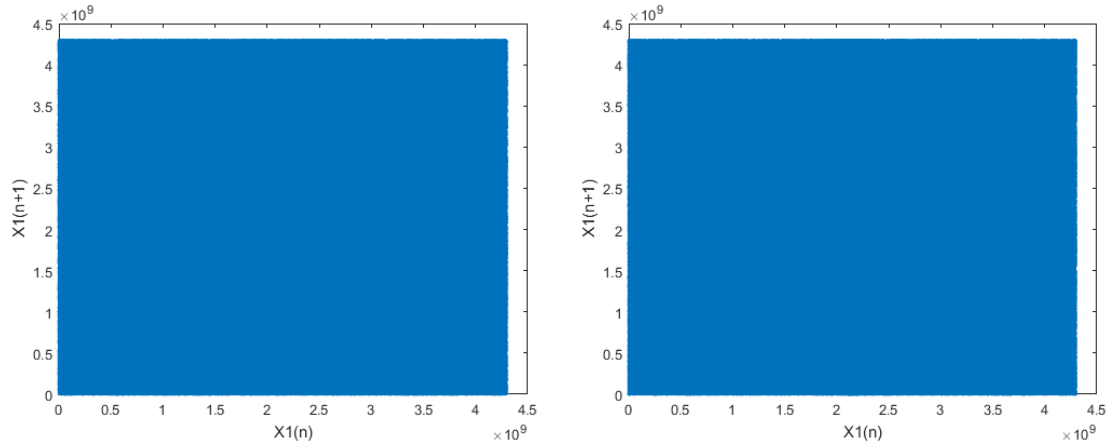


(a) Results of X1



(b) Results of X2

FIGURE 6.8 – χ^2_{exp} results versus the coupling parameter e



(a) $X1$ from coupling "LS" (b) $X1$ from coupling "LC"

FIGURE 6.9 – $X1$ in the phase space

Thirdly, no period is detected among all these generated sequences. Compared to the short period caused by the effect of finite precision shown in Section 3.3.1 in Chapter 3, the

coupling method (Equation (6.5), (6.7)) can render the output sequence $X1$ and $X2$ longer period to minimize the dynamical degradation.

In summary, the uniformity of the couplings "LL" and "LC" are not satisfactory owing to their both nonlinear derivative generating functions. The piece-wise linear functions (e.g. skew tent map and PWLCM) possess better uniformity than the nonlinear derivative functions (e.g. logistic map and Chebyshev 3rd order chaotic map), and this property can improve the overall uniformity of the coupled output sequence. But it's certain that this coupling method can improve the uniformity, hide the generating function and break the effects of finite precision effectively.

6.3 Three-dimensional coupling

Based on the analysis of 2D coupling matrix, an original 3D coupling matrix is proposed and it is described as below :

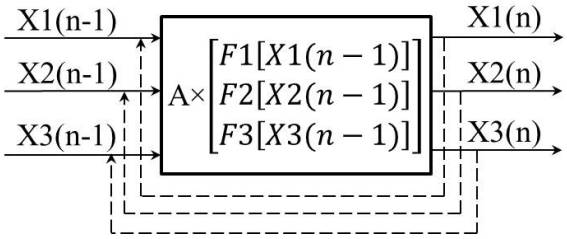


FIGURE 6.10 – 3D coupling structure

where $F1$, $F2$, $F3$ stand for chaotic maps ; $X1$, $X2$, $X3$ are the produced chaotic sequences ; $X1(n)$, $X2(n)$, $X3(n)$ means the $n-$th iterated states of $X1$, $X2$, $X3$.

The coupling matrix **A** is defined as follows :

$$\mathbf{A} = \begin{bmatrix} 2(2^{Ne}-1)+1-e1-e2 & e1 & e2 \\ 2e1 & 4(2^{Ne}-1)+1-2e1-2e2 & 2e2 \\ 3e1 & 3e2 & 6(2^{Ne}-1)+1-3e1-3e2 \end{bmatrix} \tag{6.8}$$

where two coupling parameters $e1, e2 \in \left[1, 2^{Ne}-1\right]$, and $Ne = 5$ bits.

The coupling algorithm can be described by :

$$\begin{bmatrix} X1\,(n) \\ X2\,(n) \\ X3\,(n) \end{bmatrix} = \mathbf{A} \times \begin{bmatrix} F1\,[X1\,(n-1)] \\ F2\,[X2\,(n-1)] \\ F3\,[X3\,(n-1)] \end{bmatrix} \tag{6.9}$$

As in the 2D coupling case, here different chaotic maps are combined to do the 3D coupling. The performance of different coupling combinations have been evaluated in terms of uniformity test (histogram and χ^2 test), phase space analysis and period detection. The results have been shown in Table 6.3.

TABLE 6.3 – Coupling performance of the produced sequence $X1$ [4]

Couplings	F1	F2	F3	Histogram and χ^2 test	Phase space	Period detection
LLL	Logistic	Logistic	Logistic	✓	✓	no period detected
LSP	Logistic	Skew tent	PWLCM	✓	✓	no period detected
SPC	Skew tent	PWLCM	Chebyshev 3rd order map	✓	✓	no period detected
SPS	Skew tent	PWLCM	Skew tent	✓	✓	no period detected
SSS	Skew tent	Skew tent	Skew tent	✓	✓	no period detected

Firstly, compared to the uniformity performance of 2D coupling summarized in Table 6.2 where coupling combinations "LL" and "LC" composed by nonlinear chaotic maps function cannot pass the uniformity test, Table 6.3 has shown that all the listed 3D couplings, including the combination of "LLL" whose chaotic map is the function with nonlinear derivative, are now able to pass the uniform distribution test. Thus, in the aspect of uniformity, 3D coupling can ensure uniform distribution property of the produced sequence $X1, X2, X3$ for any chaotic maps coupling combinations.

Taking the coupling combination "SPC" as an example, histogram of $X1$ is displayed in Figure 6.11, which has demonstrated its uniformity. Note that, $X2, X3$ produced by "SPC" as well as any $X1, X2, X3$ produced by other coupling combinations in Table 6.3 show the highly similar diagrams. Furthermore, the χ^2 test has been applied to the produced $X1, X2, X3$. The experimental χ^2 values χ^2_{exp} versus the coupling parameter $(e1, e2)$ have

4. $X2$, $X3$ show the same performance ; length of $X1, X2, X3$ is 10^6 ; for the test of period detection, length of $X1, X2, X3$ is 10^8.

been calculated and plotted in Figure 6.12, from which we can find that any $(e1, e2)$ can pass the χ^2 test and thus ensure the uniformity of the produced $X1, X2, X3$.

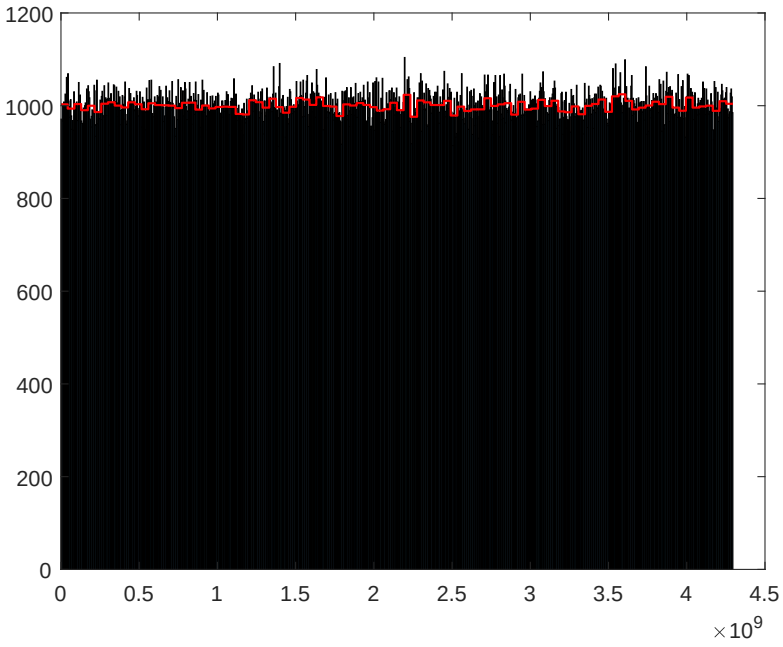
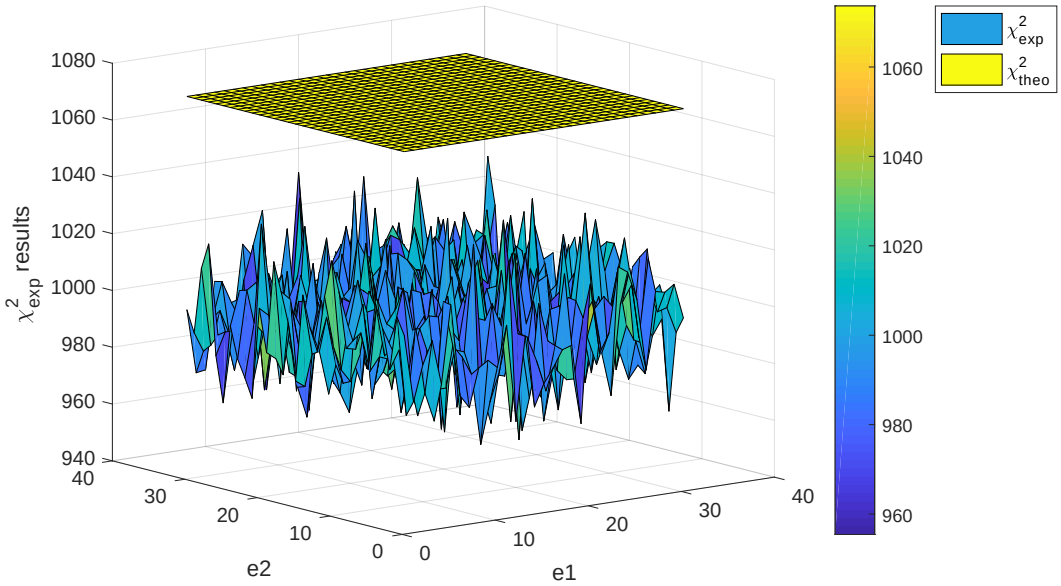
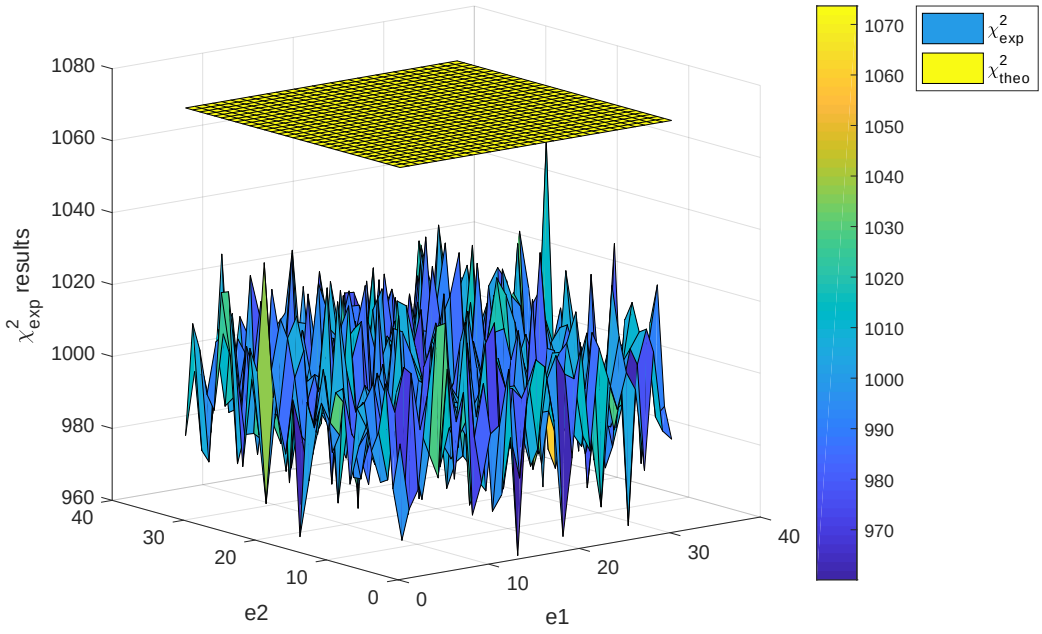


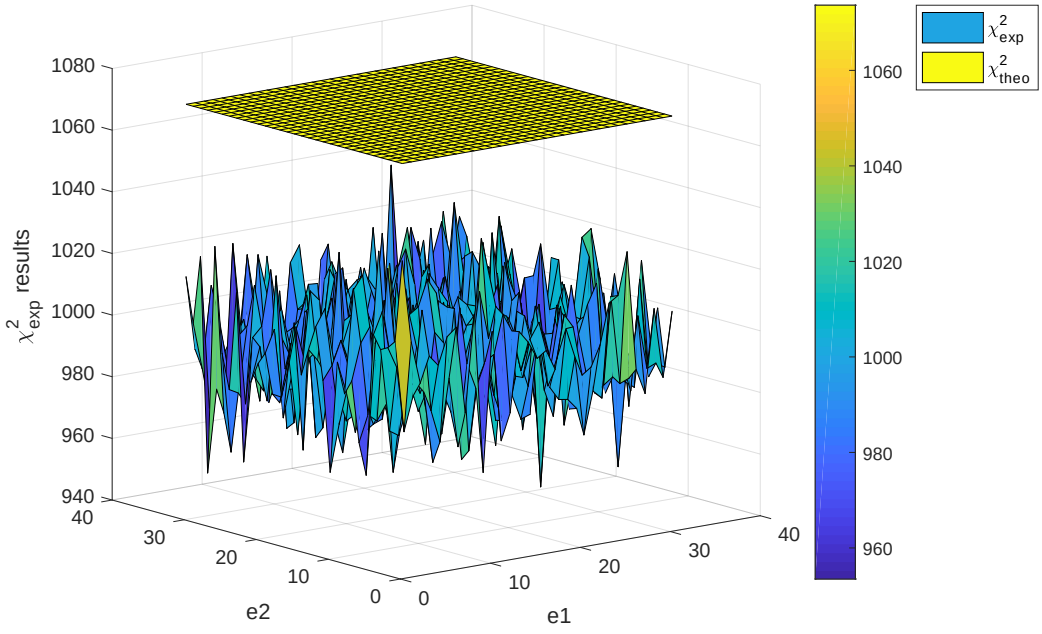
FIGURE 6.11 – Histogram of X1 generated by "SPC"



(a) χ^2 test results of X1



(b) χ^2 test results of X2



(c) χ^2 test results of X3

FIGURE 6.12 – χ^2_{exp} results in the coupling "SPC" versus the coupling parameter $(e1, e2)$ [6]

6. each χ^2_{exp} value is the average of ten χ^2_{exp} values obtained by repeating the coupling process ten times using ten randomly generated initial conditions.

Secondly, as can be seen from Figure 6.13 which has displayed the phase portrait of $X1$, the 3D coupling scheme can hide the generating function of the used chaotic maps effectively.

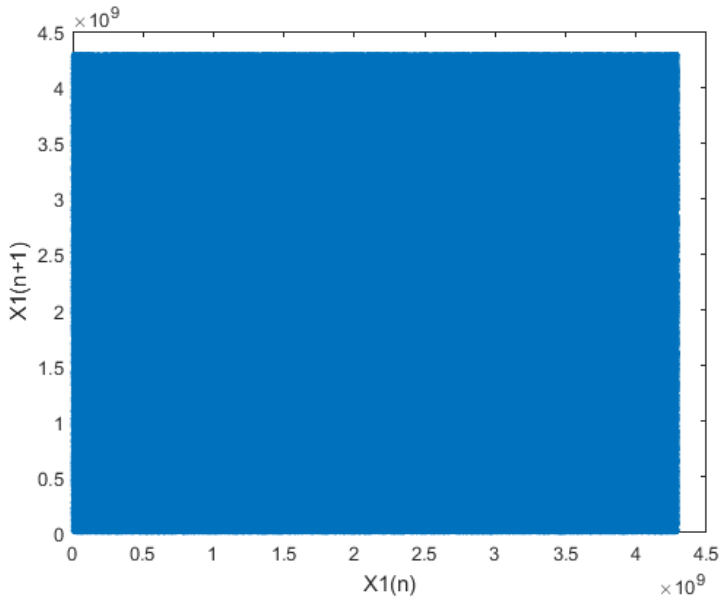


FIGURE 6.13 – Phase space of X1 generated by "SPC" [7]

In addition, no period has been detected among the generated sequences. Hence, the 3D coupling also can minimize the dynamical degradation caused by the finite precision and lengthen the period over the finite field effectively.

6.4 PRNG scheme based on chaotic coupling

Section 6.2 and Section 6.3 have proven that the coupling scheme (Figure 6.4, Figure 6.10) can greatly improve the randomness of the sequences that are generated by the original chaotic maps. Based on the coupling method, a chaos-based PRNG design framework will be presented in this section. Using the proposed framework, a new family of PRNG schemes can be put forward.

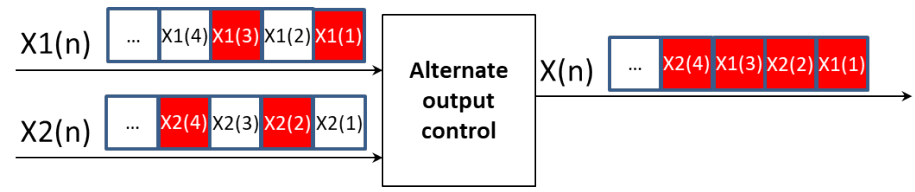
7. X2, X3 show the highly similar diagrams ; initial conditions (IC) and parameters(P) for the chaotic maps are chosen randomly ; (1) skew tent map :IC=1318743397, P=3916945839 ; (2) PWLCM : IC=1125663524,P=260726438 ; (3) Chebyshev 3-order chaotic map : IC=1701137509 ; e1=14 ; e2=17.

To increase the complexity and unpredictability of PRNGs, two types of output control methods will be proposed in the following and they will be applied to the sequences $X1, X2, X3$ to form the final pseudo-random numbers.

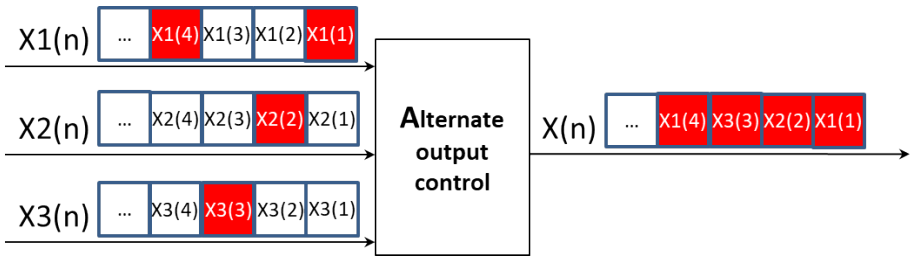
6.4.1 Two types of output control

Alternate output control

The first type of output control is named as "alternate output control". It selects each number between $X1(n)$ and $X2(n)$ (and $X3(n)$ if it is based on 3D coupling) alternatively to form the final pseudo-random sequence X. The alternate output control concept can be described by Figure 6.14.



(a) for 2D coupling scheme



(b) for 3D coupling scheme

FIGURE 6.14 – Alternate output control

The alternate output control method obeys a fixed rule to form the final output X. It selects $X1(n)$ and $X2(n)$ (and $X3(n)$, if it is based on 3D coupling scheme) in turn by an equal probability (50% for 2D coupling, 33.33% for 3D coupling).

Dynamic output control

It is preferable if there is a more complicated selection mode to increase its complexity and unpredictability. Thus, the dynamic output control is a good option.

Dynamic output control method can be described by Figure 6.15. This idea came from the work [120, 170] and it has been used to increase the randomness property of the PRNG design [123, 159]. We have also used this kind of output control method in Chapter 4.

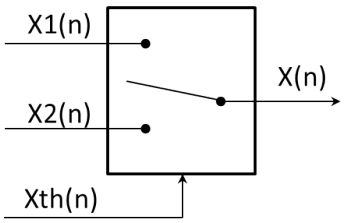


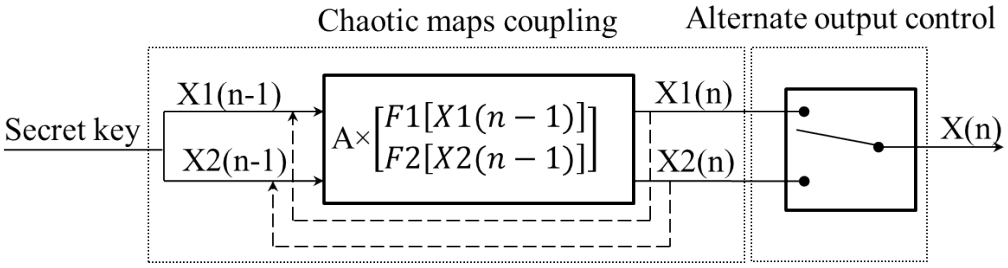
FIGURE 6.15 – Dynamic output control

Dynamic output control method selects $X1(n)$ and $X2(n)$ according to a decision sample $Xth(n)$ with a threshold Th. $Xth(n)$ can be considered as a dynamic parameter to switch between $X1(n)$ and $X2(n)$. This can be achieved by :

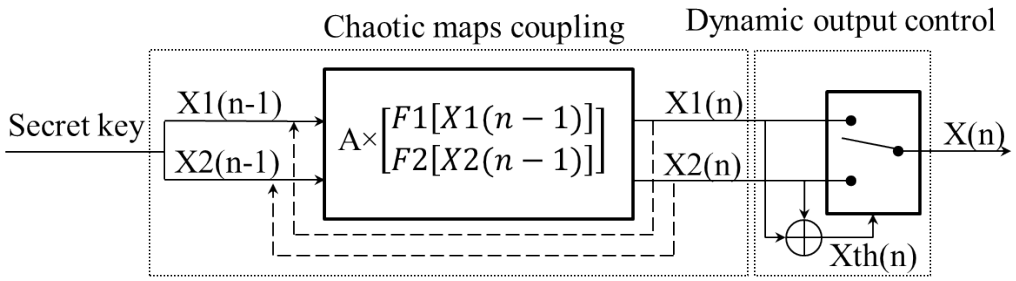
$$X\left(n\right)=\begin{cases}X1\left(n\right) & if\ Xth\left(n\right)>Th\\ X2\left(n\right) & otherwise\end{cases} \tag{6.10}$$

6.4.2 PRNG based on two-dimensional coupling

The PRNG using alternate output control method and dynamic output control method are described in Figure 6.16.



(a) using alternate output control method



(b) using dynamic output control method

FIGURE 6.16 – PRNG scheme based on 2D coupling

where $F1,\ F2$ means two chaotic maps. In Figure 6.16(a), $X(n)$ is formed by selecting $X1(n)$ and $X2(n)$ in turn alternatively. While in Figure 6.16(b), $X(n)$ is formed by Equation (6.10), where $Xth(n) = X1(n) \oplus X2(n)$ ($\oplus$ is an XOR operator) and $Th = 0.7 \times 2^N$ ($N = 32$).

Security test

If PRNG is used in cryptography, besides the randomness property, security performance becomes the primary requirement. A large key space and high sensitivity to secret key are two important security properties of a PRNG.

Firstly, the key space of a cryptosystem should be bigger than 2^{128} to resist the brute-force attack. Initial conditions and parameters of the used chaotic maps and the coupling parameter (e) constitute the secret key. Recalling the different coupling combinations in Table 6.2, the key spaces are calculated in Table 6.4. Only the couplings "SP" and "SS" meet the key space requirement. Thus, these two couplings can be chosen to design the PRNG. Note that, other couplings also can be used to design PRNGs, but they need to be paralleled to enlarge the key space.

Secondly, the sensitivity to secret key can be evaluated by the Hamming distance (D_H) :

$$D_H(X, Y) = \frac{1}{|lb|} \times \sum_{k=1}^{|lb|} (X[k] \oplus Y[k]) \tag{6.11}$$

where X, Y are two produced sequences whose secret keys are just one bit different. The bit length of X, Y is $|lb|$. $\oplus$ denotes the XOR operator.

Here, 100 randomly generated secret keys have been used to produce 100 output sequences X. Changing one bit randomly in each secret key produces a corresponding se-

quence Y. D_H has been calculated between each pair of X and Y. The average D_H over 100 D_Hs has been computed for the coupling "SP" and "SS" in Table 6.4. $D_H = 50\%$ is the optimal value meaning the bit change probability is 50%. D_Hs recorded in Table 6.4 are very close to 50% demonstrating that the high sensitivity of the produced sequence X to even a tiny change in the secret key has been achieved.

TABLE 6.4 – Security test results

Couplings	Key space	Key sensitivity ($D_H(\%)$)	
		Alternate output control	Dynamic output control
LL	2^{69} ×	-	-
LS	2^{101} ×	-	-
LP	2^{100} ×	-	-
LC	2^{69} ×	-	-
SL	2^{101} ×	-	-
SC	2^{101} ×	-	-
SP	2^{132} ✓	50.0010 ✓	50.0009 ✓
SS	2^{133} ✓	49.9996 ✓	50.0000 ✓

Statistical test

Statistical tests including uniformity (histogram and χ^2 test), phase portrait, period detection and NIST randomness test have been performed and the results of the couplings "SP" and "SS" have been summarized in Table 6.5 and Table 6.6. The NIST test results of the coupling "SS" have been shown in Table 6.7.

TABLE 6.5 – Statistical test results (alternate output method)

Couplings	Histogram	χ^2_{exp}	Phase space	Period detection	NIST test
SP	✓	1010.22 ✓	✓	no period detected	✓
SS	✓	1003.04 ✓	✓	no period detected	✓

TABLE 6.6 – Statistical test results (dynamic output method)

Couplings	Histogram	χ^2_{exp}	Phase space	Period detection	NIST test
SP	✓	1008.27 ✓	✓	no period detected	✓
SS	✓	995.87 ✓	✓	no period detected	✓

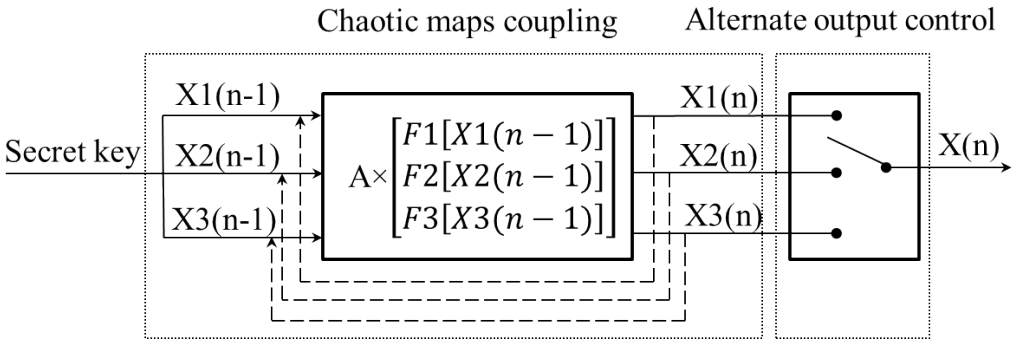
TABLE 6.7 – NIST test results(coupling "SS")

Tests	Alternate output control		Dynamic output control		Result
	P-value	Proportion(%)	P-value	Proportion(%)	
Frequency	0.456	97.000	0.035	96.000	Pass
Block-frequency	0.868	100.000	0.658	99.000	Pass
Cumulative-sums	0.630	98.000	0.263	97.000	Pass
Runs	0.182	99.000	0.024	99.000	Pass
Longest-run	0.760	97.000	0.637	99.000	Pass
Rank	0.304	99.000	0.012	100.000	Pass
FFT	0.817	99.000	0.494	99.000	Pass
Non-overlapping template	0.524	99.034	0.451	98.993	Pass
Overlapping template	0.616	99.000	0.779	99.000	Pass
Universal	0.276	100.000	0.122	100.000	Pass
Approximate entropy	0.740	100.000	0.514	100.000	Pass
Random-excursions	0.535	99.167	0.606	98.542	Pass
Random-excursions-variant	0.449	99.074	0.422	99.537	Pass
Serial	0.269	98.500	0.332	100.000	Pass
Linear-complexity	0.475	100.000	0.384	98.000	Pass

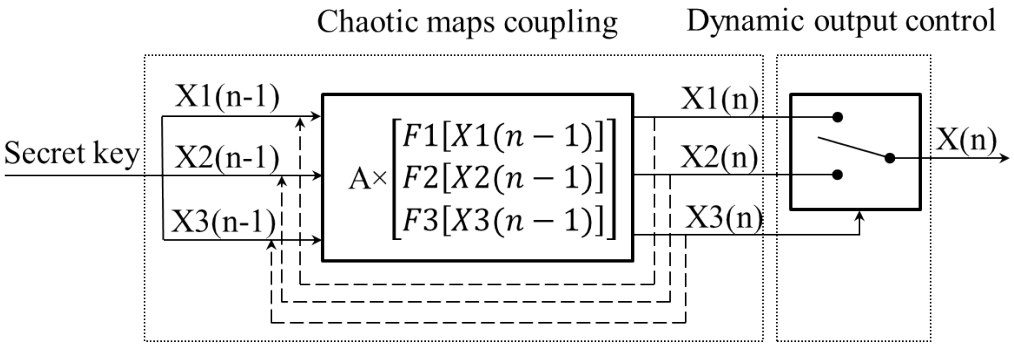
All these test results have demonstrated that both the alternate output method and dynamic output method can produce pseudo-random sequences.

6.4.3 PRNG based on three-dimensional coupling

Based on the 3D coupling (Figure 6.10, Equation (6.8)), the PRNG scheme is shown in Figure 6.17. It has the similar definitions with Figure 6.16.



(a) using alternate output control method



(b) using dynamic output control method

FIGURE 6.17 – PRNG scheme based on 3D coupling

Security test

According to Table 6.8 which clearly shows the key space and secret key sensitivity of different coupling combinations, the PRNG scheme of Figure 6.17 can provide lager key space when compared to the PRNG using 2D coupling shown in Figure 6.16. In addition, the obtained D_Hs, using the same test method described for Table 6.4, have demonstrated the high sensitivity of the PRNGs to their secret key.

TABLE 6.8 – Security test results

Couplings	Key space	Key sensitivity ($D_H(\%)$)	
		Alternate output control	Dynamic output control
LLL	$2^{101}\times$	-	-
LSP	$2^{164}\checkmark$	49.9989 ✓	49.9996 ✓
SPC	$2^{164}\checkmark$	49.9983 ✓	49.9998✓
SPS	$2^{196}\checkmark$	50.0001 ✓	49.9987✓
SSS	$2^{197}\checkmark$	50.0006 ✓	50.0004 ✓

Statistical test

Similar to Table 6.5 and Table 6.6 when we were analyzing the PRNGs based on 2D coupling scheme, the statistical test results shown in Table 6.9 and Table 6.10 have proven that the PRNG (Figure 6.17) based on 3D coupling scheme (Figure 6.10) using either output method (alternate output control or dynamic output control) can produce pseudo-random numbers. The NIST randomness test results of the couplings "SPC" and "SSS" have been

shown in Table 6.11 and Table 6.12, which have demonstrated the satisfactory randomness of the produced pseudo-random sequence X.

TABLE 6.9 – Statistical test results (alternate output method)

Couplings	Histogram	χ^2_{exp}	Phase space	Period detection	NIST test
LSP	✓	1012.66 ✓	✓	no period detected	✓
SPC	✓	1001.82 ✓	✓	no period detected	✓
SPS	✓	992.58 ✓	✓	no period detected	✓
SSS	✓	1001.87 ✓	✓	no period detected	✓

TABLE 6.10 – Statistical test results (dynamic output method)

Couplings	Histogram	χ^2_{exp}	Phase space	Period detection	NIST test
LSP	✓	1019.48 ✓	✓	no period detected	✓
SPC	✓	999.17 ✓	✓	no period detected	✓
SPS	✓	997.09 ✓	✓	no period detected	✓
SSS	✓	992.73 ✓	✓	no period detected	✓

TABLE 6.11 – NIST test results (coupling "SPC")

Tests	Alternate output control		Dynamic output control		Result
	P-value	Proportion(%)	P-value	Proportion(%)	
Frequency	0.760	98.000	0.437	100.000	Pass
Block-frequency	0.834	98.000	0.817	99.000	Pass
Cumulative-sums	0.385	99.000	0.812	99.500	Pass
Runs	0.304	100.000	0.401	99.000	Pass
Longest-run	0.154	100.000	0.999	99.000	Pass
Rank	0.554	98.000	0.059	98.000	Pass
FFT	0.475	97.000	0.596	100.000	Pass
Non-overlapping template	0.477	99.000	0.459	98.986	Pass
Overlapping template	0.851	99.000	0.972	99.000	Pass
Universal	0.740	100.000	0.367	100.000	Pass
Approximate entropy	0.983	100.000	0.401	99.000	Pass
Random-excursions	0.486	99.590	0.310	99.254	Pass
Random-excursions-variant	0.377	99.180	0.336	99.171	Pass
Serial	0.749	99.500	0.477	98.500	Pass
Linear-complexity	0.798	99.000	0.055	99.000	Pass

TABLE 6.12 – NIST test results (coupling "SSS")

Tests	Alternate output control		Dynamic output control		Result
	P-value	Proportion(%)	P-value	Proportion(%)	
Frequency	0.182	98.000	0.817	99.000	Pass
Block-frequency	0.202	99.000	0.040	98.000	Pass
Cumulative-sums	0.623	98.500	0.429	98.500	Pass
Runs	0.514	100.000	0.575	98.000	Pass
Longest-run	0.335	98.000	0.779	98.000	Pass
Rank	0.401	100.000	0.798	98.000	Pass
FFT	0.401	97.000	0.437	98.000	Pass
Non-overlapping template	0.495	99.068	0.512	99.095	Pass
Overlapping template	0.067	99.000	0.011	99.000	Pass
Universal	0.046	100.000	0.596	99.000	Pass
Approximate entropy	0.059	99.000	0.936	99.000	Pass
Random-excursions	0.735	97.817	0.451	99.632	Pass
Random-excursions-variant	0.416	98.413	0.350	99.101	Pass
Serial	0.400	99.000	0.374	99.000	Pass
Linear-complexity	0.514	99.000	0.699	99.000	Pass

6.5 Key space expandable PRNG

The PRNG based on 2D coupling is limited to 2^{133} that is achieved by using the coupling combination "SS" (coupling two skew tent map). Many other combinations have to operate in parallel structure to obtain a larger key space. Although, in general, the PRNG based on 3D coupling can provide larger key space, collision of equivalent secret key over a finite field is inevitable, which will shrink the effective key space and thus bring security risks. Furthermore, with the development of computer technology, computing speed is rapidly increasing. Thus, a larger key space is expected to prevent the brute-force attack and ensure a high security of a cryptosystem.

For this, a new key space expandable PRNG scheme is proposed in this section. This scheme not only expands the key space of the PRNG leading to an enhanced immunity against the brute-force attack, but also increases the system's complexity and security performance.

Taking the 2D coupling "SS" with dynamic output method as an example, the proposed

key space expandable PRNG scheme is shown in Figure 6.18.

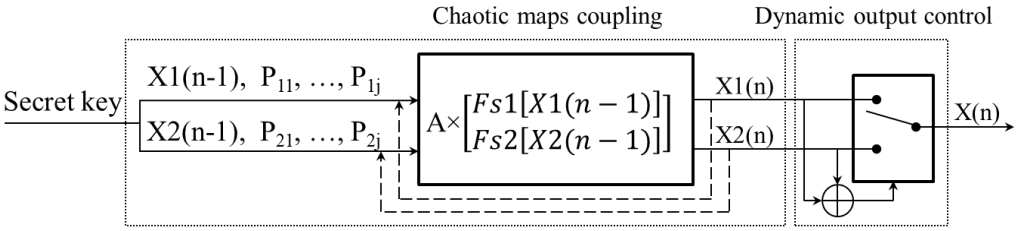


FIGURE 6.18 – Key space expandable PRNG scheme

where $Fs1$, $Fs2$ are two skew tent maps.

For $Fs1$ and $Fs2$, their corresponding initial conditions are $X1(0)$ and $X2(0)$. Their parameters are $P_{11}, ..., P_{1j}$ and $P_{21}, ..., P_{2j}$, where j is the number of parameters used in each skew tent map, and $j = 1, 2, 3, 4, ...$ The parameters are used one by one in $Fs1$ and $Fs2$. That is, when $j = 1$, P_{11} is the only parameter of $Fs1$ and P_{21} is the only parameter of $Fs2$ (i.e. coupling "SS" in Section 6.4.2) ; when $j = 2$, P_{11}, P_{12} are used in turn in $Fs1$, and P_{21}, P_{22} are used in turn in $Fs2$; similarly, when $j = 4$, P_{11}, P_{12}, P_{13}, P_{14} and P_{21}, P_{22}, P_{23}, P_{24} are used in turn in $Fs1$ and $Fs2$. All the initial conditions and parameters compose the secret key of the PRNG.

Security test

For different j, the key size is calculated as :

$$|K_j| = |X1\,(0)| + |P_{11}| \times j + |X2\,(0)| + |P_{21}| \times j + |e| \tag{6.12}$$

where the size of the initial conditions ($|X1(0)|$,$|X2(0)|$) and parameters ($|P_{11}|$,$|P_{21}|$) for $Fs1$ and $Fs2$ are $N = 32$ bits, and the size of coupling parameter ($|e|$) is $Ne = 5$ bits.

We have calculated the key space for $j = 1, 2, 3, 4$ and the results have been listed in Table 6.13. The key spaces of the PCNGs have been expanded effectively, which enhance the resistance to brute-force attack.

In addition, key sensitivity is evaluated by D_H for $j = 1, 2, 3, 4$. Using the same calculation method described for Table 6.4, the obtained D_Hs shown in Table 6.13 are very close to 50%, which have confirmed the high sensitivity of the PRNGs to their secret key.

Statistical test

The results are similar to the previous conducted experiments regarding to the statistical test. The test results shown in Table 6.13 have demonstrated that the produced sequences by the PRNG scheme of Figure 6.18 can pass the uniformity test (histogram and χ^2 test), hide the used chaotic function in phase space and exhibit longer period. NIST test results when $j = 2, 3, 4$ have been shown in Table 6.14 and Table 6.15. All the results have confirmed the good randomness and higher security (larger key space) of the proposed PRNG scheme.

TABLE 6.13 – Security and statistical test results

j	Security test		Statistical test			
	Key space	Key sensitivity ($D_H(\%)$)	Histogram and χ^2 test	Phase space	Period detection	NIST test
1	2^{133} ✓	50.0000 ✓	995.87 ✓	✓	no period detected	✓
2	2^{197} ✓	49.9996 ✓	1012.47 ✓	✓	no period detected	✓
3	2^{261} ✓	49.9991 ✓	993.92 ✓	✓	no period detected	✓
4	2^{325} ✓	49.9995 ✓	994.28 ✓	✓	no period detected	✓

TABLE 6.14 – NIST test results (j=2,3)

Test	j=2		j=3		Result
	P-value	Proportion(%)	P-value	Proportion(%)	
Frequency	0.163	98.000	0.049	100.000	Pass
Block-frequency	0.091	100.000	0.798	100.000	Pass
Cumulative-sums	0.790	98.500	0.471	100.000	Pass
Runs	0.163	98.000	0.616	97.000	Pass
Longest-run	0.097	98.000	0.122	100.000	Pass
Rank	0.851	99.000	0.475	98.000	Pass
FFT	0.851	99.000	0.154	100.000	Pass
Non-overlapping template	0.534	98.980	0.478	99.014	Pass
Overlapping template	0.276	100.000	0.868	98.000	Pass
Universal	0.616	100.000	0.554	96.000	Pass
Approximate entropy	0.616	99.000	0.575	99.000	Pass
Random-excursions	0.477	98.148	0.589	98.134	Pass
Random-excursions-variant	0.465	99.691	0.378	98.756	Pass
Serial	0.281	99.500	0.278	100.000	Pass
Linear-complexity	0.103	98.000	0.043	97.000	Pass

TABLE 6.15 – NIST test results (j=4)

Test	j=4		Result
	P-value	Proportion(%)	
Frequency	0.575	100.000	Pass
Block-frequency	0.740	98.000	Pass
Cumulative-sums	0.319	100.000	Pass
Runs	0.182	99.000	Pass
Longest-run	0.658	98.000	Pass
Rank	0.575	98.000	Pass
FFT	0.798	100.000	Pass
Non-overlapping template	0.488	99.101	Pass
Overlapping template	0.419	99.000	Pass
Universal	0.596	99.000	Pass
Approximate entropy	0.514	100.000	Pass
Random-excursions	0.342	98.713	Pass
Random-excursions-variant	0.256	98.856	Pass
Serial	0.304	99.000	Pass
linear-complexity	0.437	100.000	Pass

Note that the proposed PRNG scheme (Figure 6.18) is not restricted to the working mode described above. It can be considered as a flexible framework which can be used to produce much more different pseudo-random sequences. The flexibility can be seen in the following aspects : (1) any number of j can be chosen to design the PRNG ; (2) it holds not only for the skew tent map, the coupling scheme is also suitable for coupling different piecewise linear chaotic maps ; (3) for the output control, other control methods are also applicable (e.g. output X1(n), X2(n) alternatively ; using XOR operation between a circular shifted X1 and X2).

6.6 Conclusion

PRNG plays an important role not only in the security of a cryptosystem, but also in other various engineering fields. In this chapter, we have proposed a smart coupling of chaotic maps over a finite integer field, and based on the coupling method, a new family of PRNGs has been investigated.

Our coupling method is inspired by the idea of ultra-weak coupling that is defined over

a real continuous number field. However, due to the fact that the coupling is quite weak, the chaotic function still can be recognized by analyzing the output of the coupling structure in a phase space. This is a security drawback when the coupling structure is applied in a cryptosystem.

The ultra-weak coupling structure cannot be copied to an integer number field directly. However, if the coupling is defined in the integer number field, a tiny change in the coupling matrix will lead to a big difference in the produced sequence. Thus, the coupling matrix has been analyzed in detail in this chapter and finally we have proposed effective 2D and 3D coupling matrices in the 2D and 3D coupling schemes. The statistical experiment results have indicated that 2D and 3D coupling schemes can improve the randomness of the used chaotic maps effectively and overcome the drawback of leakage of chaotic map's function existed in the real domain defined ultra-weak coupling structure.

Based on the 2D and 3D coupling schemes, a family of PRNGs have been proposed. Different chaotic maps coupling combinations can compose the PRNG. In addition, alternate and dynamic output control methods have been presented to increase the complexity of the PRNGs and enhance the unpredictability and randomness of the produced pseudo-random sequences. Conducted security and statistical test results have verified the high reliability of applying the proposed PRNGs in cryptosystems or other PRNG required applications.

Besides, considering the key space is a limit of using 2D coupling scheme to PRNG design and it is not easy to figure out the precise effective key space, a key expandable PRNG strategy has been proposed. The expanded key space not only enhances the resistance ability of cryptosystems to the brute-force attack, but also increases complexity of the PRNG and improves the random-like features of the produced pseudo-random sequences.

Furthermore, all PCNGs employ the reformulated chaotic maps over the 32-bit finite integer field, which overcomes the security problems caused by applying the floating-point numbers to the finite precision digital software/hardware situations. Thus, they ensure the good performance of the pseudo-random numbers over different platforms and a high reliability of the PRNGs.

CHAPITRE 7

CONCLUSION AND PERSPECTIVES

7.1 Conclusion of contributions

In this thesis, we focus on the issue of using chaotic dynamics in cryptography aiming to design secure and reliable chaos-based cryptosystems and PRNGs.

Chaotic dynamics is a special behavior in nonlinear dynamical system. The natural advantages of the chaotic system, namely complex property, random-like behavior and high sensitivity to initial conditions and parameters, make it very suitable for cryptographic applications.

In Chapter 1, we have introduced the fundamentals of chaotic dynamics, which, on one hand, explained the excellent chaotic features such as complex dynamics, random-like behavior and high sensitivity to the initial conditions that are suitable for encryption purposes, and on the other hand, analyzed the singularities such as fixed points, periodic points that should be avoided carefully in cryptosystem design.

The basis of chaos-based cryptosystems and the state of the art have been analyzed in Chapter 2. In the literature analysis, we have discussed the existing problems and solutions. However, we are still facing many problems regarding to the security of cryptosystems that need to be solved, such as insufficient confusion and diffusion properties, insecure and not complex enough confusion and diffusion strategy, undependable key stream and PCNG, the dynamical degradation problem, etc. To overcome the existing problems and enhance the security of cryptosystems, effective methods and secure chaos-based cryptosystems have been proposed in this thesis. The contributions can be summarized as follows.

Firstly, in Chapter 3, four widely used discrete chaotic maps (logistic map, skew tent map, PWLCM and Chebyshev 3rd order chaotic map) have been redefined over a finite integer field, which is used to overcome the security breach caused by applying quantization, truncation or round-off approaches to the real number defined chaotic maps to satisfy the finite precision nature of the digital devices. The 32-bit finite precision is used, which not only makes the proposed cryptosystems or PCNGs can be implemented in different

platforms and guarantees the reliability of the systems, but also uses reduced hardware resources since the proposed schemes are more hardware friendly when compared to the most existing cryptosysytems that used the real number with double precision.

Chaotic maps with finite precision will definitely show dynamical degradation (finite period orbits). To overcome this drawback, a secure PCNG with ease of implementation has been proposed in Chapter 4. Based on the PCNG, a new efficient stream cipher has been developed. The conducted experiment results have verified the efficiency and security of the stream cipher.

A new secure and robust chaos-based image cryptosystem based on confusion and diffusion concept has been proposed in Chapter 5. It works with a global diffusion operation and a block cipher which is based on the AES S-box. The key stream, provided by a new designed PCNG, exhibits good security and randomness. Attackers cannot find the secret key by analyzing the key stream. This system has excellent confusion and diffusion properties, which possesses highly resistance to the common attacks.

The importance of PCNG has been embodied in the previous two chapters. Apart from the vital function that PCNG plays in the chaos-based cryptosystems, PCNG is basically a PRNG. PRNGs are important tools in plethora of applications involving various research and engineering fields. In Chapter 6, we have proposed a more reliable PRNG framework which is mainly based on a smart coupling structure and a output control method. The smart coupling can break the original orbits of the used chaotic maps, lengthen the period to minimize the bad effect of finite precision and make the output sequence possess uniformity and randomness property. Two output control methods, i.e. alternate output method and dynamic output method, have been introduced to select the sequences produced by the coupling structure to generate the final pseudo-random numbers. This operation increases the complexity and unpredictability of the PCNG. The security tests and statistical tests have been applied to the proposed PRNGs. The obtained results have demonstrated the excellent performances in terms of security and randomness of the PRNGs. Furthermore, the key space is a limit when 2D coupling structure is used in PRNG design. A key space expandable PRNG strategy has been described in this chapter. It can enlarge the key space effectively, which gives a solution to using 2D coupling to PRNG design and increase greatly the resistance to the brute-force attack.

7.2 Perspectives of future work

For the future work, the following lists several suggestions based on the proposition presented in the thesis.

The proposed PCNGs, the chaos-based stream cipher and the chaos-based block cipher in the thesis are implemented by MATLAB. But MATLAB cannot give the dependable time consumption performance of the proposed systems, especially in the case of calculating the big integer numbers that we used. Therefore, although the fully theoretical analyses and conducted simulations results have confirmed the good performance of the proposed systems, further hardware implementations are expected to verify their computational performance.

Besides, for the period detection of the proposed PRNGs in Chapter 6, theoretically, due to enhanced complex dynamics achieved by the coupling scheme and the output control operations, PRNGs can produce pseudo-random sequences with very long periods. But restricted by the software implementation, we can only verify that there is no period in the produced pseudo-random sequences up to 10^8 length (3.2×10^9 bit length). The period of the produced sequences by the proposed PRNGs can be tested using other operation environments in order to provide definite evidences that the PRNGs can generate pseudo-random sequences with extremely long period.

In addition, in this thesis, we focused on using chaotic dynamics in improving the security of symmetric-key encryption algorithm. But the chaotic features also can be used in asymmetric-key encryption systems. Chebyshev polynomials, for instance, possess chaotic characteristics and semigroup property. We only analyzed and used Chebyshev 3rd order map in our work, but it is worthy more work in exploring its attractive characteristics in the design of asymmetric-key encryption algorithms.

Furthermore, in the study of information security, chaotic dynamics also play a promising and active role in the research of fractional PCNG design, cryptographic hash function (message digest), steganography and watermarking technique,etc. With the high development of information technology and computer science, computing speed will become faster and faster, which accelerates the cryptanalysis advances and that will render any cryptographic mechanism or algorithm insecure. Therefore, facing increasingly huge amount of confidential information, it is a significant subject to establish a better dialogue between chaos and information security, and to explore more efficient and secure technology to ensure information security.

BIBLIOGRAPHIE

[1] M. Usama, M. K. Khan, K. Alghathbar, and C. Lee, "Chaos-based secure satellite imagery cryptosystem," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 326–337, 2010.

[2] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied soft computing*, vol. 11, no. 1, pp. 514–522, 2011.

[3] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Processing : Image Communication*, vol. 29, no. 5, pp. 618–627, 2014.

[4] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International journal of bifurcation and chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[5] J. S. Teh, M. Alawida, and Y. C. Sii, "Implementation and practical problems of chaos-based cryptography revisited," *Journal of Information Security and Applications*, vol. 50, p. 102421, 2020.

[6] L. Abraham and N. Daniel, "Secure image encryption algorithms : A review," *International journal of scientific & technology research*, vol. 2, no. 4, pp. 186–189, 2013.

[7] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dynamics*, vol. 92, no. 2, pp. 305–313, 2018.

[8] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K.-T. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing : Image Communication*, vol. 23, no. 3, pp. 212–223, 2008.

[9] C. Li and K.-T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal processing*, vol. 91, no. 4, pp. 949–954, 2011.

[10] M. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 407–425, 2017.

[11] D. Lambić and M. Nikolić, "Pseudo-random number generator based on discrete-space chaotic map," *Nonlinear Dynamics*, vol. 90, no. 1, pp. 223–232, 2017.

[12] E. S. Overman, "The new science of management : Chaos and quantum theory and method," *Journal of Public Administration Research and Theory*, vol. 6, no. 1, pp. 75–89, 1996.

[13] J. Gleick, *Chaos : Making a new science*. Open Road Media, 2011.

[14] H. Poincaré, "Sur le problème des trois corps et les équations de la dynamique," *Acta mathematica*, vol. 13, no. 1, pp. A3–A270, 1890.

[15] H. Poincaré, *The three-body problem and the equations of dynamics : Poincaré's foundational work on dynamical systems theory*, vol. 443. Springer, 2017.

[16] F. Diacu and P. Holmes, *Celestial encounters : the origins of chaos and stability*, vol. 22. Princeton university press, 1999.

[17] D. Salamon, "The Kolmogorov-Arnold-Moser theorem," *Math. Phys. Electron. J*, vol. 10, no. 3, pp. 1–37, 2004.

[18] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the atmospheric sciences*, vol. 20, no. 2, pp. 130–141, 1963.

[19] Sharkovskiĭ, "Coexistence of cycles of a continuous map of the line into itself,"

[20] D. Ruelle and F. Takens, "On the nature of turbulence," *Les rencontres physiciens-mathématiciens de Strasbourg-RCP25*, vol. 12, pp. 1–44, 1971.

[21] S. Smale *et al.*, "Differentiable dynamical systems," *Bulletin of the American mathematical Society*, vol. 73, no. 6, pp. 747–817, 1967.

[22] T.-Y. Li and J. A. Yorke, "Period three implies chaos," *The American Mathematical Monthly*, vol. 82, no. 10, pp. 985–992, 1975.

[23] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[24] P. Myrberg, "Sur l'itération des polynomes réels quadratiques," *J. Math. Pures Appl.(9)*, vol. 41, pp. 339–351, 1962.

[25] R. L. Devaney, P. B. Siegel, A. J. Mallinckrodt, and S. McKay, "A first course in chaotic dynamical systems : theory and experiment," *Computers in Physics*, vol. 7, no. 4, pp. 416–417, 1993.

[26] R. L. Devaney, "An introduction to chaotic dynamical systems," 1989.

[27] L. Billings and E. Bollt, "Probability density functions of some skew tent maps," *Chaos, Solitons & Fractals*, vol. 12, no. 2, pp. 365–376, 2001.

[28] K. Belkhodja, A. Moussaoui, and M. A. Alaoui, "Optimal harvesting and stability for a prey–predator model," *Nonlinear Analysis : Real World Applications*, vol. 39, pp. 321–336, 2018.

[29] I. Sushko, V. Avrutin, and L. Gardini, "Bifurcation structure in the skew tent map and its application as a border collision normal form," *Journal of Difference Equations and Applications*, vol. 22, no. 8, pp. 1040–1087, 2016.

[30] K. Feltekh, D. Fournier-Prunaret, and S. Belghith, "Analytical expressions for power spectral density issued from one-dimensional continuous piecewise linear maps with three slopes," *Signal processing*, vol. 94, pp. 149–157, 2014.

[31] E. Schöll, *Nonlinear spatio-temporal dynamics and chaos in semiconductors*, vol. 10. Cambridge University Press, 2001.

[32] D. Lathrop, "Nonlinear dynamics and chaos : With applications to physics, biology, chemistry, and engineering," *Physics Today*, vol. 68, no. 4, p. 54, 2015.

[33] D. A. Hsieh, "Chaos and nonlinear dynamics : application to financial markets," *The journal of finance*, vol. 46, no. 5, pp. 1839–1877, 1991.

[34] N. Basalto, R. Bellotti, F. De Carlo, P. Facchi, and S. Pascazio, "Clustering stock market companies via chaotic map synchronization," *Physica A : Statistical Mechanics and its Applications*, vol. 345, no. 1-2, pp. 196–206, 2005.

[35] G. Chen and X. Dong, *From chaos to order : methodologies, perspectives and applications*, vol. 24. World Scientific, 1998.

[36] R. Holmgren, *A first course in discrete dynamical systems*. Springer Science & Business Media, 2000.

[37] B. K. Shivamoggi, *Nonlinear dynamics and chaotic phenomena : An introduction*, vol. 103. Springer, 2014.

[38] A. Barugola, J.-c. Cathala, L. Gardini, and C. Mira, *Chaotic dynamics in two-dimensional noninvertible maps*, vol. 20. World Scientific, 1996.

[39] D. Chandler, "Edward lorenz, father of chaos theory and butterfly effect, dies at 90," 2008. MIT Tech Talk on.

[40] T. Kapitaniak, *Chaotic oscillations in mechanical systems*. Manchester University Press, 1991.

[41] A. Pawar, "Mandelbrot set and julia set." MATLAB Central File Exchange. Retrieved October 15, 2020, 2020. https ://www.mathworks.com/matlabcentral/fileexchange/24740-mandelbrot-set-and-julia-set.

[42] O. Garasym, R. Lozi, and I. Taralova, "Robust PRNG based on homogeneously distributed chaotic dynamics," in *Journal of Physics : Conference Series*, vol. 692, p. 012011, 2016.

[43] R. Hamza, "A novel pseudo random sequence generator for image-cryptographic applications," *Journal of Information Security and Applications*, vol. 35, pp. 119–127, 2017.

[44] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing : Image Communication*, vol. 41, pp. 144–157, 2016.

[45] S. M. Ulam, "On combination of stochastic and deterministic processes," *Bull. Amer. Math. Soc.*, vol. 53, p. 1120, 1947.

[46] A. Lasota and M. C. Mackey, *Chaos, fractals, and noise : stochastic aspects of dynamics*, vol. 97. Springer Science & Business Media, 1994.

[47] E. Ott, *Chaos in dynamical systems*. Cambridge university press, 2002.

[48] A. Naanaa, "Fast chaotic optimization algorithm based on spatiotemporal maps for global optimization," *Applied Mathematics and Computation*, vol. 269, pp. 402–411, 2015.

[49] H. Bin, B. Li-yong, D. Hong-wei, and Z. Lei, "Analysis of chaos optimization algorithm based on homogenizing regulator with chebyshev mapping," in *2018 11th International Conference on Intelligent Computation Technology and Automation (ICICTA)*, pp. 8–12, IEEE, 2018.

[50] M. Hénon, "A two-dimensional mapping with a strange attractor," in *The Theory of Chaotic Attractors*, pp. 94–102, Springer, 1976.

[51] R. Lozi, "Un attracteur étrange du type attracteur de Hénon," *Le Journal de Physique Colloques*, vol. 39, no. C5, pp. C5–9, 1978.

[52] V. I. Arnol'd and A. Avez, "Ergodic problems of classical mechanics," 1968.

[53] Z. Hua, S. Yi, Y. Zhou, C. Li, and Y. Wu, "Designing hyperchaotic cat maps with any desired number of positive lyapunov exponents," *IEEE Transactions on Cybernetics*, vol. 48, no. 2, pp. 463–473, 2017.

[54] F. Chen, K.-w. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold cat map," *Theoretical Computer Science*, vol. 552, pp. 13–25, 2014.

[55] C. Li, K. Tan, B. Feng, and J. Lü, "The graph structure of the generalized discrete arnold's cat map," *arXiv preprint arXiv :1712.07905*, 2017.

[56] D. R. Stinson and M. Paterson, *Cryptography : theory and practice*. CRC press, 2018.

[57] L. Kocarev, "Chaos-based cryptography : a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[58] S. El Assad, M. Farajallah, and C. Vladeanu, "Chaos-based block ciphers : An overview," in *2014 10th International Conference on Communications (COMM)*, pp. 1–4, IEEE, 2014.

[59] V. Patidar, N. Pareek, and K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[60] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[61] H. E.-d. H. Ahmed, H. M. Kalash, and O. S. F. Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption," *Informatica*, vol. 31, no. 1, 2007.

[62] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[63] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[64] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and chaos*, vol. 8, no. 06, pp. 1259–1284, 1998.

[65] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.

[66] J. Chen, F. Han, W. Qian, Y.-D. Yao, and Z.-l. Zhu, "Cryptanalysis and improvement in an image encryption scheme using combination of the 1d chaotic map," *Nonlinear Dynamics*, vol. 93, no. 4, pp. 2399–2413, 2018.

[67] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.

[68] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Processing*, vol. 143, pp. 122–133, 2018.

[69] Z. Li, C. Peng, W. Tan, and L. Li, "A novel chaos-based color image encryption scheme using bit-level permutation," *Symmetry*, vol. 12, no. 9, p. 1497, 2020.

[70] X. Wang, L. Feng, R. Li, and F. Zhang, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model," *Nonlinear Dynamics*, vol. 95, no. 4, pp. 2797–2824, 2019.

[71] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons & Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

[72] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 22023–22043, 2019.

[73] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

[74] W. Zhang, K.-w. Wong, H. Yu, and Z.-l. Zhu, "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 8, pp. 2066–2080, 2013.

[75] M. Farajallah, S. El Assad, and O. Deforges, "Cryptanalyzing an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28225–28248, 2018.

[76] A. Broumandnia, "The 3D modular chaotic map to digital color image encryption," *Future Generation Computer Systems*, vol. 99, pp. 489–499, 2019.

[77] A. B. Joshi, D. Kumar, A. Gaffar, and D. Mishra, "Triple color image encryption based on 2D multiple parameter fractional discrete fourier transform and 3D arnold transform," *Optics and Lasers in Engineering*, vol. 133, p. 106139, 2020.

[78] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *International Journal of Bifurcation and chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[79] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A new design of cryptosystem based on S-box and chaotic permutation," *Multimedia Tools and Applications*, pp. 1–22, 2020.

[80] X. Zhang, Z. Zhao, and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer," *Signal Processing : Image Communication*, vol. 29, no. 8, pp. 902–913, 2014.

[81] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps," *Chaos, solitons & fractals*, vol. 31, no. 3, pp. 571–579, 2007.

[82] Y. Wang, K.-W. Wong, C. Li, and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Physics Letters A*, vol. 376, no. 6-7, pp. 827–833, 2012.

[83] M. Khan, T. Shah, and M. A. Gondal, "An efficient technique for the construction of substitution box with chaotic partial differential equation," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1795–1801, 2013.

[84] X. Wang and Q. Wang, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 567–576, 2014.

[85] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[86] G. Zaibi, F. Peyrard, A. Kachouri, D. Fournier-Prunaret, and M. Samet, "Efficient and secure chaotic S-Box for wireless sensor network," *Security and Communication Networks*, vol. 7, no. 2, pp. 279–292, 2014.

[87] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Information Sciences*, vol. 486, pp. 340–358, 2019.

[88] H. Diab, "An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations," *IEEE Access*, vol. 6, pp. 42227–42244, 2018.

[89] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," *Optics communications*, vol. 284, no. 12, pp. 2775–2780, 2011.

[90] H. Liu, X. Wang, *et al.*, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.

[91] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia tools and applications*, vol. 71, no. 3, pp. 1469–1497, 2014.

[92] B. Idrees, S. Zafar, T. Rashid, and W. Gao, "Image encryption algorithm using S-box and dynamic Hénon bit level permutation," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 6135–6162, 2020.

[93] M. Wang, X. Wang, Y. Zhang, S. Zhou, T. Zhao, and N. Yao, "A novel chaotic system and its application in a color image cryptosystem," *Optics and Lasers in Engineering*, vol. 121, pp. 479–494, 2019.

[94] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Optics and Lasers in Engineering*, vol. 115, pp. 7–20, 2019.

[95] S. Zhou, Z. Wei, B. Wang, X. Zheng, C. Zhou, and Q. Zhang, "Encryption method based on a new secret key algorithm for color images," *AEU-International Journal of Electronics and Communications*, vol. 70, no. 1, pp. 1–7, 2016.

[96] J.-x. Chen, Z.-l. Zhu, C. Fu, H. Yu, and L.-b. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 3, pp. 846–860, 2015.

[97] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. A. Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[98] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 20, no. 7, p. 535, 2018.

[99] J. Chen, Z.-l. Zhu, L.-b. Zhang, Y. Zhang, and B.-q. Yang, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption," *Signal Processing*, vol. 142, pp. 340–353, 2018.

[100] H. Diab, "A selective self-adaptive image cryptosystem based on bit-planes decomposition," *IJ Network Security*, vol. 21, no. 1, pp. 47–61, 2019.

[101] Z. Lin, C. Guyeux, S. Yu, Q. Wang, and S. Cai, "On the use of chaotic iterations to design keyed hash function," *Cluster Computing*, vol. 22, no. 1, pp. 905–919, 2019.

[102] H. Yang, K.-W. Wong, X. Liao, W. Zhang, and P. Wei, "A fast image encryption and authentication scheme based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 11, pp. 3507–3517, 2010.

[103] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[104] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps," *AEU-International Journal of Electronics and Communications*, vol. 68, no. 3, pp. 186–192, 2014.

[105] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics & Laser Technology*, vol. 82, pp. 121–133, 2016.

[106] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35–51, 2017.

[107] Y. Luo, J. Lin, J. Liu, D. Wei, L. Cao, R. Zhou, Y. Cao, and X. Ding, "A robust image encryption algorithm based on chua's circuit and compressive sensing," *Signal Processing*, vol. 161, pp. 227–247, 2019.

[108] Y. Luo, S. Tang, J. Liu, L. Cao, and S. Qiu, "Image encryption scheme by combining the hyper-chaotic system with quantum coding," *Optics and Lasers in Engineering*, vol. 124, p. 105836, 2020.

[109] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation," *Optics & Laser Technology*, vol. 121, p. 105777, 2020.

[110] A. Belazi, A. A. Abd El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Optics and Lasers in Engineering*, vol. 88, pp. 37–50, 2017.

[111] A. Shafique and F. Ahmed, "Image encryption using dynamic S-box substitution in the wavelet domain," *Wireless Personal Communications*, pp. 1–26, 2020.

[112] T.-H. Chen and K.-C. Li, "Multi-image encryption by circular random grids," *Information Sciences*, vol. 189, pp. 255–265, 2012.

[113] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.

[114] P. Hellekalek, "Good random number generators are (not so) easy to find," *Mathematics and Computers in Simulation*, vol. 46, no. 5-6, pp. 485–505, 1998.

[115] L. E. Bassham III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, *et al.*, *Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications*. National Institute of Standards & Technology, 2010.

[116] P. L'Ecuyer and R. Simard, "TestU01 : AC library for empirical testing of random number generators," *ACM Transactions on Mathematical Software (TOMS)*, vol. 33, no. 4, pp. 1–40, 2007.

[117] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101–111, 2014.

[118] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption," *Signal Processing*, vol. 147, pp. 133–145, 2018.

[119] H. Li, L. Deng, and Z. Gu, "A robust image encryption algorithm based on a 32-bit chaotic system," *IEEE Access*, vol. 8, pp. 30127–30151, 2020.

[120] R. Lozi, "New enhanced chaotic number generators," *arXiv preprint arXiv :0705.4626*, 2007.

[121] M. L. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 723–744, 2018.

[122] C. Zhu, S. Li, and Q. Lu, "Pseudo-random number sequence generator based on chaotic logistic-tent system," in *2019 IEEE 2nd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE)*, pp. 547–551, IEEE, 2019.

[123] O. Jallouli, S. El Assad, M. Chetto, and R. Lozi, "Design and analysis of two stream ciphers based on chaotic coupling and multiplexing techniques," *Multimedia tools and applications*, vol. 77, no. 11, pp. 13391–13417, 2018.

[124] X. Lv, X. Liao, and B. Yang, "A novel pseudo-random number generator from coupled map lattice with time-varying delay," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 325–341, 2018.

[125] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Information Sciences*, vol. 450, pp. 361–377, 2018.

[126] Y. Zhang, "The fast image encryption algorithm based on lifting scheme and chaos," *Information Sciences*, vol. 520, pp. 177–194, 2020.

[127] M. Garcia-Bosque, A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, and S. Celma, "Chaos-based bitwise dynamical pseudorandom number generator on FPGA," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 1, pp. 291–293, 2018.

[128] J. S. Khan, J. Ahmad, S. S. Ahmed, H. A. Siddiqa, S. F. Abbasi, and S. K. Kayhan, "DNA key based visual chaotic image encryption," *Journal of Intelligent & Fuzzy Systems*, vol. 37, no. 2, pp. 2549–2561, 2019.

[129] S. M. Ismail, L. A. Said, A. A. Rezk, A. G. Radwan, A. H. Madian, M. F. Abu-Elyazeed, and A. M. Soliman, "Generalized fractional logistic map encryption system based on FPGA," *AEU-International Journal of Electronics and Communications*, vol. 80, pp. 114–126, 2017.

[130] J. Hou, R. Xi, P. Liu, and T. Liu, "The switching fractional order chaotic system and its application to image encryption," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 2, pp. 381–388, 2016.

[131] C. Guyeux, Q. Wang, and J. M. Bahi, "A pseudo random numbers generator based on chaotic iterations : application to watermarking," in *International conference on web information systems and mining*, pp. 202–211, Springer, 2010.

[132] B. D. Ripley, *Chapter 2. Stochastic simulation*, vol. 316. John Wiley & Sons, 2009.

[133] R. A. Elmanfaloty and E. Abou-Bakr, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation," *Chaos, Solitons & Fractals*, vol. 118, pp. 134–144, 2019.

[134] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018 : A year in review," *Journal of Information Security and Applications*, vol. 48, p. 102361, 2019.

[135] L. Chen, B. Ma, X. Zhao, and S. Wang, "Differential cryptanalysis of a novel image encryption algorithm based on chaos and line map," *Nonlinear Dynamics*, vol. 87, no. 3, pp. 1797–1807, 2017.

[136] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[137] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[138] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[139] Z. M. Z. Muhammad and F. Özkaynak, "Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique," *IEEE Access*, vol. 7, pp. 99945–99953, 2019.

[140] R. Huang, X. Liao, A. Dong, and S. Sun, "Cryptanalysis and security enhancement for a chaos-based color image encryption algorithm," *Multimedia Tools and Applications*, pp. 1–27, 2020.

[141] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal processing*, vol. 144, pp. 444–452, 2018.

[142] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *Journal of Information Security and Applications*, vol. 54, p. 102566, 2020.

[143] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu, and S. Miao, "Image block encryption algorithm based on chaotic maps," *IET Signal Processing*, vol. 12, no. 1, pp. 22–30, 2017.

[144] J. M. K. Mastan and R. Pandian, "Cryptanalysis of two similar chaos-based image encryption schemes," *Cryptologia*, pp. 1–12, 2020.

[145] A. Beloucif, O. Noui, and L. Noui, "Design of a tweakable image encryption algorithm using chaos-based schema," *International Journal of Information and Computer Security*, vol. 8, no. 3, pp. 205–220, 2016.

[146] Y. Liu, Z. Qin, and J. Wu, "Cryptanalysis and enhancement of an image encryption scheme based on bit-plane extraction and multiple chaotic maps," *IEEE Access*, vol. 7, pp. 74070–74080, 2019.

[147] W. Wen, Y. Zhang, M. Su, R. Zhang, J.-x. Chen, and M. Li, "Differential attack on a hyper-chaos-based image cryptosystem with a classic bi-modular architecture," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 383–390, 2017.

[148] R. Boriga, A. C. Dăscălescu, and I. Priescu, "A new hyperchaotic map and its application in an image encryption scheme," *Signal Processing : Image Communication*, vol. 29, no. 8, pp. 887–901, 2014.

[149] W. Zhang, H. Yu, and Z.-l. Zhu, "Color image encryption based on paired interpermuting planes," *Optics Communications*, vol. 338, pp. 199–208, 2015.

[150] J.-x. Chen, Z.-l. Zhu, C. Fu, L.-b. Zhang, and Y. Zhang, "An efficient image encryption scheme using lookup table-based confusion and diffusion," *Nonlinear Dynamics*, vol. 81, no. 3, pp. 1151–1166, 2015.

[151] Y. Liu, X. Tong, and J. Ma, "Image encryption algorithm based on hyper-chaotic system and dynamic S-box," *Multimedia Tools and Applications*, vol. 75, no. 13, pp. 7739–7759, 2016.

[152] W. Zhang, H. Yu, Y.-l. Zhao, and Z.-l. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 118, pp. 36–50, 2016.

[153] D. Ponnain and K. Chandranbabu, "Security analysis of an image encryption algorithm based on paired interpermuting planes and a modified scheme," *Optik*, vol. 127, no. 19, pp. 8111–8123, 2016.

[154] G. Hu, D. Xiao, Y. Wang, and X. Li, "Cryptanalysis of a chaotic image cipher using latin square-based confusion and diffusion," *Nonlinear Dynamics*, vol. 88, no. 2, pp. 1305–1316, 2017.

[155] X. Zhang, W. Nie, Y. Ma, and Q. Tian, "Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box," *Multimedia Tools and Applications*, vol. 76, no. 14, pp. 15641–15659, 2017.

[156] J. Wu, X. Liao, and B. Yang, "Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 142, pp. 292–300, 2018.

[157] Q. Wang, S. Yu, C. Li, J. Lü, X. Fang, C. Guyeux, and J. M. Bahi, "Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems," *IEEE Transactions on Circuits and Systems I : Regular Papers*, vol. 63, no. 3, pp. 401–412, 2016.

[158] W. S. Sayed, A. G. Radwan, A. A. Rezk, and H. A. Fahmy, "Finite precision logistic map between computational efficiency and accuracy with encryption applications," *Complexity*, vol. 2017, 2017.

[159] M. A. Taha, S. E. Assad, A. Queudet, and O. Deforges, "Design and efficient implementation of a chaos-based stream cipher," *International Journal of Internet Technology and Secured Transactions*, vol. 7, no. 2, pp. 89–114, 2017.

[160] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers : from theory to practical algorithms," *IEEE Transactions on Circuits and Systems I : Regular Papers*, vol. 53, no. 6, pp. 1341–1352, 2006.

[161] S. Lian, J. Sun, J. Wang, and Z. Wang, "A chaotic stream cipher and the usage in video protection," *Chaos, Solitons & Fractals*, vol. 34, no. 3, pp. 851–859, 2007.

[162] B. Stoyanov and K. Kordov, "Novel secure pseudo-random number generation scheme based on two tinkerbell maps," *Advanced Studies in Theoretical Physics*, vol. 9, no. 9, pp. 411–421, 2015.

[163] D. Joan and R. Vincent, "The design of Rijndael : AES-the advanced encryption standard," in *Information Security and Cryptography*, springer, 2002.

[164] T. Omrani, R. Rhouma, and R. Becheikh, "LICID : a lightweight image cryptosystem for IoT devices," *Cryptologia*, pp. 1–31, 2019.

[165] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on hopfield chaotic neural network," *Optics and Lasers in Engineering*, vol. 115, pp. 107–118, 2019.

[166] M. Z. Yildiz, O. Boyraz, E. Guleryuz, A. Akgul, and I. Hussain, "A novel encryption method for dorsal hand vein images on a microcomputer," *IEEE Access*, vol. 7, pp. 60850–60867, 2019.

[167] M. Khan, I. Hussain, S. S. Jamal, and M. Amin, "A privacy scheme for digital images based on quantum particles," *International Journal of Theoretical Physics*, vol. 58, no. 12, pp. 4293–4310, 2019.

[168] A. Adeel, J. Ahmad, H. Larijani, and A. Hussain, "A novel real-time, lightweight chaotic-encryption scheme for next-generation audio-visual hearing aids," *Cognitive Computation*, pp. 1–13, 2019.

[169] Y. Luo, R. Zhou, J. Liu, S. Qiu, and Y. Cao, "An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26191–26217, 2018.

[170] S. Hénaff, I. Taralova, and C. Moog, "Systemes non-linéaires sous-échantillonnés," in *Conférence Internationale Francophone d'Automatique*, 2010.

Titre : Dynamique non-linéaire, applications au chiffrement basé sur le chaos

Mots clés : dynamique non-linéaire, système chaotique, crypto-système basé sur le chaos, algorithme de chiffrement, chiffrement de flux, chiffrement par bloc, générateur de nombres pseudo-aléatoires (PRNG)

Résumé : Les systèmes chaotiques présentent des comportements dynamiques non-linéaires complexes. Ils possèdent des propriétés spécifiques, à la fois déterministes et pseudo-aléatoires, qui les rendent prometteurs pour la conception d'algorithmes de chiffrement sécurisé. Les crypto systèmes basés sur le chaos peuvent être classés en chiffrement par flux et chiffrement par blocs. La conception d'un Générateur de Nombres Pseudo-Chaotiques (PCNG) présentant des propriétés pseudo-aléatoires et chaotiques imposées est cruciale pour la sécurité d'un crypto système. Cependant, des niveaux insuffisants de confusion et de diffusion dans l'algorithme de cryptage utilisant un PCNG pas assez performant conduisent à des failles de sécurité. La conception de cartes chaotiques à partir d'une fonction de variables réelles peut menacer la fiabilité d'un crypto système basé sur le chaos.
Pour cette raison nous proposons des cartes chaotiques reformulées sur un corps fini de nombres entiers codés sur 32 bits. Cela permet de surmonter les problèmes d'erreur de quantification et optimise ainsi l'utilisation des ressources informatiques. De plus, nous proposons deux nouveaux algorithmes de chiffrement, le premier est basé sur le chiffrement par flux utilisant un PCNG efficace. Le second est un chiffrement robuste par blocs qui est fondé sur des composants chaotiques et la S-box de l'Advanced Encryption Standard (AES). Ce dernier algorithme présente d'excellentes propriétés de confusion et de diffusion. Les propriétés statistiques ainsi que les cas tests standards de cryptage d'images ont été vérifiés pour les deux algorithmes qui se sont avérés être sûrs et fiables. En outre, un Générateur de Nombres Pseudo-Aléatoires (PRNG) basé sur un schéma de couplage de fonctions chaotiques innovant a été proposé. Les excellentes propriétés statistiques et chaotiques du générateur sont conservées pour un large choix de paramètres couplés. Le générateur proposé peut donc être utilisé pour des applications cryptographiques ou toutes applications nécessitant un PRNG.

Title : Nonlinear dynamics, applications to chaos-based encryption

Keywords : nonlinear dynamics, chaotic system, chaos-based cryptosystem, encryption algorithm, stream cipher, block cipher, pseudo-random number generator (PRNG)

Abstract : Chaotic systems are known to exhibit complex nonlinear dynamics. They present both random-like and deterministic features, which render chaos-based encryption very promising for the design of secure cryptosystems. Chaos-based cryptosystems can be classified into stream ciphers and block ciphers. A well designed pseudo-chaotic number generator (PCNG) with enhanced chaotic features and pseudo-randomness plays a crucial role in the security of a chaos-based cryptosystem. However, an insufficient level of confusion and diffusion in the encryption algorithm and unreliable PCNGs may lead to a security breach. Meanwhile, the adopted real number domain defined chaotic maps may menace the reliability of a chaos-based cryptosystem.
In this thesis, the chaotic maps under investigation have been reformulated over a finite N-bit (N=32) integer field, which overcomes the quantification problems and reduces the resource utilization. In addition, a new stream cipher based on an efficient PCNG and a robust block cipher based on chaotic components and the S-box of Advanced Encryption Standard (AES) with excellent confusion and diffusion properties have been proposed. Both have been verified to be secure and reliable. Furthermore, a pseudo-random number generator (PRNG) framework based on a newly designed smart coupling of chaotic maps has been explored. It has good flexibility and can be used in cryptographic or other PRNG required applications.