SECURITY OF DIGITAL IMAGES USING DYNAMICAL SYSTEMS

by

Amina Souyah

Thesis Submitted For The Award Of The Degree Of

Doctor Of Philosophy

In Computer Science

Department of computer science

Faculty of Exact sciences

University of Djilali Liabes (UDL)

December,2017

Advisor: Prof. Kamel Mohamed Faraoun, University of Djilali Liabes UDL

Signature of the Author _____

Certified by _____

PhD Program Director Date

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

CA	Cellular Automata
VLSI	Very-Large-Scale-Integration
DES	Data Encryption Standard
IDEA	International Data Encryption Algorithm
AES	Advanced Encryption Algorithm
1D	One Dimensional
2D	Two Dimensuinal
r	Raduis
RCA	Reversible Cellular Automata
MCA	Memory Cellular Automata
RMCA	Reversible Memory Cellular Automata
RGB	Red,Green and Blue
X^2	Chi-square
NPCR	Number of Pixel Change Rate
UACI	Unified Average Changing Rate
Ps	Plaintext sensitivity
Ks	Key sensitivity
HD	Hamming Distance
QTD	Quadtree Decomposition
LTS	Logistic Tent System
CLF-XOR	Coordinate Logic-Filter-XOR
C#	C sharp
ECA	Elementary Cellular Automata
PRNG	Pseudo-Random Number Generator
CNN	Cellular Neural Network
Mod	Modulo
PRP	Pseudo-Random Permutation
CPA	Chosen Plaintext Attack
CCA	Chosen Ciphertext Attack
PWLCM	Piecewise Linear Chaotic map
LMCA	Linear Memory Cellular Automata
RE	Randomized Encryption
Wh	Weighted histogram
SHA	Secure Hash Algorithm
eXOR	Expanded XOR
NCA	Nonlinear Chaotic map
CBC	Cipher Block Chaining
2D-LASM	TWO-Dimensional Logistic-Adjusted-Sine Map
BLP	Bit-Level Permutation
CT	Computed Tomography
MR	Magnetic Resonance
X	X-ray
LSB	Least-Significant Bit
NIST	National Institute of Standards and Technology

Acknowledgments

All the thanks are offered to my **ALLAH**, ...
After, i would like to express, my gratitude to:
Particularly, my supervisor Prof. Kamel Mohamed FARAOUN for his advice, help, and support throughout this thesis.
So much appreciate the generous help, advice, encouragements, moral supports of my friends during the taken period to give birth to this work.
Last but not least, special thanks go to my parents, and all the members of my family for their moral supports and faith in me.

Abstract

Cryptography as an art and science concerns mainly the protection of communicating data e.g., digital image, audio and video files, from unauthorized interceptions as well as fraudulent changes. It builds under the assumption that if the behavior is obvious, the point of attack is achievable, so that the aim here is to conceal any noticeable information about the original data. These security needs are established by means of a well-designed cryptosystem, in which the evaluation of its quality is quantified by, to which extent it can be employed in practice for data encryption and decryption transformations without the key being broken. For decades of years, serious efforts have been devoted to investigate and develop means from various branches of knowledge, and then employed them as tools in the area of designing secure cryptosystems. Of particular interest, are those proposals involve the use of dynamical systems. The very appealing observed point is that, the attractive features of dynamical systems e.g., unpredictability, complex chaotic behavior can be reached by simple mathematical models. This latter has been the leading point to establish the bridge between the theory of dynamical systems and cryptography. From the viewpoint of, exploiting and developing these complex models as a base in the design of efficient cryptographic means.

This thesis involves the use of two different types of dynamical systems in discrete-time, namely cellular automata-based dynamical systems and chaos-based dynamical systems, and investigates the existing cryptographic methods related to them, to provide new and efficient proposals for image content preservation. The key contributions throughout this thesis are: firstly, a novel fast and efficient randomized encryption cipher based on quadtree decomposition mechanism (QTD) in combination with special class of cellular automata, namely one dimensional 4^{th} order reversible memory cellular automata (RMCA) tailored to digital image encryption; secondly, a new image encryption method based on chaos jointly special class of cellular automata, namely two dimensional 4^{th} order reversible memory cellular automata (RMCA) with Moore neighborhood; thirdly, a new chaotic cipher algorithm for efficient and secure image content preservation, specialized for both standard and medical images. Each of these proposals is evaluated by means of the common and typical assessment tools. The obtained results are interesting in terms of security degrees and time-consuming, and point to the advocacy of the designed cipher algorithms.

Keywords:
Cryptography, Cellular automata-based dynamical systems, chaos-based dynamical systems, image content preservation.

Résumé

La cryptographie en tant que science s'occupe principalement de la protection des données échangées, stockés ou manipulées, dans leurs différents formes possibles tel que les images numériques, les fichiers audio et vidéo et les messages électroniques, contre des interceptions non autorisées ainsi que des modifications frauduleuses. La cryptographie fonctionne sous l'hypothèse que si le comportement est évident, le point d'attaque devient réalisable, de sorte que l'objectif est de cacher toute information notable sur les données d'origine. Les besoins de sécurité sont généralement établis au moyen d'un crypto-système sécurisé. Depuis des décennies, de sérieux efforts ont été déployés pour étudier et développer de nouvelles approches de chiffrement et de cryptographie en général, à partir de divers domaines et modèles mathématiques et physiques existants. Particulièrement, plusieurs possibilités sont offertes on utilisant la théorie des systèmes dynamiques et chaotiques. Il est trés intéressant d'observer que les caractéristiques attrayantes des systèmes dynamiques, tel que l'imprévisibilité et le comportement chaotique complexe, peuvent être atteintes par de simples modèles mathématiques. Le comportement chaotique complexe a été le point de départ pour établir le pont entre la théorie des systèmes dynamiques et la cryptographie, et a permis l'exploitation et le développement de ces modèles complexes comme une base dans la conception de moyens cryptographiques efficaces.

Dans le cadre de cette thèse, on s'intéresse à l'utilisation en cryptographie de deux types différents de systèmes dynamiques discrets, à savoir : les systèmes dynamiques à base d'automates cellulaires et les systèmes dynamiques basés sur le chaos. On présente donc premièrement les méthodes cryptographiques existantes qui leur sont associées pour fournir finalement de nouvelles propositions efficaces permettant la protection du contenu des images numériques. Dans ce travail on propose premièrement un nouveau mode de chiffrement aléatoire rapide et efficace, basé sur le mécanisme de décomposition Quadtree (QTD), en combinaison avec la classe des automates cellulaires à mémoire réversible d'ordre 4 (RMCA), et adapté aux images numériques. Une deuxième approche combinant les systèmes chaotiques et les (RMCA) et aussi proposée et validée expérimentalement. Finalement, on propose un algorithme de chiffrement basée sur les modèles chaotique dédiée au chiffrement des images standards et médicales. Chacune des trois approches est évaluée au moyen d'outils d'valuation communs et typiques. Les résultats obtenus sont satisfaisants en termes de degrés de sécurité, de temps de consommation, et de robustesse des algorithmes de chiffrement conçus.

Mots clés :
Cryptographie, systèmes dynamiques à base d'automates cellulaires, systèmes dynamiques basés sur la théorie du chaos, protection du contenu d'image.

ملخص البحث

التشفير كفن و علم يهتم أساسا بحماية بيانات التواصل على سبيل المثال، الصور الرقمية، ملفات الصور و الفيديو من أي تدخل غير مسموح به أو كذلك التغييرات الاحتيالية. هذا العلم مبني على فريضية أنه، إذا وجد أي وضوح على مستوى المعلومة المشفرة، فإن نقطة إختراق أمن المعلومة محقق. فإذا يكمن الهدف هنا في اخفاء أي معلومة ملحوظة ـ يمكن أن تستغل ـ حول البيانات الاصلية. تقام هذه الاحتياجات الامنيه من خلال نظام تشفير مصمم تصميما جيدا، بحيث أن جودة هذا الاخير يمكن أن تعلم من مدى فعالية نظام التشفير في ممارسة تشفير البيانات على المستوى العملي من دون أن يتم أي اختراق للكلمة المفتاحية. على مدى عقود من الزمن، جهود كبيرة تم تكريسها من أجل استثمار و تطوير أليات و وسائل من مختلف فروع المعرفة، ثم بعد ذلك استخدامها كأدات في مجال تصميم نظم الترميز الأمنة. على وجه الخصوص ، تلك المقترحات اللتي تقوم على استخدام الأنظمة الديناميكية. النقطة الجوهرية هنا، هي أن خصائص الأنظمة الديناميكية مثل عدم القدرة على التنبؤ والسلوك الفوضوي المعقد يمكن الاستفادة منه في علم التشفير بواسطة نماذج رياضية بسيطة. وكان هذا الأخير وجهة رائدة لإقامة جسر بين نظرية النظم الديناميكية والتشفير. من وجهة نظر استغلال وتطوير هذه النماذج المعقدة كقاعدة في تصميم وسائل التشفير الفعالة.

هذه الأطروحة تهتم باستخدام نوعين مختلفين من الأنظمة الديناميكية القائمة على الخلوية و الأنظمة الديناميكية القائمة على الفوضى، و الإستفادة من مقترحات التشفير الموجودة، من أجل تقديم مقترحات جديدة و فعالة لحماية محتوى الصور الرقمية. المساهمات الأساسية في هذه الأطروحة كالتالي : تتمثل أول مساهمة في تصميم نظام أمن للتشفير العشوائي باستخدام ألية تقسيم QTD المساهمة الثانية تتمثل في ادماج النظام الديناميكي الخلوي مع النظام الديناميكي الفوضوي في تصميم نظام أمن للتشفير خاص بالصور. المساهمة الثالثة تكمن في استخدام النظام الديناميكي الفوضوي كأداة في تصميم نظام أمن للتشفير خاص بالصور العادية و الصور الطبية. بعد تقييم المقترحات تم اثبات فعاليتها من حيث درجة حفظ المعلومة أمنة بالإضافة إلى الوقت الضرفي المناسب للتشفير.

كلمات مفتاحية:
التشفير، النظام الديناميكي الخلوي، النظام الديناميكي الفوضوي، حماية محتوى الصورة.

Personal publications

Published journal/conference papers

- SOUYAH, Amina et FARAOUN, Kamel Mohamed. Fast and efficient randomized encryption scheme for digital images based on Quadtree decomposition and reversible memory cellular automata. Nonlinear Dynamics, 2016, vol. 84, no 2, p. 715-732.
- SOUYAH, Amina et FARAOUN, Kamel Mohamed. An image encryption scheme combining chaos-memory cellular automata and weighted histogram. Nonlinear Dynamics, 2016, vol. 86, no 1, p. 639-653.
- SOUYAH, Amina et FARAOUN, Kamel Mohamed. A Review on Different Image Encryption Approaches. In : Modelling and Implementation of Complex Systems. Springer International Publishing, 2016. p. 3-18.

Submitted journal/conference papers

- SOUYAH, Amina et FARAOUN, Kamel Mohamed. An efficient and secure chaotic cipher algorithm for image content preservation. Communications in Nonlinear Science and Numerical Simulation, Submission 12-Nov-2016, 26 Pages.

Introduction and Thesis overview

Nowadays, with the remarkable advances in digital communication technologies, and the rapid growth of computer power and storage, a challenging problem has been opened, that is, how to protect confidential information related to individuals' privacy from unauthorized staffs, especially in the scenario of open-networks. This situation demands an urgent need to secure systems. To meet this requirement, a variety of means have been exploited and developed, aiming to reach sensitive information content protection. Of a special interest, cryptography as the art and science [109], is considered as the obvious and the paramount method of data preservation [76, 138], it is also categorized as the branch of both computer science and mathematics [3]. The process of encoding the plaintext content, and rendering it unintelligible to all except the legitimate parties is called encryption, the process of decoding and recovering the plaintext from its ciphertext version is referred as decryption. The system that handles both encryption and decryption procedures is called cryptosystem. The security degrees of a cryptosystem are quantified from its extensive employment in practice without being broken [91]. Cryptanalysis is the art of science deals with the study and analysis of cryptosystems, aiming to break their security [111] [88] [59, 60]. Cryptography and cryptanalysis are both branches of cryptology, dissimilar but complementary to each other.

Nevertheless, dynamical systems are governed by means of an evolution rule, and evolved deterministically in time, so that, the current state of the system is transformed to a new state. Dynamical systems are featured by their erratic and complex chaotic behavior, the very appealing is that, these dynamical properties can be arisen based on simple mathematical models. Moreover, it was remarked that these complex systems can be investigated as an origin for encryption and decryption transformations, in which the initial state of a dynamical system is the key of the cryptosystem [91]. In other words, it is possible to exploit the theory of dynamical systems in the realm of cryptography. This thesis deals with two different types of dynamical systems: cellular automata-based dynamical systems and chaos-based dynamical systems.

Cellular automata (CA) as a special type of discrete dynamical systems, have been first

arisen and investigated within the research of Von Neumann and Ulam. The simple framework of CA has grasped considerable attention of growing number of researchers, leading to their application in various scientific research areas, including information security [36] [37]. Interest from the scientific community has arisen and boosted for decades of years in connection to CA-based cryptographic means. This occurred clearly in the establishment of books, specialized conferences, special issues of several journals on CA, and a large number of proposals in the scientific literature [36]. Due to their simplicity, modular and cascable structure, CA have become an attractive concept for modeling complex systems by means of simple underlying rules, and best suited in use for VLSI implementations [32].

Chaos theory is a type of nonlinear dynamical systems, that received considerable attention from the scientific community, especially after the contribution of Lorenz [85]. The interesting dynamical properties of chaos have been investigated and developed in the way of modeling complex behavior, based on simple mathematical models. This astounding found is very beneficial when attempting to explain and predict about the behavior of real systems such as physical processes, evolution of economical systems, communication engineering applications ... etc [101]. In other words, chaos theory can be viewed as an appealing methodology built by simple mathematical techniques, aiming to understand and model real and complex systems. Indeed, it is very interesting to incorporate chaos in modern communication applications, including cryptography. The bridge between chaos dynamical systems and cryptography consists of benefiting from the close connection between these different disciplines, so that, the main features of chaos are very related to secure cryptosystem requirements, and hence investigating chaotic systems as tools of proposals for information protection.

This thesis advocates the investigation of CA-based dynamical systems and chaos-based dynamical systems, in the realm of cryptography, as tools in the design of new encryption algorithms for image content preservation.

Motivations and Research Problem

Since there has been a remarkable growth in computational power, and with the unstoppable and daily usage of digital images over open networks, a serious issue for researchers is opened to investigate better solutions for secure storing and transmitting the content of these digital visual data. In particular those involving sensitive and confidential information related to military, patients' digital medical images, or even personal interest [33, 47, 57, 144], that should be only accessible by their authorized staffs. Therefore, whenever a digital image is needed to be employed within any application, its content preservation turns to be a critical concept. Due to the specific characteristics of digital images like large data size, bulk data capacity, low entropy, strong pixel correlation and

high redundancy, traditional encryption methods such as DES, IDEA, AES, are not adequate to deal with visual data content requirements, since they are originally designed for securing textual data [19, 20, 26, 28, 49, 57, 63, 66, 81, 92, 97, 116, 129, 132, 139]. Moreover, these traditional means seem to not be efficient especially for practical use regarding the non reasonable speed and power for performing image encryption. To this end, considerable efforts have been devoted to investigate better solutions for image content protection in a variety of concerned aspects, as regards to security level, complexity, and time performance, especially under the scenario of real-time communications. In particular, investigating the theory of dynamical systems for image encryption is one of the main actual research directions. This thesis is concerned by the employment of two different types of dynamical systems, in the design and realization of efficient and secure crypto-algorithms for image encryption, herein, cellular automata and chaotic dynamical systems.

In this research, cellular automata (CA) is the first exploited concept as a base in the design of new image encryption algorithms, the appealing paradigm is motivated by its quite simple underlying rules, that achieve complex features, and hence effectively lead to model complex systems [24].

It is required for a good cipher to accomplish some basic cryptographic significance, namely, confusion, diffusion and randomness, these desirable properties can be reached with the specific features of chaotic systems like ergodicity, sensitivity to initial conditions/ system parameters and random behavior [12, 14, 22, 56, 73, 77, 82, 102, 103, 106, 108, 124, 143, 150], so that, this type of dynamical systems seems to be a good candidate to be investigated as a base to design new proposals for image encryption, especially in practical use, as regards to their reasonable computational time, high security level and complexity [52, 61, 105]. This interesting paradigm is selected as the second investigated concept in this effort.

Contributions of this Thesis

This thesis deals with the incorporation and investigation of dynamical systems in the realm of cryptography. The intent of this work is to design and validate novel image encryption proposals, for the sake of providing performance enhancements in terms of security level and execution-time compared to existing cryptographic methods in the scientific literature.

Within this effort, three novel proposal approaches based on dynamical systems for image content preservation are designed, realized and evaluated. The former contribution [118] exploited CA-based dynamical systems as an origin in the design of the first cryptosystem. The second contribution [119] involved the use of chaos jointly CA dynamical systems as

tools in the design of the second cryptosystem, aiming really to benefit from the strong-point of the two different dynamical paradigms. As the latter part, the third contribution advocated the employment of chaos-based dynamical system as a base in the design of the third cryptosystem. The robustness and effectiveness of the newly proposed cryptosystems are evaluated by means of the commonly employed cryptographic attacks, regarding key space attacks, key sensitivity attacks, statistical attacks, differential attacks besides to other security and time consuming issues. A comparison in terms of security level and time performance is provided in relation with existing methods in the scientific literature. We have to bear in mind that all the proposed cipher algorithms are performed under only one round. Indeed, the obtained results of all the proposed cryptosystems point to the reached security enhancements and time consuming reduction compared to certain existing methods. Moreover, a comprehensive and up-to-date review on different image encryption approaches [120] is provided throughout this thesis, the study covered the analysis of each presented proposal, by introducing its advantages and limitations in terms of security level and time performance.

Structure of this Thesis

This thesis is organized into five chapters.

Chapter 1 presents an introduction to cryptology, this includes the essential concepts of cryptography, and the different cryptanalysis techniques. Then, the basic notions and terminologies behind the theory of dynamical systems is presented, comprising: first the preliminaries on the theory of cellular automata (CA) as a special type of dynamical systems, and the primary investigated paradigm as a tool in the design of cryptosystems; and after the preliminaries on the theory of chaos as another type of dynamical systems, and the second exploited concept as an origin in the design of cryptosystems. Furthermore, the common and typical security assessment tools that are employed to evaluate the performance of the designed cryptosystems in terms of security level and time-consuming are covered.

Chapter 2 provides a comprehensive and up-to-date review on image encryption methods based on cellular automata, cellular automata jointly chaos, and chaos dynamical systems. The review also paves a comparative study in terms of the commonly employed cryptographic attacks to break the security of cryptosystems.

Chapter 3 consists mainly of three sections. First of all, the mathematical background of CA is presented. Then, the chapter discusses the system design and realization of two newly proposed cipher algorithms. The first contribution exploits the use of CA, whereas the second contribution investigates the incorporation of chaos with CA, as tools in the

design of the cryptosystems. After that, a comparative study in terms of qualitative and quantitative assessments is introduced with respect to related existing methods. Indeed, the obtained results point to the advocacy of the proposed contributions.

Chapter 4 comprises mainly of four sections. First of all, the mathematical background of the work is presented. Then, the chapter discusses the system design and realization of a novel proposed cipher algorithm. The contribution exploits the use of chaos-based dynamical systems as an origin in the design of the cryptosystem, and suggests a new confusion technique, namely nonlinear bit-level shuffling and circular-shifting. After that, the effectiveness of the newly proposed confusion strategy is provided. As a latter part, a comparative study in terms of qualitative and quantitative assessments is introduced with respect to related existing methods. Indeed, the extensive analysis and tests are validated the robustness of our method against the commonly known cryptographic attacks, and point to the reached security enhancements and time-consuming reduction compared to certain existing methods.

Chapter 5 introduces a conclusion of this thesis, and paves the way for future work.

It is very appealing to offer a complete and well-structured introduction and thesis overview, aiming to present the navigating issue and the different topics that will be covered in this thesis. The remainder chapters were chosen to be written independently, for the sake of given the reader the opportunity to directly go for the chapter/s of interest, without loss of information.

Chapter 1

Preliminary knowledge

Cryptography is the art and science, concerned by keeping the sensitive information secret [109], it is acknowledged as the paramount technique of data preservation against passive and active fraud [76]. Nevertheless, the erratic and the complex behavior of dynamical systems, can be achieved from simple mathematical models, this important observation has received considerable attention of member of researchers from various branches of science over decades of years. For the sake of investigating such desirable features of a dynamical system, is to connect it to similar concepts within a neighboring branch of science, this neighboring branch of science is cryptography [16]. The bridge between these dissimilar scientific disciplines, herein dynamical systems and cryptography, is to exploit dynamical systems as basis to design new cryptographic means [16]. This thesis is concerned with two different kinds of dynamical systems: at first, cellular automata (CA) as a type of dynamical systems is employed as a tool to design secure cryptosystems, a preliminary overview on the theory of CA is discussed in section 2.1.1; at the latter part, chaos as another type of dynamical systems is investigated as an origin of new cryptographic proposals, a preliminary overview of chaos theory is discussed in section 2.1.2. Section 1.3 gives some common and typical security assessment tools that are employed to evaluate the effectiveness of the designed cryptosystem in terms of security level and time performance, and ensure its resistance to cryptographic attacks. At the end, section 1.4 gives a conclusion to this chapter.

1.1 Cryptology

The paramount of investigating principles for the sake of rendering valuable information meaningless, is roughly along with the beginning of writing language [114]. Cryptology is a science that deals with the study of cryptosystems [127], i.e., the transformation of the information into a meaningless form, so that, it can be accessible/distinguishable by the

communicating parties only. This science consists of two related disciplines:

1. The design of tools and framework which conduct to the task of information concealing.

2. Assessment of the constructed cryptographic method.

These two steps are quite dissimilar but complementary to each other as branches of cryptology, which are: cryptography and cryptanalysis.

1.1.1 Cryptography: foundation and essential concepts

Cryptography has an origin to the Greek krýpto "hidden" and the verb gráfo "to write", and it is about the conversion of data from its original form or plaintext to an unreadable form or gibberish, i.e., ciphertext and back again at the other end [70, 126]. The transformation of the plaintext into the ciphertext is referred as encryption, while the reverse operation, i.e., the transformation of the ciphertext into the plaintext is referred as decryption. The oldest employment of cryptography is traced along with the Egyptian hieroglyphic, in which a comprehensive code i.e., hieroglyph is exchanged to another code only readable by the legitimate parties, however, in such type of encryption, the used code should be modified for every sender-recipient pair communication, and hence it is impractical. As time went on, the system of encryption was developed to a more comprehensive one, and relied on a transformation procedure jointly with an external parameter, namely, the key. So, from now on the communicating parties have no need to a prior knowledge about the code conforming the ciphertext, but the transformation procedure and the key. Due to the invention of the telegraph within 1844, and the radio in 1985, cryptography was dramatically influenced and developed, aiming to meet the provisions of the new communications scope. The former encryption/decryption transformation is language character based. Nevertheless, the advent of telegraph and radio and their employment as tools for communication, necessitate the conversion of language letters into a new code which is zero and one based, so that, this is the bit era, and henceforth the encryption/decryption transformation deals with a set of 0 and 1. To this sense, the encryption and decryption procedures are relied on mathematical techniques and a secret key. We extend our speech to discuss more formally about the concept, by means of mathematical notations: The encryption procedure is defined by the following function:

$$e_{k_e} = P \rightarrow C \tag{1.1}$$

where $e_{k_e} \in E$, is the encryption rule or function, $k_e \in K_e$, the encryption key-space is denoted by K_e, and is a finite set of all the possible secret keys. P=$\{p_0, p_1, \ldots, p_{|p|}\}$ is a finite set of possible plaintexts (i.e., plaintext space), and C=$\{c_0, c_1, \ldots, c_{|c|}\}$ is a finite

set of possible ciphertexts (i.e., ciphertext space). The decryption procedure is defined by the following function:

$$d_{k_d} = C \rightarrow P \tag{1.2}$$

where $d_{k_d} \in D$, is the decryption rule or function, $k_d \in K_d$, is the decryption key-space. it should be noticed that d_{k_d}: $C \rightarrow P$ and e_{k_e}: $C \rightarrow P$ are functions that satisfy $d_{k_d}(e_{k_e}(p))$=p,for each plaintext $p \in P$. In case of the decryption key herein k_d can be deduced from the encryption key herein k_e and vice versa, or they are equal to each other, the cryptographic method is referred as secret key (i.e., symmetric) cryptosystem, see Figure 1.1. On the other hand, if the decryption key k_d is different from the encryption key k_e,the cryptographic method is referred as public key (i.e., asymmetric) cryptosystem, see Figure 1.2. Moreover, symmetric cryptosystems are classified on two categories: stream cipher and block cipher, the former one operates on a plaintext at a unity of one bit (or byte) at a time; whereas the latter part operates on the plaintext at a unity of blocks of fixed number of bits. In this thesis all the considered cryptosystems belong to the category of symmetric algorithms, in which k_e=k_d=k.Until now, the encryption and decryption procedures are no more than some types of selected mathematical techniques. Due to the works of Claude Shannon (1916-2001), especially, his most influential cryptographic contribution, namely, "Communication Theory of Secrecy Systems" [112] published in Bell system technical journal in 1949, that made a valuable impact on the scientific study of cryptography, wherein Shannon presented two principles, that should be satisfied in the design of secure cryptosystems, which are: confusion and diffusion. In the former property, the cryptosystem's input with respect to its corresponding output should be statistically independent with a very difficult way, so that, to defeat any exploit by the cryptanalyst; within the latter part one, any bit on the plaintext or the secret key should conduct to a change of many bits on the ciphertext [87]. Such two concepts are still largely employed in the design of modern cryptographic algorithms [74].

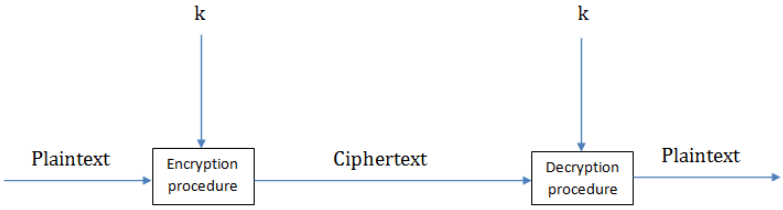


Figure 1.1: Encryption and decryption with the same key: symmetric cryptosystem

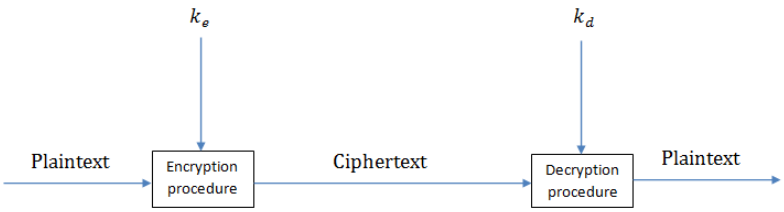


Figure 1.2: Encryption and decryption with two different keys: asymmetric cryptosystem

In the late of 20^{th} century, and with the boost in both computer and internet technology, cryptography is radically revolutionized, a rich theory is emerged, guiding to the thorough study of cryptography as a science [72]. Before the modern era, cryptography was limited by solely preserve the content of the valuable information from unauthorized parties. Nevertheless, modern cryptography covers much more than the problem of confidentiality, encompassing the study of cryptographic means, for the sake of ensuring the security of both digital information, transactions, and distributed computations [72], and it concerns the following additional objectives [74] [88] :

- **Authentication**: ensures that during a secure communication, the concerned parties should identify each other, in other words, it should be ensured that any communicating entity is the validated/legitimate one.
- **Integrity**: ensures that during a secure communication, the unauthorized parties have no ability to modify the information content by illegal means.
- **Non-repudiation**: a procedure to confirm that the information is sent by the original entity, so that, the receiver parties can not ensure the opposite.
- **Access control**: a process of keeping the resources from any non permitted use i.e., it controls who has the right for resources access, with all the limitations, conditions, and the permission level of access.
- **Signature**: a mean to prove the entity authorship.
- **Authorization**: the authorized parties can provide the permission to someone doing something at his side.

1.1.2 Cryptanalysis: types of attacks applied on a cryptosystem

A cryptanalysis is a technique that aims to recover the original form of information, having solely the ciphertext form, and without any prior knowledge about the employed secret key. Extensive efforts should be devoted by modern cryptography, in the way of the design and realization of cryptographic methods with satisfactory level of security, for the sake of image content preservation. In this sense, it is advocated the design of secure means, in such away the conversion of the encryption and decryption procedures can not be successfully achieved beyond the knowledge of the secret key, these essential requisites refer to the core kerckhoffs' Assumption [88]. Indeed, a secure cryptosystem is one in which, it is effortless to obtain $c_i{=}e_k(p_i)$, whereas the recovery of the plaintext by means of $p_i{=}e_k^{-1}(c_i)$ is a difficult problem in term of computational complexity, of course with no knowledge about the secret key, so by this way, it remains for the cryptanalyst to apply the best attack for a well- designed cryptosystem from the viewpoint of security level, herein, exhaustive search i.e., brute force attack, in which it is a trivial technique, based on the attempt of all possible keys until the right one comes up, to recover the plaintext from the ciphertext. Nevertheless, the practicability of such type of attacks is relied on the size of the key-space, besides to the computational power of the attacker. To provide a sufficient immunity against brute force attacks and elude the effect of computational technology at a reasonable time, the key-space of a given cryptographic algorithm should be larger than 2^{100} suggested rule 15 by the authors of [7]. On the other hand, the evaluation of the cryptosystem should be considered from the practical aspects rather than the theoretical ones. Once the communicating parties have established a communication over an insecure channel, see Figure 1.3, the role of the third party i.e., cryptanalyst is to work either on the deduction of the employed secret key, or the development of certain methods to recover the plaintext from the ciphertext, out of the knowledge of the secret key, by means of investigating any statistical dependency between the ciphertext and the secret key, or the ciphertext and the plaintext. All the possible techniques of cryptanalysis that can be performed to a given cryptosystem are compared to exhaustive search in terms of data and complexity, so that, an attack can be considered as successful if its complexity is significantly less than the one consumed by brute force attack. By the following, the most common types of attacks, which are based on a variety of assumptions, are discussed [74] [122]:

- **Ciphertext-only attack**: the cryptanalyst intercepts the produced ciphertext by means of the cipher algorithm. It is the hardest type of cryptanalysis, in which the attacker depends on just some form of redundancy that can be detected in the ciphertext, and employed to retrieve some valuable information about the plaintext, aiming to deduce the key, some parts of the key, or key-equivalent information.

- **Known-plaintext attack**: the cryptanalyst processes some ciphertexts with their matching plaintexts. The goal is to use these plaintext-ciphertext pairs to obtain some information that may help in deducing the key or the key-equivalent information.
- **Chosen-plaintext attack**: the cryptanalyst is able to choose any plaintext and obtain its corresponding ciphertext, without any revealing of the key. The attacker tries to deduce any statistical dependency between the plaintext-ciphertext pairs, aiming to achieve any valuable information about the key.
- **Chosen-ciphertext attack**: the cryptanalyst is able to choose any ciphertext and obtain its corresponding plaintext. It is the strongest attack model among all the aforementioned ones. As previously, the attacker attempts deducing any correlations between the plaintext-ciphertext pairs, aiming to achieve useful information about the key.

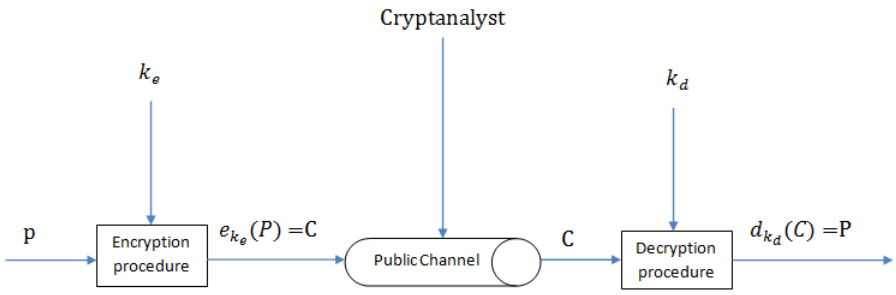


Figure 1.3: Encryption and decryption scheme

Indeed, the consumed resources play a paramount role in the assessment of the success of these four cryptographic attacks, according to which the amount and the type of data is important [74]. Hence, a given cryptosystem should be evaluated in term of each of these cryptographic attacks, to point to the achieved degree about its security.

1.2 Dynamical systems

A dynamical system is a mathematical model deals with the formalization of the temporal evolution of a certain scientific concept process by starting with a certain initial state [78]. The notion of a dynamical system consists of a set of its possible states (state space), in which the current state of the system is defined by means of the past states, and governed by an evolution rule. The dynamics of the system is traced by its state space. if there is

a unique subsequent state predicted by means of the past states of the system, then the given dynamical system is deterministic, otherwise, if there is a probability distribution of possible subsequent states, then the underlying dynamical system is stochastic or random [5]. Indeed, the core component of a dynamical system, is its evolution rule, this latter relies on its state, the time, and an additional information, namely, the control parameters, which is a vector consisting of a set of d variables. Moreover, the evolution rule of a deterministic dynamical system is a map [78]:

$$\varphi = \Lambda \times T \times U \to U \tag{1.3}$$

Where $\Lambda \subset R^d$ denotes a set of control parameters' values, T represents a set of times, and U is the state space of the dynamical system (or phase space), according to a tradition from classical mechanics [5]. The evolution of a dynamical system refers to the change of its state over time. If the set of times is R, then the dynamical system is termed continuous-time dynamical system or flow, whereas with $T{=}Z$ the dynamical system is termed discrete-time dynamical system or map [78]. According to the linearity of the function φ, two types of dynamical systems are considered: those with φ is a linear function; and those with φ is a nonlinear function. Systems of the former type are termed linear dynamical systems, whereas those of the latter part are called nonlinear dynamical systems. Indeed, linear dynamical systems can be systematically analyzed by means of linear algebra techniques [44]. Nevertheless, nonlinear dynamical systems are featured by certain dynamical properties, which are determined by means of the temporal evolution of the underlying system. This thesis is dealt with deterministic discrete-time dynamical systems only.

1.2.1 Preliminaries on Cellular automata

Cellular automata (CA, for short) are a particular type of discrete dynamical systems [4] [65,79,80,125]. They are spatially and temporally discrete mathematical models, featured by their complex emergent behavior, starting with simple configuration composed of simple units termed as cells in an n-dimensional space, and governed by simple functions referred as dynamical transition rules.

Cellular automata were originally introduced by John Von Neumann as formal models, appeared on his works on biologically motivated computation and self-replication [128]. At the beginning, Von Neumann tried to work with black and white cells, i.e., two states solely, after and under the proposal of his colleague Stanislaw Ulam, he took a decision to investigate on a discrete two-dimensional system, composed of 29 different states, henceforth, the system is featured by its complicated dynamics, competent to handle self-reproduction. On the other hand, Von Neumanns CA mechanism considered as the first discrete parallel computational model, and referred formally as a universal computer, in

which the recursive functions can be computed, and the universal Turing machine can be imitated [4].

Stephen Wolfram's works in the 1980s conducted to a valuable impact on the study of cellular automata based cryptographic means. In [133], Wolfram studied the first proposal in the branch of secret key cryptographic methods, henceforth, many researchers had investigated CA as a tool in the design of variant cryptographic techniques. In recent years, CA based ciphers for image confidentiality has grasped the attention of several researchers, lead to a large number of proposals in the scientific literature, see section 2.1 of chapter 2). Wolfram's studies investigated extensively one-dimensional cellular automata, leading to make the groundwork for further research.

Cellular automata can be considered as a simple model of a spatially extended decentralized system [25], composed of a number of simple units termed as cells [38, 86], each cell is featured by its state within a finite number of states. The cell's state at a step $t+1$ is a function of the state of a fixed number of cells referred as the neighborhood at the preceding time step i.e., t. This function is the underlying rule, and the neighborhood of a given cell is formed by the cell itself and its surrounding cells. Iterating CA is governed by means of a rule, starting with an initial configuration, wherein the overall cells should be assigned by initial states, such state values are changed synchronously over time to produce a new configuration. In particular, one dimensional CA in a simplest case is represented as an array of cells, determined over binary state alphabet i.e., each cell's state is either 0 or 1. Such type of CA is referred as elementary CA (a term given by Wolfram). For each cell termed as a central cell, a neighborhood of radius r is defined, in which it is composed of $m{=}2 \times r + 1$ cells, including the cell selected to be updated (central cell), this makes $n{=}2^m$ possible patterns of neighborhood, and 2^n as the total number of rules. So that, with $r{=}1$ they are 256 rules, with $r{=}2$ they are 2^{32} rules ... etc.

By the following an example with radius one rule is exhibited on Figure 1.4.

With $r{=}1$, the neighborhood is consisted of 3 cells, namely, the central cell its immediate left neighbor, and its immediate right neighbor, hence, there exist 8 possible patterns. The state of the cell selected to be updated over time is changed according to an underlying rule. As an example, the rule definition introduced previously on Figure 1.4 says that: if the three neighboring cells in the CA configuration at time t have the pattern 010, then the central cell's state should be 1 on the next time step. The standard conversion suggested by Wolfram is usually the base to term a given rule, so that, the rule is named by means of its binary representation derived from the definition of the rule, in the aforementioned example, the definition of the rule consists of the bits 00011110, which refers to the binary representation of number 30. To deal with a finite size of CAs, generally cyclic boundary

conditions is adopted, according to which CA is considered as a circle grid.

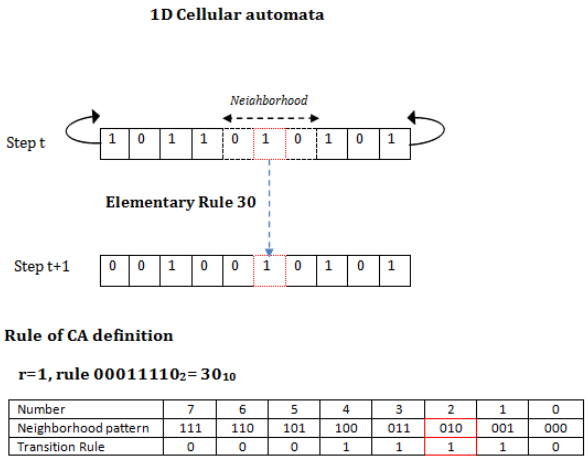
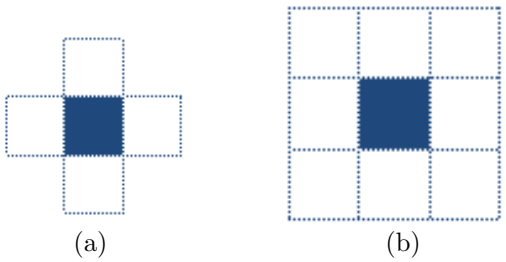


Figure 1.4: 1D cellular automata mechanism with Rule 30

Two dimensional cellular automata have been extensively investigated in various branches of knowledge, but in fact, such computational model has an origin to Von Neumann's self reproducing automaton, in which a two dimensional grid was used. Such class of CA is featured by its two typical neighborhood options, namely, Von Neumann neighborhood, comprising the horizontal and vertical adjacent cells, and Moore neighborhood, consisting of all the eight immediately neighboring cells, see Figure 1.5 [4] [2].



(a) (b)

Figure 1.5: Typical neighborhood options: (a) Von Neumann type; (b) Moore Type

On the other hand, such concept has been also widely employed as a tool to design image encryption schemes, regarding to the obvious similarities between this concept and the matrix representation of images [43]. If the same transition rule is performed to update each cell's state, then the CA is said to be uniform, otherwise it is termed as non-uniform

CA [95]. Cellular automata is said to be linear CAs, if the employed transition rule is a linear function, otherwise it is referred as non-linear CAs [4]. The reversibility of cellular automata is a crucial feature to force the backward evolution, a CA is said to be reversible, if there is a reversible rule that always gives the possibility to recover the initial state of CA [39]. In the above example, each cell at time $t+1$ depends solely on the states of its neighbors at the preceding time t, however, if such dependence is expanded to cover states of neighbors at the preceding times $t-1$, $t-2$, ..., etc, then the CA is said to be memory cellular automata (MCA). In this dissertation, both 1D 4 order reversible memory cellular automata, and $2D$ 4 order reversible memory cellular automata with Moore neighborhood are employed as tools in the design of efficient and secure cipher algorithms for image confidentiality, the mathematical background within these concepts is introduced in section 3.1 of chapter 3.

1.2.2 Preliminaries on Chaos theory

Chaos theory is a branch of nonlinear dynamical systems [75], that has been found in the second half of 20^{th} century [85], subsequent to the examination of a variety of dynamical systems, in which although the prior knowledge of their evolution rules, and initial conditions, their future appeared to be random and erratic [101]. The chaotic behavior has been also observed in various applications within different branches of knowledge, comprising engineering, biology, economics, etc. Nowadays, a series of interesting applications are revealed, among which chaotic cryptography, that is an area of permanent interest [76], especially after the advocacy of members of researchers, and their declaration about the existence of remarkable relationship between chaos and cryptography [7, 8].

1.2.2.1 Chaos and cryptography

As it was stated previously within section 1.2, Shannon within his most influential contribution to cryptography [112], introduced two paramount principles that must be achieved by any well-designed cryptosystem. Those principles are confusion and diffusion. The confusion principle of a secure cipher algorithm ensures that the ciphertext is statistically independent from the plaintext and the secret key, so that, any possible clue or leakage of information associated to either the plaintext or the secret key is concealed. Nevertheless, the diffusion principle aims to render a minor alteration at a bit unity on the plaintext or the secret key, conduct to significant changes on the ciphertext.

Along with Shannon's cryptographic contribution, a relationship between chaos and cryptography is established, in the sense that confusion and diffusion principles have their matching counterparts in the area of chaotic dynamical systems [76] .The diffusion principle within a chaotic system guarantees that any negligible alteration on its initial conditions, control parameters, or both, conduct to the product of a completely different

trajectory (or orbit), i.e., those generated chaotic orbits rely with a difficult way on the initial conditions and control parameters of the corresponding chaotic system. On the other hand, the confusion principle within a chaotic system ensures that by exploiting the produced set of chaotic orbits, it is not achievable to recover the correct values of the employed initial conditions and control parameters. So that, the mixing property and the ergodic feature of chaotic systems point to the independency to initial conditions with respect to control parameters. As a conclusion, dynamical systems are well-suited to be investigated as a base in the design of cryptosystems, if they exhibit chaotic behavior. In other words, if they point to the achievable confusion and diffusion principles in connection with the initial conditions and control parameters, see Figure 1.6.

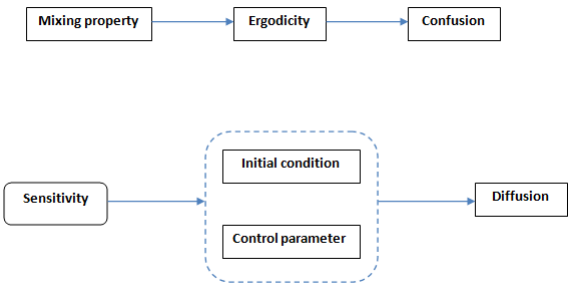


Figure 1.6: Relationship between chaos and cryptography

1.2.2.2 Fridrich typical chaos-based image cipher

In his paramount contribution to cryptography, Fridrich traced the core structure in the area of chaos-based cipher algorithms for image content preservation [54, 55]. The typical structure, see Figure 1.7, has been largely cited since 1997, and henceforth, advocated in a variety of proposals appeared in the scientific literature, see section 2.2 of chapter 2.

Fridrich typical paradigm comprises two iterative modules: confusion module and diffusion module. In the confusion module, each plain image's pixel is relocated with no occurred modification on its value, i.e., permutation at a pixel level, such shuffling is ruled by means of any appropriate 2D chaotic system, namely, Standard map, Cat map, and generalized Baker map, aiming to conceal the correlations among neighboring pixels under $n \geq 1$ permutation rounds. The confusion key is composed of the parameters of the employed chaotic dynamical system. The diffusion module is governed by a sequential mode of pixel-diffusing, and controlled by using a chaotic key-stream, for the sake of changing the statistical features of the plain image, in such a way a minor alteration on the plain image or secret key conducts to significant changes appeared over the entire corresponding

cipher image. The diffusion key consists of the parameters of the employed chaotic system. The overall confusion and diffusion modules are performed under m number of rounds, until reaching a sufficient level of security.

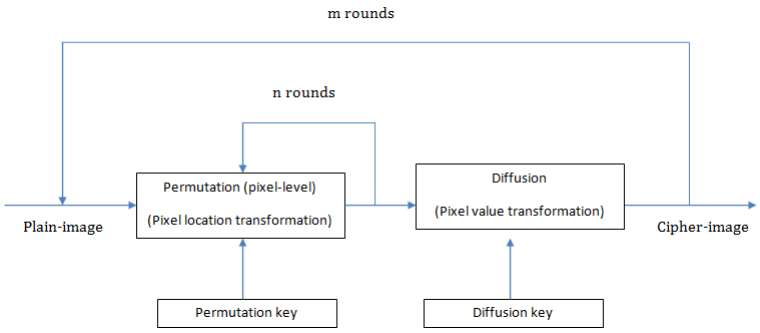


Figure 1.7: Typical chaos-based image cipher

The security of Fridrich chaos-based image cipher is studied in detail in [83]. According to which, the authors clarifies certain flaws related to the cryptosystem, and later some solutions were discussed to enhance the overall security of the cryptosystem, besides to the suggestion of some remarks to the appropriate choice of chaotic system, diffusion function, and the needed number of rounds. Moreover, the authors of [115] cryptanalyzed the Fridrich's cipher under chosen plaintext attack, by exploiting its algebraic flaws. The proposed attack aims to reveal the employed secret permutation instead of the underlying secret key, and it can be generalized to other ciphers that adopt the same structure as the Fridrich one.

1.3 Common and typical security aspects assessment tools

1.3.1 Statistical analysis

1.3.1.1 Uniformity analysis

The histogram is a commonly employed metric as a qualitative check of data distribution [57], for the sake of evaluating the robustness of the cryptosystem against statistical attacks. For a well-designed cryptosystem, such metric should conceal any noticeable information about either the plain image or the relationship between this latter and the cipher image. An image histogram is a graphical representation, that exhibits the distribution of pixel values, by plotting the amount number of pixels within every grayscale level value. The graphical representation of the cipher image histogram is important, but not sufficient to guarantee the uniformity of the cipher pixels distribution. To this end,

the Chi-square test is carried out to point to the uniformity feature of the given cipher image histogram. Such statistical test is calculated by the following formula [17, 47]:

$$X^2_{exp} = \sum_{i=1}^{Nv} \frac{(o_i - e_i)^2}{e_i} \tag{1.4}$$

Where Nv denotes the total number of levels (in case of grayscale image, Nv=256),o_i are the occurrence frequencies of each gray level (0-255), and e_i represents the expected occurrence frequency of the uniform distribution, and it is calculated as: e_i=$M \times N \times P/256$ (M is the number of rows, N number of columns and P is the number of plane, for grayscale image P=1).Experimentally, the Chi-square value for a well-designed cryptosystem should be less than the theoretical value, i.e.,$X^2_{exp} < X^2_{th}\ (256, \alpha)$=293 , where α=0.05 , represents the level of significance, and Nv=256.

1.3.1.2 Entropy analysis

Information entropy is a key metric for expressing the unpredictability and randomness of information, it is introduced by Shannon in 1948 [113]. As regards to the image information, the distribution of its grayscale values is computed, so that, the closer entropy to its theoretical value, reflects the more uniform the distribution of image grayscale values is. Let m denotes the information source, so the formula for measuring information entropy is:

$$H(m) = -\sum_{n=1}^{L} P(m_i) log_2 P(m_i) \tag{1.5}$$

1.3.1.3 Local entropy analysis

Shannon entropy [113] is a quantitative statistical test for randomness, it is referred by the authors of [138] as global Shannon entropy, in which it was pointed out its ineffectiveness to measure the true randomness of a given image. As a matter of fact, a new qualitative metric of randomness is proposed, namely, local Shannon entropy, this latter is based on the employment of global Shannon entropy over a series of local blocks within a given image. As regards to the methodology depicted in [138], the given cipher image is subdivided into 30 non-overlapping blocks of pixels, each of which has 1936 cipher pixels, the local Shannon entropy is the sample mean value of the global Shannon entropies of these 30 considered blocks of pixels, as a last step the obtained value follows hypothesis tests for the sake of making a qualitative measure on the subjected cipher image i.e., either to reject or accept it as a random image.

1.3.1.4 Correlation analysis

An image with its meaningful visual content, is featured by its high correlation and redundancy among neighboring pixels, either in horizontal, vertical and diagonal directions. A well-designed cryptosystem should conceal such relations between adjacent pixels, and exhibit a good performance of balanced 0-1 and zero correlation [43]. To assess the immunity of a given cryptosystem to such kind of attacks, first N pairs of neighboring pixels are randomly selected from the plain image and its corresponding cipher version in each direction. Then, the correlations of adjacent pixels within a given image are quantified by computing the correlation coefficient r_{xy} of each pair by means of the following formulas:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{1.6}$$

$$cov(x,y) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{1.7}$$

$$E(x) = \frac{1}{N} \times \sum_{i=1}^{N} x_i \tag{1.8}$$

$$D(x) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))^2 \tag{1.9}$$

Where x_i and y_i stand for the gray-level values of the i^{th} pair of the chosen neighboring pixels within the image, and N is the whole number of samples.

1.3.1.5 Nist statistical test for cipher images

The output of a well-designed cryptosystem should possess a sufficient immunity against any possible statistical attack within cryptographic applications. In general, statistical tests are widely employed for the sake of evaluating the randomness of Pseudo Random Number Generators (PRNGs) [100], however such tests can also adopted for the produced cipher texts [142]. In this context, National Institute of Standards and Technology (NIST) statistical tests suite [110] is employed, aiming to assess the randomness of the output cipher image.

1.3.2 Sensitivity test

1.3.2.1 Robustness against differential attacks

For the sake of secret key recovery, an attacker might attempt to distinguish any noticeable information between the plain image and its cipher version, by observing the influence of

a one pixel change on the whole cryptosystem output. A well designed cryptosystem is one in which a tiny alteration on its plain image conducts to a major transformation on its cipher image, and hence, such type of attacks is rendered void. To realize the experiment, the subsequent procedure should be adopted:

1. The plain image herein P_1 is encrypted to have a cipher image C_1.
2. The plain image herein P_2 is obtained by applying a minor change on a one randomly selected pixel, the altered plain image P_2 is encrypted under the employment of the same secret key to produce the corresponding cipher image C_2.

The influence is quantitatively measured by means of the two commonly used metrics [135, 136, 140]:

- Number of pixel change rate (NPCR): it computes the number of pixel differences between two cipher images herein C_1 and C_2, by means of the following formulas:

$$NPCR = (\frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} D(i,j)) \times 100 \tag{1.10}$$

Where N and M denote the image's width and height respectively, and $D(i,j)$ is defined as:

$$D(i,j) = \begin{cases} 0, if C_1(i,j) = C_2(i,j) \\ 1, if C_1(i,j) \neq C_2(i,j) \end{cases} \tag{1.11}$$

- Unified average changing intensity (UACI): it computes the average intensity of differences between two cipher images herein C_1 and C_2, by means of the following formula:

$$UACI = (\frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{|C_1[i,j] - C_2[i,j]|}{255}) \times 100 \tag{1.12}$$

1.3.2.2 Plain image sensitivity

For the sake of revealing the degree of sensitivity of the proposed cipher's input (i.e., plain image), and how much of dissimilarities can be achieved by its output, after a minor change on its input, the following procedure is handled: two plain images P_1 and P_2 , which differ by one randomly selected bit (the Least Significant Bit (LSB)), are enciphered to attain two cipher images C_1 and C_2, respectively. The hamming distance (HD) (in bits) between these two cipher images is computed by means of the following formula [47]:

$$P_s = \frac{\sum_{i=1}^{lb} C_1 \oplus C_2}{lb} \times 100 \tag{1.13}$$

Where lb is the length in bits of the plain/cipher images. The closer the hamming distance is to 50% (probability of bit changes), the more the designed cryptosystem achieves the avalanche effect, and hence, the plaintext sensitivity attacks are rendered void.

1.3.2.3 Key sensitivity

Another crucial property required by a well-designed cryptosystem, is its sensitivity to secret key, which conducts to produce completely different ciphertexts, under a minor change on the secret key (at a bit-unity). In other words, an attacker with a partly correct guess of the key, is unable to reveal parts from the plaintext [57]. In practice, the following scenario is adopted for key sensitivity assessment:

1. The plaintext herein P is encrypted by the secret key K_1 to produce the ciphertext C_1.

2. The secret key herein K_2 is altered with a minor change at a bit-unity, and then the encryption of the plaintext P is performed using the modified key K_2 to obtain the ciphertext C_2.

The influence is quantitatively measured by means of the hamming distance metric (see equation 1.13), and the percentage of difference between each pair of ciphertexts C_1 and C_2 using the following formula:

$$Diff = (\frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} sg(C_1(i,j) - C_2(i,j))) \times 100 \tag{1.14}$$

Where M is the number of image's rows, and N is the number of image's columns, and $sg(x)$ is defined as follows:

$$sg(x) = \begin{cases} 0, if x = 0 \\ 1, if x \neq 0 \end{cases} \tag{1.15}$$

1.3.3 Key space analysis

A well designed cryptosystem is one in which the best attack is an exhaustive search (i.e., brute force attacks) [74]. Owing to the remarkable growth in computational power, the key space has to be no smaller than 2^{128} [51, 104].

1.3.4 Performance analysis

1.3.4.1 Computational speed analysis

Time consuming is also a crucial factor to be considered, with respect to the security level, in the design of a secure cryptosystem. Therefore, a good combination between computational performance and satisfactory level of security is more than essential, especially for real-time applications scenario. The performance of a given cryptosystem is determined by the running speed assessment, such latter is computed by means of the average encryption/decryption times.

1.3.4.2 Computational complexity analysis

Another way to evaluate the performance of a cryptosystem in terms of theoretical aspects, is to calculate its computational complexity. This latter is quantified by means of the arithmetic operations constituted each cryptosystem's procedure, and it is denoted in term of big-O notation [141].

1.4 Conclusion

This thesis deals with the incorporation of dynamical systems in the area of cryptography, in the sense of investigating the desirable properties of dynamical systems, and their simple mathematical representation in the design of secure and efficient cryptographic algorithms that are best suited for image content preservation. The chapter is mainly comprised three sections. Section 1.1 is subdivided into two subsections: first of all, cryptology as a science that studies both the art of designing and breaking cryptosystems is introduced, then, a brief history of cryptography along with its foundation, in addition to its essential concepts are covered in subsection 1.1.1, as a latter part, the cryptanalysis as a branch of cryptology, interested by breaking the security of cryptosystems based on some commonly used types of attacks is discussed in subsection 1.1.2. Section 1.2 aims to give the basic notions and terminologies behind dynamical systems, in which cellular automata (CA) as a type of dynamical systems, and the primary investigated tool within this thesis in the design of cryptosystems, its preliminary overview is discussed within subsection 2.1.1, as the last part, chaos as another type of dynamical systems, and the second investigated tool within this thesis in the design of cryptosystems, its preliminary overview is presented within

subsection 2.1.2.Section 1.3 introduces some common and typical security assessment tools that are employed to evaluate the effectiveness of the designed cryptosystem in terms of security level and time performance, and ensure its resistance to cryptographic attacks.

Chapter 2

A review on different image encryption methods

For decades of years, researchers investigate and develop innovative methods for image content protection. This chapter puts a focus on those methods involve the use of cellular automata-based dynamical systems and chaos-based dynamical systems, and it is structured as follows: a review on some relevant existing methods based on cellular automata (CA), cellular automata jointly chaos is presented in section 2.1. Section 2.2 concerns existing methods employ chaos based dynamical systems. A comparative study in term of the commonly used cryptographic attacks to break the security of a cryptosystem is given in section 2.3. At the end, section 2.4 concludes this chapter.

2.1 Cellular automata, cellular automata jointly chaos based methods

The idea of using cellular automata as a base to design efficient cryptographic techniques refers first to the studies of Steven Wolfram [133]. After, the investigation of CA concept in the field of cryptography has become a hot research topic, interpreted in the large number of CA-based ciphers proposed in the scientific literature. This section aims to review the most salient existing methods for image encryption.

2.1.1 Cellular automata based methods

Chen et al. [31] presented a novel cipher algorithm for image security. The proposal is based on the employment of cellular automata mechanism, and its membership to the iterated product cipher framework. The basic idea within the contribution is to change the pixel values by means of data reformation keys step, and CA substitution step. The

former step is ruled by 2D Von Neumann CA to produce CA keys, whereas the second one is governed by a recursive CA mechanism to modify the pixel values, and controlled by means of the generated CA keys of the previous step. Both steps are arithmetic and logical operations based. The proposed method is characterized by its membership to lossless encryption category, large key-space, good confusion and diffusion properties, and the ability to withstand the most considered cryptographic attacks such as cipher image only attacks and chosen cipher image attacks, however known/chosen plain image attacks can be made possible but more difficult than the ones enciphered data streams.

Chatzichristofis et al. [24] introduced a new encryption scheme for visual multimedia content. The proposal is based on the incorporation of Coordinate Logic-Filter-XOR (CLF-XOR, for short) and cellular automata, in which is considered as a buffered stream cipher technique, since the encryption is performed for only one byte at a time. Two key images are employed during the encryption process, the former key image is featured by its same dimensions as the plain image, whereas the second one is generated by means of the structure of an artificial image, this latter is relied on the use of superposition of 1DCA time space diagrams, and a random number generator based-CA. The method is characterized by its membership to lossless encryption category, and for each time the algorithm is executed, different cipher images are produced under a giving key image, even with the use of the same key image. An implementation using C# programming language of the proposal is available online through the img(Rummager) application.

A new and simple image encryption scheme is presented in [68]. The proposal is based on the simplest class of cellular automata, namely, elementary cellular automata (ECA, for short) of length 8 under periodic boundary conditions, such kind of CA is investigated, for the sake of achieving a simple hardware structure and reducing the computational resources for real time application requirements. The encryption and decryption procedures are performed by means of attractors, these latter are produced by the evolution of ECA under a chosen rule and initial state (stateone). The attractor is considered as an encryption function, according to which each plain image pixel value is changed by the state of this attractor, the number of times parameter for enciphering each pixel value is calculated using a pseudo-random number generator (PRNG) with a seed. The proposed scheme belongs to lossless encryption category, its secret key is composed of the used transition rule, stateone and the seed of PRNG, and it is best suited for both grayscale and color images. The given extensive experimental results and performance evaluation reveal the effectiveness of the algorithm, in term of sufficient security and fast execution time, on the other hand this designed scheme wasn't adapted for binary images, since each attractor of ECA is featured by its 8 state mostly, this weakness was noticed by the author to be the focus of a future work.

Abdo et al. [1] suggested a novel and simple image encryption algorithm. The proposal is based on elementary cellular automata (ECA) under periodic boundary conditions and unity attractors, in conjunction with cellular neural network (CNN, for short). The secret key is composed of the initial conditions and control parameters of CNN system, the two employed rules and unity attractors. First of all, the CNN system is iterated to generate three one-time chaotic key-streams used in the encryption procedure, in which its control parameters are plain image related, then, these chaotic sequences contributed in the phase of determining the selected rule for pixel ciphering, and the number of the states used in the encryption function (unity attractor), it should be noticed that the rule states employed in the encryption process are dissimilar from that of the decryption one, after that, the encryption is governed by means of modular arithmetic addition (mod 256), and bitwise XOR operations. Due to the mechanism of generating chaotic key-streams is based on the plain image features, any alteration on this latter conducts to different parameters, and thus distinct key-streams, which renders the proposed algorithm has the capacity to resist some of known plain image/cipher image attacks. The given extensive experimental results and performance evaluation reveal the effectiveness of the algorithm, in term of sufficient security and fast execution time.

A novel image encryption scheme is introduced in [90]. The proposal is based on a specific type of cellular automata, namely, 1D reversible cellular automata (RCA, for short), with respect to its membership to the category of block ciphers. The encryption procedure is carried out by means of a special class of RCA, i.e., reversible second order cellular automata, according to which the pseudo random permutation (PRP, for short) is constructed, this PRP is contributed as a base to design a new parallelizable encryption algorithm. As the first step, the plain image is divided into fixed length blocks of 256 bits, then, the encryption of each block is performed as follows: the PRP is a function Φ that takes as input the secret key K, and the nonce n_i (variable for each plain block), and the plain block PB_i to produce the corresponding cipher block CB_i as output, as a last step, the encrypted blocks are rearranged to form the final cipher image. The function Φ is defined using the following equation [90]:

$$\Phi : I^{128} \times I^{32} \times I^{128} \rightarrow I^{256} \tag{2.1}$$

$$(k_i, n_i, PB_i) \rightarrow CB_iF(k_i, n_i, PB_i) \tag{2.2}$$

The given extensive experimental results and performance evaluation reveal the effectiveness of the algorithm, in term of sufficient security and fast execution time.

A novel cipher algorithm for fast authenticated and randomized encryption is introduced

in [50]. The proposal is based on the use of a special class of cellular automata, namely, second order reversible cellular automata, characterized by its membership to block cipher category, and its specialization on text data encryption. First of all, the plain text is divided into fixed block length of 256 bits, then, a mixing step is handled for each plain block, this latter is ruled by means of XOR bitwise operation and addition arithmetic operation (modulo 256), after that, an encryption step is performed to each resulted block, this step is based on evolving the RCA mechanism under a transition rule for n times of iterations, moreover, another mixing step, that is based on addition arithmetic operation (modulo 256) and XOR bitwise operation, is applied to the cipher block resulted from the previous step, to have a final cipher block, the process is carried out for all the plain text blocks sequentially, as a final step, the resulted final cipher blocks are rearranged to form the cipher text. The decryption procedure is as equal as the encryption one, running in backward direction with the same transition rule. The proposal is carried out under just one round, in which it can perform two cryptographic objectives, namely, the encryption as it is explained above, and the integrity, this latter is carried out as follows: to perform the RCA mechanism under second order, we have to start with two configurations (i.e., pre-initial data, and the first plain block), and to end with two configurations as well, namely the first one is the cipher block and the latter is a final configuration, the author exploited the final configuration (256 bit length), to ensure plain text authentication, according to which this extra data is splitted into two sub blocks of 128 bits each one, and the key extension mechanism is applied in the reverse direction, to recover at the end of this step two configurations of 128 bits length, if these latter match to the random initial data as the first recovered configuration, and the secret key as the second one, we confirm that the cipher text is not altered, otherwise we ensure that a modification is occurred in the cipher text during transmission. The given extensive experimental results and performance evaluation reveal the effectiveness of the algorithm, in term of sufficient security and fast execution time, besides to its capacity to resist both known/chosen plain text attacks (CPA secure), and chosen cipher text attack (CCA secure).

2.1.2 Cellular automata jointly chaos based methods

Martin del Rey et al. [41] presented a new cipher algorithm for image encryption. The proposal is based on discretized cat map, cellular automata and permutation-diffusion architecture under 6 number of rounds. At the confusion stage, plain-image's pixels are permuted using discretized cap map that displays good cryptographic features. At the diffusion stage, the values of the confused-image's pixel are changed sequentially using one-dimensional (1D) reversible cellular automata (RCA), aiming to diffuse the effect of one pixel overall the other image pixels, the cipher image is obtained at the end of this process. An extension of the proposed work [41] is given in [42] with the same authors, in which the confusion phase remains the same whereas in the diffusion phase two-dimensional

(2D) reversible memory cellular automata (RMCA, for short), with Moore neighborhood is investigated instead of 1D cellular automata. From the given security results, the two proposals possess acceptable security level, however this latter can be achieved under some number of rounds, besides to the use of higher dimensional chaotic map, which are indeed two time consuming factors, hence, these cipher algorithms have really slow execution time.

Wang et al. [130] suggested a novel image encryption scheme. The proposal is based on the incorporation of reversible cellular automata (RCA) with chaos. The confusion phase is ruled by means of the generated chaotic sequences using intertwining logistic map, with complex chaotic behavior, as a former step, each plain image pixel is divided into two units of 4 bits each one, then, these units are shuffled under the control of the chaotic sequences, aiming to not just change the pixel position but its value as well, to further introduce a certain diffusion effect within just this phase. The diffusion phase is governed by 2D periodic boundary RCA, and applied to just the higher 4 bits of the confused image's pixels, since it was found that these 4 higher bits contain 94.125 % the total pixel's information, this phase is iterated for many number of rounds to attain the cipher image. The given extensive experimental results demonstrate the sufficient security level of the proposed cipher algorithm, besides to its immunity against the most known cryptographic attacks.

Bakhshandeh et al. [11] suggested a novel image encryption approach. The proposal is based on the employment of a special class of memory cellular automata (MCA, for short) combined chaos. In the permutation phase, a Piecewise Linear Chaotic Map (PWLCM) is adopted to permute the pixels of the plain-image at the pixel level, the generated chaotic sequences are key-related. In the diffusion stage, both logistic chaotic map and 1D linear memory cellular automata (LMCA, for short) are employed, in which the permuted image is divided into blocks of equal sizes. For every block, its hash value is computed to handle the authentication purpose (i.e., verify the integrity of the original image), after it is enciphered using both 1D LMCA and logistic chaotic map to obtain the cipher image, it should be mentioned that the generated chaotic sequences in this phase are both key/plain-image related, however the generated key-streams in the permutation have no relation with the characteristics of the plain-image, this failing is exploited in [69] to break the security of the cryptosystem under chosen plain-text attack, and it was noticed that a total breaking using brute force attacks is possible, besides to the low sensitivity to plain-image that is experimented, and lead to the non-resistance to differential attacks. So, the generated key-streams in both the permutation and diffusion modules should have a dependency to plain-image characteristics, to avoid the commonly used attacks to break cryptosystems i.e., known/chosen plain-text attacks [67], in addition to that some suggested improvements are illustrated and experimented in [69] to enhance the sensitivity to plain-image and withstand all the aforementioned attacks.

Wang et al. [131] presented a new image encryption scheme. The proposal is based on the combination of Langton's Ant cellular automata and chaos. First of all, the plain image is converted to 1D array of pixels, then, the Langton's Ant cellular automata mechanism is adopted to scramble these pixels, under the controlling of the generated chaotic sequences using intertwining logistic map in the confusion phase, as a final step, each confused pixel is diffused by adopting a sequential mode, under the controlling of the generated chaotic sequences using Piecewise Linear Chaotic Map (PWLCM, for short), to attain the cipher image. The given extensive experimental results demonstrate the sufficient security level of the proposed cipher algorithm, besides to its immunity against the most known cryptographic attacks.

Martin del Rey et al. [43] suggested a new encryption algorithm for RGB digital images. The proposal is based on the incorporation of 2D chaotic cat map, with reversible memory cellular automata (RMCA, for short). First of all, the plain image is splitted into its three components, namely, R, G, and B channels, each component is represented by a matrix, in which the permutation is handled at a pixel level, and controlled by a different 2D chaotic cat map, this phase it iterated for n number of rounds. Each confused matrix is then diffused by means of a special family of CA, namely, RMCA over F_2^8 under m number of rounds. The proposed cipher is performed for some number of rounds, in which the initial values of both 2D chaotic cat map, RMCA, and the number of iterations in both confusion and diffusion is generated by following an efficient key scheming. The given extensive experimental results validate the sufficient security level of the proposed cipher algorithm, besides to its immunity against the most known cryptographic attacks.

An encryption algorithm for RGB digital images is introduced by Yaghouti Niyat et al. [96]. The proposal is based on the conjunction of non-uniform cellular automata framework and chaos. As a former step, the plain image is subdivided into its three components, namely, Red, Green, and Blue ones, then, a permutation phase is carried out at a pixel level by means of the generated chaotic sequences of 3D Arnold cat map, after that, a key image with the same size of the plain image to be encrypted is generated, using 1D non-uniform cellular automata, in which 8 transition rules are adopted, namely, 165,105,90,150,153,101,30 and 86, with periodic boundary conditions, the initial configuration of 8 cells of CA is produced using 1D logistic chaotic map, this latter is also contributed in the selection of the used transition rule within the mechanism of key image generation, as a final step, the Chen hyper chaotic map is performed to select values from the produced key image, for the sake of image encryption, after applying all the aforementioned steps, the image components are combined to form the final cipher image. The given extensive experimental results validate the sufficient security level of the proposed cipher algorithm, besides to its immunity against the most known cryptographic attacks.

2.2 Chaos based methods

Most of chaotic proposals to cipher digital images typically follow the classical architecture suggested by Fridrich [55], which turned out to be the most referenced and salient work in the area of image encryption. During the last two decades, remarkable efforts were devoted to improve the typical Fridrich's paradigm, which can be viewed in various aspects, and interpreted in the large number of Chaos-based image ciphers proposed in the scientific literature. This section aims to review the most relevant existing methods for image encryption.

Gao et al. [58] presented a new cipher algorithm for image content protection. The proposal is based on the employment of total shuffling matrix, logistic chaotic map, hyper-chaotic system, and under the adoption of confusion-diffusion architecture. In the confusion stage, the plain-image is considered as two-dimensional arrays, and both image's rows and columns permutation are applied using two generated chaotic sequences of one dimensional (1D) logistic chaotic map, in order to de-correlate the relationship between adjacent pixels. In the diffusion stage, a hyper-chaos and XOR operation are performed to obtain the final ciphered-image. The proposed approach has the superiority of using hyper-chaos system as a base to design new crypto-systems for image encryption, a tiny modification in the secret key leads to a totally different cipher image i.e., sensitivity to secret key is achieved, besides to the large key space which leads to the immunity of the crypto-system against brute force attacks. On the other hand, the use of 1D logistic map in the confusion stage weakens more the scheme in which such kind of maps is clarified in [9] to not be selected as a base of chaotic crypto-systems, the sensitivity to plain-image's small modifications is low, and the generated chaotic sequences that are employed in both confusion and diffusion stages are unchangeable whatever the used plain-image, this failing makes the crypto-system vulnerable to known/chosen plain-text attacks. Moreover, by exploiting the low sensitivity to plain image's tiny modifications, and the non-changeable generated key-streams in both confusion/diffusion, the proposed approach [58] is cryptanalyzed by the authors of [107], in which three couples of plain-images/cipher images are sufficient to break totally the cryptosystem by chosen plain-text attack (CPA), and chosen cipher-text attack (CCA), further more the same authors suggested to modify only the diffusion phase, by making the generated key-streams plain-image related. More recently in [149], the improvement of the cryptosystem of [107] is analyzed in detail, according to which it was found that even after the improvement of [107] , the cryptosystem still suffer from the low plain-image change and the non-resistance to known/chosen plain-text attacks, and the authors of [149] enhanced the security of the cryptosystem by making both confusion/diffusion phases plain-image related, so experimented results and simulations clarified that the cryptosystem becomes more sensitive to plain-image change and CPA secure.

The work reported in [151] introduced a new cipher algorithm for image encryption. The proposal is based on 2D Arnold cat map, logistic chaotic map, permutation at bit-level, and under the adoption of confusion-diffusion architecture. In the confusion stage, each plain-image's pixel is divided into its composed 8 bits, the positions of these bits are relocated using the generated chaotic sequences of cat map. According to the found results of that the higher 4 bits of each pixel (i.e., 8^{th},7^{th}, 6^{th} and 5^{th}) hold how about 94.125 % of the whole image's information and the lower 4 bits (i.e., 4^{th} ,3^{rd}, 2^{nd} and 1^{st}) hold less than 6 %, two different approaches are proposed to shuffle these two groups (i.e., the first is 4 higher bits and the second is 4 lower bits). At first, an independent permutation is performed for each bit of the first group using generated sequences of cat map with different coefficients. Then, the second group is considered as a whole in permutation to decrease the runtime. The notable effect of this permutation is not only the location of each pixel is changed but also its value as well making the possibility of achieving confusion and diffusion possible in this stage. In the diffusion stage, the classical Fridrich's diffusion is adopted (i.e., the encryption of pixels is performed sequentially at a pixel level) using generated sequences of logistic chaotic map. The proposed approach is featured by its large key space which leads to the immunity of the cryptosystem against brute force attacks, the permutation phase is performed at a bit level leading to achieve both confusion and diffusion effects within only this phase, to further enhance the diffusion mechanism of the cryptosystem, high sensitivity to secret key, plain image and good statistical results are exhibited, in addition to the employment of higher-dimensional chaotic map (i.e., 2D cat map) that can overcome the drawbacks of one-dimensional (1D) chaotic maps. On the other hand, the produced chaotic key-streams in both confusion and diffusion modules have no dependency to the characteristics of the plain-image, which leads to the failing of non-resistance to known/chosen plain image attacks, the investigation of 1D logistic chaotic map in the confusion stage weakens more the algorithm, in which such kind of maps is clarified in [9] to not be selected as a base of chaotic ciphers. The security of the cryptosystem is analyzed in detail in [147], so besides to the aforementioned limitations especially that of the generated chaotic sequences in both confusion and diffusion stages are unchanged whatever the given plain-image, that is considered quite sufficient to break the cryptosystem under chosen plain-image attack, another flaws are shown as: the first pixel (0,0) remains unchanged during all the permutation phase, the connectivity between pixels exists only in the same groups, the fixed value of the parameter α=4 increases the insecurity of the cryptosystem, and even the use of 1D logistic chaotic map is unsuitable as a base to design cryptosystems due to its limitations [9]. An improved scheme is proposed with the authors of [147] to overcome the limitations of the original work [151], in which the following considerations are taken into account: 1. The encryption procedure is introduced as the first stage, then a bit-level permutation is applied using Arnold cat map, 2. Incorporation of the characteristics of the plain-image at the permutation stage,

3. Flipping the sub-images that are obtained from the groups of bits is handled as a solution to make the first pixel changeable, and as a last improvement, 4. For the sake of changing the parameter , it should be set to the value of the final parameter of the secret keys.

An image encryption algorithm is presented by the authors of [137]. The proposal is based on two-dimensional logistic map, and adopted the permutation-diffusion architecture under some number of rounds. In the permutation stage, the plain-image is considered as a matrix i.e., 2D array of M rows and N columns, using the 2D logistic map, two chaotic sequences are generated of $M \times N$ length, and after they are reshaped to form two matrices, to further perform row/column shuffling relied on these generated matrices to obtain the permuted image. In the diffusion stage, the permuted image is divided into $S \times S$ blocks, where S is the length of the block of pixels determined by the plain-image's format (4×4 for grayscale/RGB images and 32×32 for binary ones), and then each block is encrypted with the generated sequences of 2D logistic map. A transposition step is added which aims to shift each diffused image's pixel, using a reference image generated by means of 2D logistic map from the previous step, and hence, the cipher image is attained after accomplishing such final operation. The proposed approach is featured by its large key-space, high sensitivity to both key/plain image minor alterations, and the employment of higher-dimensional chaotic map herein 2D logistic map that can overcome the drawbacks of one-dimensional (1D) chaotic maps. On the other hand, it should be mentioned that the generated chaotic sequences have no dependency with respect to the characteristics of the plain-image, that may lead to the non-resistance to known/chosen plain-text attacks.

Mirzaei et al. [89] introduced a new cipher algorithm for image security. The proposal is based on the employment of chaotic systems, the parallel enciphering, and the adoption of confusion-diffusion architecture. As a primary step, the original image is subdivided into 4 equal sub-images, in which the position of each sub-image is scrambled using 4 generated chaotic numbers of logistic chaotic map. In the confusion stage, both row/-column permuting is carried out by means of two generated sequences of logistic chaotic map to obtain the shuffled-image. In the diffusion stage, both Lorenz and Chen's systems are used to generate 15 groups used in encryption, each pixel of the shuffled-image that is subdivided into four equal blocks (sub-images) is enciphered using the matching pixel value of the plain-image, the value of other block and the values of corresponding chosen group. The generated chaotic sequences that are used in both confusion/diffusion stages are key-related. The proposed approach is featured by its large key-space, and high sensitivity to both key/plain image small modifications. On the other hand, and as it was aforementioned, the produced chaotic sequences in both confusion and diffusion modules have no dependency to the characteristics of plain-image, which conducts to the failing of non-resistance to known/chosen plain-text attacks (i.e., the scheme is not CPA secure).

Yang Song et al. [117] presented a new cipher algorithm for image content protection. The proposal is based on a new spatiotemporal chaotic system, nonlinear chaotic map (NCA) and permutation-diffusion architecture. As a primary step, the plain-image is converted to a one dimensional (1D) array of pixels in which a bitwise XOR operation is applied between pixels, to obtain the diffused image. In the confusion stage, the sum of plain-image's pixels is calculated and the results is converted to [0,1] range, and used as initial condition to produce the key-stream of NCA map, as a solution to make the generated sequences changeable and plain-image related, a pixel permutation between the diffused image and the generated key-stream is performed to obtain the shuffled image. In the diffusion stage, the generated spatiotemporal chaotic sequence is employed to diffuse again the shuffled image, by means of bitwise XOR operation. The proposed approach is featured by its large key space, high sensitivity to both key/plain image small modifications, and the produced chaotic sequences in the permutation phase is plain-image's related (i.e., changeable with any change applied to the plain-image). On the other hand, the produced chaotic sequences for the diffusion phase are independent from the processed plain-image, this failing is exploited in [13] to break the security of the cryptosystem under chosen plain-text attack, and it was noticed that a total breaking is possible however under a large number of plain-image/ciphered image pairs. So, the generated key-streams in both permutation and diffusion modules should have a dependency to plain-image characteristics, to avoid the commonly used attacks to break cryptosystems i.e., known/chosen plain-text attacks [67].

A new cipher algorithm for image encryption is presented by the authors of [148]. The proposal is based on the integration of two existing one-dimensional (1D) chaotic maps, aiming to introduce a number of chaotic maps with excellent chaotic behaviors. The performance of the proposed chaotic system is experimented, in which larger ranges with respect to excellent chaotic properties are found, such desirable features can easily overcome the limitations of 1D chaotic maps: of discontinuous range, non uniform data distribution, shorter periodicity, small key space ... etc. Furthermore, these results are investigated to design a new image cryptosystem that is performed overall 4 encryption rounds. In each round, a random pixel is inserted in the beginning of each image's row as the first operation, after row separation, 1D substitution, row combination, and image rotation are performed to produce the cipher image. The proposed approach satisfied all the searched cryptographic properties of a good cipher of confusion, diffusion, besides to the randomized encryption property, i.e., using the same set of keys with the same original plain image in each time the algorithm is able to generate a completely different, non-repeated cipher images. This latter ensures the resistance to the commonly used attacks for breaking the security of cryptosystems, namely, chosen/known plaintext attacks.

Another image encryption algorithm based on mixing the use of chaotic system with s-box substitution is proposed by Attaullah et al. in [10]. The employed chaotic system is relied on that investigated in [148] i.e., the combination of two existing one-dimensional (1D) chaotic maps (seed maps). The proposed approach is considered as an extension of [148], by engendering S-box substitution, and it is performed under 4 encryption rounds. Each round is composed of six steps, at first an arbitrary pixel is inserted at the beginning of each plain- image's row, in which this latter is separated and considered as a 1D data matrix, a substitution is applied to change the value of each pixel in 1D matrix, a rotation of 90 degrees counter clockwise is handled, and as a last step each pixel is substituted by values from S-boxes, the process is repeated four times to obtain the final cipher image. The performance of the cryptosystem is experimented, in which excellent confusion and diffusion properties are obtained, the resistance to chosen/know plaintext attacks is achieved, due to the arbitrary encryption, besides to data loss and noise attacks as well.

El Assad et al. [47] introduced a new cipher algorithm for image content protection. The proposal is based on a modified version of 2D Arnold Cat map, permutation at bit-level, the membership to block ciphers with CBC mode category, and the adoption of confusion-diffusion architecture. In the diffusion stage, the plain-image is divided into blocks of 32 bytes, and the process is governed by means of binary matrix of size 32×32 in combination with XOR bitwise arithmetic operation, and it is performed under rd number of rounds, aiming to achieve a local diffusion. In the confusion stage, a conversion from integer to binary type is performed as the first step, and then a bit permutation is carried out using a modified version of 2D cat map, that are more powerful than the usual employed one, at a bit unity level, according to which not only the pixel position is modified but also its value, that reflect the achievement of both confusion and diffusion at the permutation layer, the process is performed under rp number of rounds, after that a conversion type from binary to integer is handled to pass to the next round, with such manner the cryptosystem is repeated for r rounds. The used generator for producing the needed chaotic key-streams for the cryptosystem is based on the one proposed in [48]. The proposed approach is characterized by its large key-space, high sensitivity to both key/plain image small modifications, besides to the employment of higher-dimensional chaotic map (i.e., a modified 2D cat map) that can overcome the drawbacks of one-dimensional (1D) chaotic maps. On the other hand, the cryptosystem is handled under a CBC mode (a sequential mode) i.e., any error that affects the transmitted cipher image at a bit unity level leads to the alteration of the remaining bits after that one (i.e., the transmission of the error).

Murillo-Escobar et al. [94] proposed a new cipher algorithm for color image encryption. The proposal is based on the employment of chaotic system, the plain image features for producing one-time chaotic sequences, and the adoption of confusion-diffusion architecture under only one encryption round. The proposed contribution is ruled by means of

an optimized pseudorandom chaotic sequence, and controlled by 1D logistic map with optimized distribution, for the sake of fasten the encryption procedure, and overcome the drawbacks of one-dimensional (1D) chaotic maps of discontinuous range, non-uniform data distribution, ... etc, the overall cryptosystem steps are relied on the one proposed by the same authors in [93]. The produced chaotic sequences are relied totally on the plain image characteristics and the used external secret key, aiming to withstand chosen/known plain-image attacks. Numerical simulations were performed to demonstrate the effectiveness of the proposed approach to be used in practical applications.

The authors of [66] presented a new cipher algorithm for image encryption. The proposal (LAS-IES) is based on two-dimensional Logistic-adjusted-Sine map (2D-LASM), mechanism of inserting random values to plain-image, and the adoption of confusion-diffusion architecture under two encryption rounds. The proposed 2D chaotic map herein 2D-LASM is featured by its large chaotic range, unpredictability, and a good ergodicity comparing it with several existing chaotic maps, this chaotic map is investigated as a base to construct the LAS-IES algorithm. The produced chaotic sequences that are used within the cryptosystem are key-related, however the mechanism of inserting random values that is applied firstly to the plain-image makes the scheme performing a randomized encryption (RE), i.e., in each time the operation of encryption is executed with the same plain-image/used secret keys, the algorithm is able to produce a new cipher image, such mechanism ensured the resistance to both known/chosen plain-image attacks. In the confusion stage, plain-image's pixels are shuffled at a bit level, to further achieve both confusion and diffusion in the permutation phase. In the diffusion stage, a sequential mode of encrypting pixels is adopted (i.e., for enciphering a new pixel, the previous one is utilized) with the generated chaotic matrix from 2D-LASM. The proposed approach is featured by its large key-space, high sensitivity to both key/plain image little alterations, the scheme performs a random-like enciphering (i.e., a randomized encryption (RE)), in addition to the employment of new 2D chaotic map with excellent chaotic behavior in comparison with several existing chaotic maps in the scientific literature.

A novel image encryption algorithm is suggested by the author of [45]. The proposal is based on the use of chaotic system, a newly proposed bit-level permutation based confusion, and the adoption of permutation-substitution model. The confusion stage is ruled by means of a newly proposed permutation strategy, namely, Circular inter-intra pixels bit-level permutation, the idea within such mechanism is firstly to transform each plain image's row to its binary equivalent format, and then the circular rotations are performed and controlled by means of chaotic sequences, the number of circular shifts and its direction are extracted from the accumulation of the logical value 1, if the obtained number value is divisible by eight, then the permutation is handed at a pixel level, otherwise at bit-level will be the case. Moreover, the mechanism of bit migrating from one pixel to

another one next to it, is referred as inter bit-level permutation by the author, and bit passing from one bit-plane to another is referred as intra pixels bit level permutation. Within the diffusion stage, the resulted scrambled image is encrypted by means of two uncorrelated produced chaos-based matrices to attain the final cipher image. Numerical simulations were performed to demonstrate the effectiveness of the proposed approach to be used in practical applications.

Li et al. [81] introduced a new cipher algorithm for image security. The proposal is based on the employment of 5D multi-wing hyper chaotic-system, and the incorporation of pixel-level permutation with bit-level permutation. As a first step, the plain image is converted to 1D array of pixels format, then the sum of all image's pixels are calculated, and contributed in the mechanism of producing chaotic sequences by means of hyper chaotic system, after that a permutation at a pixel-level is handled, aiming to de-correlate the relations between adjacent pixels, and attain the shuffled image. Within the second step, a bit-level permutation is handled, according to which the shuffled image is subdivided into sub-matrices of 4×4 each, and then this latter is multiplied with a constant matrix of the same size, such kind of permutation is carried out to further modify both pixel position and value, aiming to enhance the diffusion effect of the cryptosystem, and thus, strengthen its security. As a final step, a sequential mode of pixel diffusing is handled, and controlled by means of the produced one-time key-stream of hyper chaotic system to obtain the final cipher image. Numerical simulations were performed to demonstrate the effectiveness of the proposed approach to be used in practical applications.

Xu et al. [139] proposed a novel cipher algorithm for image content protection. The proposal is based on the use of chaotic system, block scrambling, and the adoption of confusion and diffusion model under one encryption round. First of all, the plain image is subdivided into two equal sub-images. In the confusion stage, two chaotic matrices are generated using 1D logistic chaotic map and two secret keys, these produced matrices are contributed in the mechanism of constructing swapping control table, x coordinate table and y coordinate table, according to which each plain pixel within the two sub images blocks is relocated. After combining the two scrambled sub images, the resultant image is transformed to 1D array of pixels, and a diffusion mechanism is handled, this latter is ruled by means of XOR arithmetic operation and the computed dynamic indexes, to further attain the final cipher image. Numerical simulations were performed to demonstrate the performance of the proposed approach in term of security level and speed of calculations.

2.3 Comparison of different methods in the literature

A comparative study in term of the commonly employed cryptographic attacks such as: exhaustive key search, known-plaintext attack, chosen-plaintext attack (CPA), chosen ciphertext attack (CCA), and differential/ statistical attacks is given, including the reviewed existing methods. Table 2.1 exhibits the obtained comparative results of all the reviewed methods.

Table 2.1: Comparative results in term of the commonly cryptographic attacks, including the reviewed methods

Method	Resistance to exhaustive search	CPA secure	CCA secure	Resistance to differential/statistical attacks
Ref. [31]	yes	no	yes	yes
Ref. [24]	yes	yes	no	yes
Ref. [68]	yes	no	no	yes
Ref. [1]	yes	yes	no	yes
Ref. [90]	yes	yes	no	yes
Ref. [50]	yes	yes	yes	yes
Ref. [41]	yes	no	no	no
Ref. [42]	yes	no	no	no
Ref. [130]	yes	no	no	yes
Ref. [11]	no	no	yes	no
Ref. [131]	yes	yes	no	yes
Ref. [43]	yes	no	no	yes
Ref. [96]	yes	no	no	yes
Ref. [58]	yes	no	no	no
Ref. [151]	yes	no	no	yes
Ref. [137]	yes	no	no	yes
Ref. [89]	yes	no	no	yes
Ref. [117]	yes	no	no	yes
Ref. [148]	yes	yes	no	yes
Ref. [10]	yes	yes	no	yes
Ref. [47]	yes	no	no	yes
Ref. [94]	yes	yes	no	yes
Ref. [66]	yes	yes	no	yes
Ref. [45]	yes	no	no	yes
Ref. [81]	yes	yes	no	yes
Ref. [139]	yes	no	no	yes

2.4 Conclusion

Several image encryption methods are proposed in the scientific literature based on different strategies such as cellular automata, chaos theory, or cellular automata jointly chaos.

Nevertheless, most of these methods suffer from some security failings that lead to their broken either by: brute force attacks in case of small key-space; differential attacks in case of low diffusion effect that lead to low NPCR and UACI values; statistical attacks in case of any detectable clue that can reveal any meaningful information about the original data; or the generated chaotic key-streams that are key-related i.e., that they are unchangeable in each encryption process, this latter is the commonly used failing even in the design of new chaotic proposals, which conducts to the non-resistance to both known/chosen plain-text attacks, as a solution to overcome this limitation several crypt-analyzers notice to introduce the characteristics of the plain-image in the generation of the chaotic key-streams, in order to make them changeable in each time the cipher algorithm is executed even with the same set of keys.

Chapter 3

Design and Realization of Secure and Efficient Cellular automata-based cryptosystems

Cellular automata (CA) is a class of discrete dynamical systems. The process of designing and developing CA-based cryptosystems, has grasped the attention of many researchers for several last decades, owing to the simple underlying rules of CA, that are effectively implemented, and conducted to complex behaviors after the iterative application of these simple rules [21, 34, 35, 40, 46, 64, 68, 121].
In this chapter two cipher algorithms for image content protection are designed and realized. The proposed cryptosystems are sufficiently efficient in terms of security level and time consuming, under just one encryption round, and hence they are best suited for real time applications. The first cipher algorithm proposes for the first time in the literature of CA based cipher design, the employment of quadtree decomposition mechanism (QTD) in combination with a special class of CA, namely, 4^{th} order 1D reversible memory cellular automata (RMCA), the proposal satisfies a randomized encryption property (RE), and consists of the iterative application of two modules: (1) a mixing module which is governed by a simple modular addition arithmetic operation, and a sequential mode of pixel mixing, aiming to introduce a certain diffusion effect within just this primary step; (2) a diffusion module that is ruled by means of quadtree decomposition strategy jointly 4^{th} order 1D reversible memory CA, to further enhance the diffusion of the overall cryptosystem and achieve a sufficient level of security. The second cipher algorithm is based on chaos in incorporation with cellular automata, aiming to benefit from the strongpoint of the two different dynamical system concepts. The proposal introduces a new metric to represent the characteristic of the plain image, this latter together with the external secret key contribute in the mechanism of key generation overall the cryptosystem, and consists of two

iterative modules: (1) a confusion module which is governed by a permutation at a bit level, and controlled by means of 1D chaotic system, herein Logistic Tent system (LTS), to further change the pixel value as well as its location, suck kind of shuffling permits to introduce a certain diffusion mechanism within only this phase; (2) a diffusion module is subdivided into two sub modules: the former one is based on a sequential mode of pixel diffusing, and controlled by 1D LTS chaotic system, for the sake of accelerating more the diffusion process and spread the influence of a single bit over the others, and a latter part sub module is ruled by means of quadtree decomposition mechanism in cooperation with a special class of cellular automata, namely, 4^{th} order 2D reversible memory cellular automata, aiming to improve the diffusion of the overall cryptosystem and achieve a sufficient level of security. The chapter is structured as follows: section 3.1 presents the basic definitions around cellular automata. The first and the second proposed approaches are covered in detail in section 3.2. A comparative study of performance, in terms of security level and execution time, is introduced in section 3.3. At the end, section 3.4 gives a conclusion to this chapter.

3.1 Mathematical background

3.1.1 One dimensional cellular automata

One dimensional cellular automata (1DCA, for short) are special class of discrete dynamical systems, formed by a finite one dimensional array of N identical objects named cells. Each cell which is denoted by $< i >$ is characterized by its state S_i^t at time t that is defined on a finite state's set S. A cellular automaton evolves deterministically in discrete time steps, changing the states of all cells according to a local transition rule F that defines the new state S_i^{t+1} of each cell $< i >$ using its previous state, and the states of its corresponding neighbors. A cell's neighborhood V_i is a specific selection of cells that are relatively chosen according to the i's position of the cell considered to be updated and its r left and right neighbors, including the cell itself. In general, a symmetric neighborhood is defined using the aforementioned parameter r noted a radius, this latter specifies the set of positions for the $2r + 1$ neighboring cells by:

$$NB(i) = \{i - r, i - r + 1, \ldots, i - 1, i, i + 1, i + 2, , \ldots, i + r - 1, i + r\} \tag{3.1}$$

To deal with finite size automatons boundaries, the cells of the array are concatenated together in a cyclic form to consider a periodic boundary condition. The transition rule F is then applied to each neighborhood of a given cell $< i >$, to compute and update its state to S_i^{t+1} according to the following equation:

$$S_i^{t+1} = F(V_i) = F(S_{i-r}^t, S_{i-r-1}^t, \ldots, S_i^t, \ldots, S_{i-1+r}^t, S_{i+r}^t) \tag{3.2}$$

When the set S of possible states is equal to $\{0,1\}$, corresponding CAs are named binary cellular automata. In such case, the transition rule is defined by the binary representation of the possible new state's values, corresponding to all possible 2^{2r+1} neighborhood configurations on $2r+1$ bits, so the number of possible transition rules for a binary one dimensional CA is then equal to $2^{2^{2r+1}}$ A configuration C^i is defined by the states of all the automaton cells by C^i=$(S_0^t, S_1^t, \ldots, S_{N-1}^t)$, while the transition rule F is extended to the global transition map Φ that describes the dynamic evolution of the CA's configurations C^{t+1}= $\Phi(C^t)$ starting from any given initial configuration C^0. If Φ is bijective, then the corresponding CA is reversible and the backward evolution becomes possible using the inverse global transition map Φ^{-1} [134]. Within conventional paradigm of cellular automata, we consider that the state of each cell $< i >$, at time $t+1$ is only depending on the states of its neighbor cells at time t. Nevertheless, one can consider CAs for which the state of each cell at time $t+1$, depends also on corresponding states at previous time steps $t-1$,$t-2$, ... etc. Such class of CAs is named memory cellular automata (MCA) [6], having the interesting property to be reversible whatever is the used transition rule F. Specifically, in a K^{th} order MCA, states of new configuration C^{t+1} depend on K previous ones C^t,..., C^{t-K} . Using K different transition rules F_1, F_2, ..., F_K, each state S_i^{t+1} of the configuration is defined by:

$$S_i^{t+1} = F^1(V_i^t) \oplus F^2(V_i^{t-1}) oplus \cdots \oplus F^k(V_i^{t-k+1}) \tag{3.3}$$

where V_i^t denotes the neighborhood of the cell $< i >$ at time step t. Accordingly, the global transition map can then be defined on the set C of possible configurations by:

$$\psi : C \times C \times \cdots \times C \to C \tag{3.4}$$

$$C^{t+1} = \psi(C^t, C^{t-1}, \ldots, C^{t-1+k}) = \Phi^1(C^t) \oplus \Phi^2(C^{t-1}) \oplus \cdots \oplus \Phi^k(C^{t-k+1} \tag{3.5}$$

where Φ_1, Φ_2,..., Φ_{k-1}, Φ_k are global transition maps corresponding to the transition rules F_1,F_2,...,F_K. In order to ensure reversibility of a given MCA, we can easily show that it suffices that the global transition map Φ_k be equivalent to the identity function ($\Phi_k(C^i$=$C^i \ \forall \ i$). Hence, the MCA defined by the following equation:

$$C^{t+1} = \Phi^1(C^t) \oplus \Phi^2(C^{t-1}) \oplus \ldots \Phi_{k-1}(C^{t-k+2}) \oplus C^{t-k+1} \tag{3.6}$$

is reversible for any set of the transition functions, and admits as a reverse the MCA defined by the following equation:

$$B^{t+1} = \Phi^{K-1}(B^t) \oplus \Phi^{k-2}(B^{t-1}) \oplus \dots \Phi_1(B^{t-k+2}) \oplus B^{t-k+1} \tag{3.7}$$

Where the B_i's denotes the possible configurations of the inverse MCA.

The proof of this proposition is trivial. Let's consider the configurations (C^{t+1},C^t,...,C^{t-k+1}) generated using the K^{th} order MCA defined by equation (3.7). We show that the configuration C^{t-k+1} can be recovered by applying the MCA defined in equation (3.8) on the configurations (C^{t+1},C^t,...,C^{t-k+2}).

When running the inverse MCA, configurations are handled in reverse order such that : B^{t-k+2}=C^t, ...,B^t=C^{t-k+2} and B^{t+1}=C^{t-k+1} . Hence, using equation (3.8) we have:

$$\begin{aligned} B^{t+1} &= \Phi^{K-1}(B^t) \oplus \Phi^{K-2}(B^{t-1}) \oplus \dots \oplus \Phi^1(B^{t-k+2}) \oplus B^{t-k+1} \\ &= \Phi^{K-1}(C^{t-k+2}) \oplus \Phi^{K-2}(C^{t-k+3}) \oplus \dots \oplus \Phi^1(C^t) \oplus C^{t+1} \\ &= \Phi^1(C^t) \oplus \Phi^2(C^{t-1}) \oplus \dots \oplus \Phi^{k-1}(C^{t-k+2}) \oplus C^{t+1} \end{aligned} \tag{3.8}$$

By substituting the term C^{t+1} in equation (3.9) using equation (3.7) we obtain:

$$\begin{aligned} B^{t+1} &= \Phi^1(C^t) \oplus \Phi^2(C^{t-1}) \oplus \dots \oplus \Phi^{k-1}(C^{t-k+2}) \oplus \Phi^1(C^t) \oplus \Phi^2(C^{t-1}) \oplus \dots \oplus \Phi^{k-1}(C^{t-k+2}) \\ &= [\Phi^1(C^t) \oplus \Phi^1(C^t)] \oplus [\Phi^2(C^{t-1}) \oplus \Phi^2(C^{t-1})] \oplus \dots \oplus [\Phi^{k-1}(C^{t-k+2}) \oplus \Phi^{k-1}(C^{t-k+2})] \oplus C^{t-k+1} \\ &= 0 \oplus 0 \oplus \dots \oplus 0 \oplus C^{t-k+1} \\ &= C^{t-k+1} \end{aligned} \tag{3.9}$$

Consequently, the MCA defined by equation (3.8) can always recover the configuration C^{t-k+1} from the configurations (C^{t+1},C^t,...,C^{t-k+2}).As a result, it is the inverse of the MCA defined by equation (3.7).

3.1.2 Two dimensional cellular automata

Two-dimensional cellular automata (CA, for short) are simple models of computation described by a 4-tuple $A = (C, S, V, f)$, where C=$\{< i, j > 1 \leq i \geq r, 1 \leq j \geq c\}$ is the cellular space formed by a rectangular array of $r \times c$ identical objects called cells, each cell has a state in the state set $S = Z_2 = \{0, 1\}$ .Every cell's neighborhood is defined by a set

V , and the neighborhood of a cell is expressed by its indexes of $< i, j > \in C$:

$$V_{ij} = \{< i + \alpha, j + \beta >, (\alpha, \beta) \in V\} \tag{3.10}$$

In this work, Moore neighborhood is exploited, and it is formed by the cell itself (which will be updated) and its eight surrounding cells as:

$$V = \{(-1,-1), (-1,0), (-1,1), (0,-1), (0,0), (0,1), (1,-1), (1,0), (1,1)\} \tag{3.11}$$

The local transition function $f : Z_2^9 = Z_2$ is the function that determines the evolution of CA throughout the time i.e., the changes of state for each cell, by taking into account its current state and the states of its considered neighbors. Thus, if $S_{ij}^t \in Z_2$ is the state of the cell $< i, j >$ at time t, the next state of this cell is given by the following formula:

$$S_{ij}^{t+1} = f(S_{i-1,j-1}^t, S_{i-1,j}^t, S_{i-1,j+1}^t, S_{i,j-1}^t, S_{i,j}^t, S_{i,j+1}^{t+1}, S_{i+1,j-1}^t, S_{i+1,j}^t, S_{i+1,j+1}^t) \tag{3.12}$$

In order to solve the problem of finite cellular space, periodic boundary condition is established:

$$S_{ij}^t = S_{uv}^t \longleftrightarrow i \equiv u(modr) and j \equiv v(modc) \tag{3.13}$$

As abovementioned, every cell at time t depends only on the states of its neighbors at the previous time t-1. However, if such dependence is expanded to take into consideration the states of neighbors at previous times t-2 , t-3 ,. . ., then the CA is called memory CA.

The reversibility of cellular automata is an important property to make the backward evolution possible and one says that CA is reversible if there is another cellular automaton that produces the inverse evolution [53].

We denote by C the set of all possible configurations of CA, and the configuration at the next time step is given by the global transition function as follows:

$$\Phi = C \longrightarrow C \tag{3.14}$$

$$C^t \longrightarrow C^{t+1} = \Phi(C^t) \tag{3.15}$$

And

$$\phi : C \times \ldots \times C \longrightarrow C \tag{3.16}$$

$$(C^t, \ldots, C^{t-k}) \longrightarrow C^{t+1} = \Phi(C^t, \ldots, C^{t-k}) \tag{3.17}$$

For memory CA.

A 4^{th} order reversible memory CA is exploited in this work, and it is of the form:

$$C^{t+1} = \Phi(C^t, \ldots, C^{t-3}) = \Psi_0(C^t) \oplus \Psi_1(C^{t-1}) \oplus \Psi_2(C^{t-2}) \oplus (C^{t-3}) \tag{3.18}$$

Where Ψ_k is defined by the following transition function:

$$S_{ij}^{t+1} = \lambda_1 S_{i-1,j-1}^t \oplus \lambda_2 S_{i-1,j}^t \oplus \lambda_3 S_{i-1,j+1}^t \oplus \lambda_4 S_{i,j-1}^t \oplus \lambda_5 S_{i,j}^t \oplus \lambda_6 S_{i,j+1}^t \oplus \lambda_7 S_{i+1,j-1}^t \oplus \lambda_8 S_{i+1,j}^t \oplus \lambda_9 S_{i+1,j+1}^t \tag{3.19}$$

For each $1 \leq i \geq 9$ $\Psi_i^k \in Z_2$.The type of cellular automata is reversible [123], and its inverse evolution is possible following the formula:

$$C^{t+1} = \Psi_0(C^t) \oplus \Psi_1(C^{t-1}) \oplus \Psi_2(C^{t-2}) \oplus (C^{t-3}) \tag{3.20}$$

3.2 New proposals

This section aims to discuss in detail the methodology of the proposed cipher algorithms, herein cryptosystem-A and cryptosystem-B.

3.2.1 Fast and efficient randomized encryption scheme for digital images based on Quadtree decomposition and reversible memory cellular automata (Cryptosystem-A)

The proposed cipher algorithm is comprised mainly of the iterative application of two modules: a mixing phase and a diffusion phase. The overall proposal is controlled by means of an efficient CA-based key scheming mechanism. The structure of the cryptosystem is pictorially shown in Figure 3.1 for the encryption procedure part, and Figure 3.3 for the decryption procedure part.

3.2.1.1 Encryption procedure

The proposed approach is based on the use of one dimensional (1D) reversible memory cellular automata (RMCA) in cooperation with quadtree decomposition mechanism (QTD, for short), under one encryption round. The proposal satisfies a randomized encryption property i.e., for every time the algorithm is executed with the same used plain image/set of keys, it can produce a totally new cipher image, this desired property renders the scheme CPA secure (i.e., resistance against known/chosen plain image attacks), and it consists of the iterative application of two modules: In the former module, a mixing phase is adopted to the plain-image for de-correlating the relationship between neighboring pixels and accomplishing a satisfactory level of security using just one encryption round. In the latter part, a QTD technique is employed to the mixed-image in which it is divided consecutively into 4 equal sub-images, these sub-images constitute the four initial configurations of the 4^{th} order RMCA, the encryption rules (i.e., sub-keys) are obtained from the used secret key by using an efficient CA-based key-generation mechanism, the technique of division and employing RMCA is carried out until reaching 4×4 block size, in that case a XOR operation is performed with the last generated rule to obtain the final cipher image.

Randomized Encryption For the sake of withstanding to the commonly used attack, to break the security of the cryptosystems, namely, chosen plaintext attack (i.e., to be CPA-secure), the cipher algorithm should provide the property of randomized encryption (RE). This property is satisfied by any encryption method that produces two different cipher images, whenever the same plain image is encrypted under the same set of keys. Hence, an attacker cannot employ any previous information about a given plain image, to break the semantic security of the system and reveal any useful information about the key. To this end, and before applying the encryption procedure, a random bit alteration is handled, this latter aims to modify one bit from the plain image at a random location. The altered bit position is generated by means of any secure random bit generator that can produce random numbers which are: one-time used and unpredictable. The underlying effect of this mechanism is to produce a completely random and different image, for each time the cipher algorithm is executed with the same plain image, and even with identical set of keys (i.e., randomized encryption).

Mixing module This process is governed by means of a simple modular operation (modulo 256), and a sequential mode of pixel mixing, periodic boundary conditions technique is handled, to further solve the problem of boundaries. The above explained mechanism is applied to the four sub-quadrants (i.e., initial configurations) of the plain image, namely, $(C^0)_0$, $(C^1)_0$,$(C^2)_0$ and $(C^3)_0$ (such kind of subdivision will be covered bellow within the diffusion module), in which the pixels of each configuration are merged in both forward and backward directions, to propagate elementary possible alterations of any single bit of

the plain image to several locations on the same configuration. Such propagation is easily amplified later by the MCA evolution mechanism, in which it conducts to a high avalanche of changes in the produced cipher image, de-correlates the relations among neighboring pixels, accomplishes a certain diffusion effect within just this phase, and thus avoids using several consecutive rounds of confusions, as it is generally used by chaotic based image cryptosystems, for the sake of enhancing the enciphering/deciphering execution time. The following pseudo-algorithm illustrates the details of mixing module, where each configuration is considered as an 1D array of n bytes, namely, $A[0, \ldots, n-1]$.

```
Procedure MixConfiguration;
Input : configuration A    // that can be either (C0)0,(C1)0,(C2)0 or (C3)0
Output : a mixed version of the configuration A
For i:=1 to n-1 do A[i]:=(A[i]+A[i-1]) mod 256; // mixing in the forward
    direction
For i:=n-2 dowto 0 do A[i+1]:=(A[i+1]+A[i]) mod 256; // mixing in the backward
    direction
End
```

Diffusion module During this process, the whole plain-image is firstly decomposed into four equal quadrants according to the quadtree decomposition strategy. These four blocks are considered as four initial configurations $(C^0)_0$,$(C^1)_0$,$(C^2)_0$ and $(C^3)_0$ of a 4^{th} order MCA, that is defined according to equation (3.7). The transition rules of this MCA are derived from the secret key using an efficient key scheming mechanism (as will be explained in section 3.2.1.2). Before applying the constructed MCA during four iterations, each initial configuration passes with a mixing mechanism, as described in the above section (i.e., mixing module), to produce new four configurations, namely, $(C^4)_0$, $(C^5)_0$, $(C^6)_0$ and $(C^7)_0$, aiming to introduce sufficient dependencies between the plain image's pixels. These dependencies are amplified later by the MCA evolution mechanism to achieve higher plain-image sensitivity, and avoid the use of several confusion/diffusion rounds. The resulted configurations are then combined to form a new image, whereas the upper left resulting bloc $(C^4)_0$ is recursively subdivided into four equal size quadrants that define new configurations, i.e., $(C^0)_1$,$(C^1)_1$,$(C^2)_1$ and $(C^3)_1$,for a 4^{th} order constructed MCA using a new set of transition rules derived from the secret key. This new MCA is iterated to produce new configurations, namely, $(C^4)_1$, $(C^5)_1$,$(C^6)_1$ and $(C^7)_1$ that replace the sub-blocks of $(C^4)_0$. The process is repeated recursively by dividing the block $(C^4)_i$ at each level i until reaching the deepest possible level m, where the size of the block $(C^4)_m$ is equal to 4×4 pixels. At this level, and since the size is equal to 16 bytes (128 bits), the corresponding block $(C^4)_m$ is simply diffused using just the XOR bitwise operation

with the last generated sub-key. According to the presented process, three transition rules (sub-keys) are needed at each level, so the total number of required sub-keys is equal to $3m + 1$.

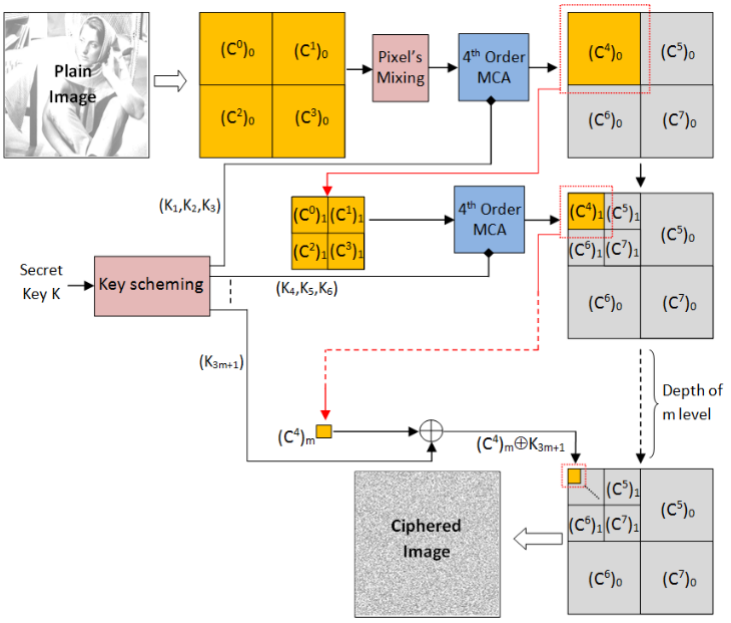


Figure 3.1: Encryption procedure part of cryptosystem-A

3.2.1.2 Key expansion mechanism

According to the design of our proposal, several sub-keys (i.e., transition rules) are required during the diffusion module, more precisely in the application of quadtree decomposition mechanism, to further define the transition rules of the related MCAs. Since the employed MCAs are of 4^{th} order, three different transition rules are needed by each MCA, i.e., three different sub-keys are required at each decomposition level. The quadtree decomposition depth depends on the plain image's size: for a square image of $L \times L$ pixels, the exact number m of decompositions is equal to $[log_2(L)] - 1$.Hence, the number of required sub-keys is equal to $3 \times ([log_2(L-2)]) + 1$.

In the proposed cipher algorithm, the sub-keys are derived from the secret key K (128bits), using a non-uniform class of cellular automata that alters the transition rules at each position, by means of a pair of control bits extracted from the secret key, which is considered as an initial configuration, then a set of four transition rules, namely, 90, 105, 150 and 165 are employed to update the state of each cell's position, these transition rules are stored

in a table named T_i that is updated after each iteration, by applying a cyclic left rotation. For a given cell at a position $< i >$, the choice of the rule to be applied, is based on the index value derived from the current cell state and the state of its right neighbor, so the four possible values are 00, 01, 10 and 11. If we consider T_j the rules table state at iteration j, then the state S_i^{t+1} at the position $< i >$ of a new configuration is determined using the following equation :

$$S_i^{t+1} = T_j[S_i^t \times S_i^{t+1}](V_i) = T_j[S_i^{t+2} \times S_{i+1}^t](S_{i-1}^t, S_i^t, S_{i-1}^{t+1}) \tag{3.21}$$

By evolving the non-uniform CA, each new configuration defines a new generated sub-key. The process is continued until all sub-keys are generated. Figure 3.2 shows details of the key expansion mechanism. As will be demonstrated from the obtained experimental results in section 3.3, the proposed key scheming ensures a high confusion of the cryptosystem, reflecting the high sensitivity of the cipher image to elementary bit's flipping of the secret key.

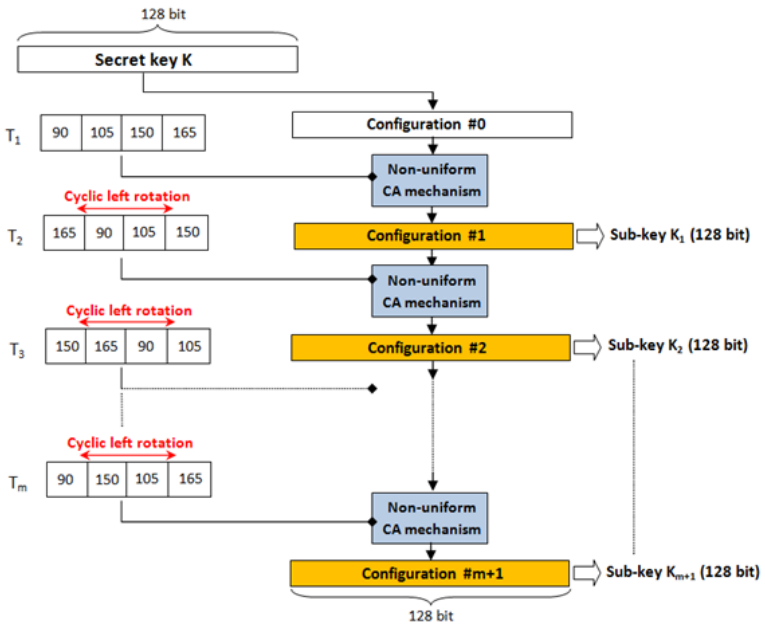


Figure 3.2: Key expansion and sub-keys derivation scheme

3.2.1.3 Decryption procedure

The decryption procedure is like the one described above in section 3.2.1.1 (encryption procedure), in which it must be applied in the reverse order. First of all, the reverse diffusion module is performed to the cipher image, which is governed by the quadtree decomposition strategy (QTD) in incorporation with reversible memory cellular automata (RMCA), and as a latter part, a reverse mixing module is carried out to the output mixed image, this phase is ruled by means of addition modular operation, and a sequential mode between pixels, aiming to retrieve the original image, which is identical to the employed plain image, except the altered one bit used to handle the randomized encryption, however this is negligible with respect to the size of the image, and visually imperceptible. As the proposed cipher algorithm belongs to the category of symmetric ciphers, the same sub keys (i.e., transition rules) of the encryption procedure, must be employed in the reverse order.

Reverse diffusion module The diffusion procedure is performed in a deterministic way to recover the mixing image from the cipher one. After generating the sub-keys using the same key scheming mechanism, see section 3.2.1.2, the upper left block of 4×4 pixels is extracted from the cipher image, and combined with the sub key K_{3m+1} , to perform the bitwise XOR operation, for recovering the configuration $(C^4)_m$, this latter is combined with the three other remained neighborhood blocks of 4×4 pixels, namely, $(C^5)_m$,$(C^6)_m$ and $(C^7)_m$, respectively, and formed the $(C^0)_m$ configuration, together with $(C^1)_m$, $(C^2)_m$ and $(C^3)_m$ other configurations, that are all correspond to the quadtree decomposition depth of the m^{th} level, the inverse 4^{th} order MCA is handled, under the employment of three produced sub keys in the reverse order, namely, K_{3m-2},K_{3m-1} and K_{3m} (of 128 bits each one) as transition rules, to further recover the $(C^4)_{m-1}$ configuration of the $(m-1)^{th}$ level. We should notice that at each reconstruction level, the set of used transition rules matches to the set of sub-keys that are derived by the key scheming mechanism. The process is continued recursively in a bottom-up manner, until reaching the last configurations, i.e., $(C^0)_0$, $(C^1)_0$, $(C^2)_0$ and $(C^3)_0$.

Reverse mixing module The mixing procedure is carried out in a deterministic way to recover the plain image from the mixing one, obtained after performing the above explained diffusion module. This mixing image is expressed by its four equal blocks of $L/2 \times L/2$ pixels (L is the length the whole image), namely, $(C^0)_0$, $(C^1)_0$, $(C^2)_0$ and $(C^3)_0$, each of which is passed with the mixing phase, which is governed by means of a simple modular operation (modulo 256), a sequential mode between pixels, and handled in forward and backward directions, starting from the last pixel to the first one. The following pseudo-algorithm illustrates the details of reverse mixing module, where each configuration is considered as an 1D array of n bytes, namely,$A[0, \ldots, n-1]$.

```
Procedure MixConfiguration;
Input : configuration A    // that can be either (C0)0,(C1)0,(C2)0 or (C3)0
Output : a mixed version of the configuration A
For i:=n-1 to 1 do A[i]:=(A[i]-A[i-1]) mod 256; // mixing in the forward
    direction
For i:=0 dowto n-2 do A[i+1]:=(A[i+1]-A[i]) mod 256; // mixing in the backward
    direction
End
```

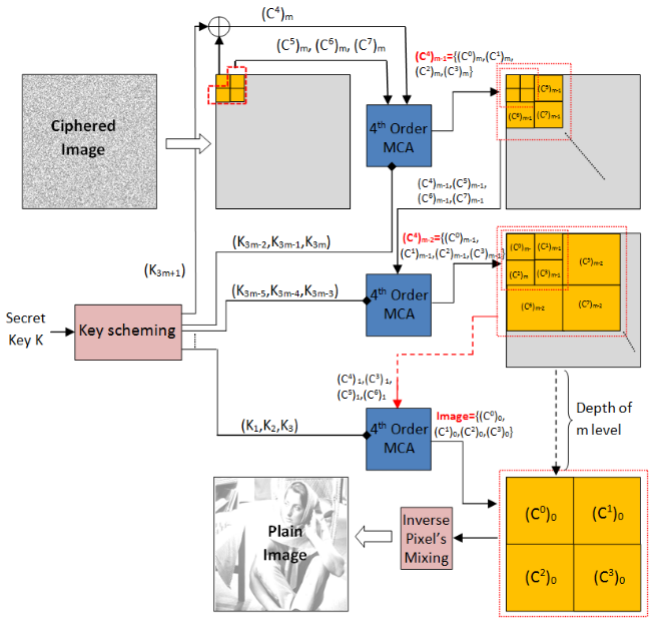


Figure 3.3: Decryption procedure part of cryptosystem-A

3.2.2 An image encryption scheme combining chaos-memory cellular automata and weighted histogram (Cryptosystem-B)

The proposed cipher algorithm is comprised mainly of the iterative application of two modules: a confusion phase and a diffusion phase. The overall proposal is controlled by means of any cryptographically secure pseudorandom bit generator, in incorporation with 1D chaotic system, namely, Logistic Tent System (LTS, for short) (which will be discussed in detail during chapter 4) in the key scheming mechanism. The structure of

the cryptosystem is pictorially shown in Figure 3.4 for the encryption procedure part, and Figure 3.5 for the decryption procedure part.

3.2.2.1 Encryption procedure

The proposed approach is based on the use of an improved 1D chaotic system, namely, Logistic Tent System (LTS) and reversible memory cellular automata (RMCA), the encryption process is performed by following the permutation-diffusion architecture under just one round. Firstly, a random pixel overwriting mechanism is handled, and the new measure of plain-image's weighted histogram (Wh, for short) is inserted instead. This mechanism ensures the immunity of the proposed method to known/chosen plain-image attacks (CPA secure) like the following : the incorporation of the Wh value as a new metric that handles the plain image's characteristics together with the secret key, in the procedure of extracting the initial values of the used chaotic map (LTS), this conducts to a random-like generating key-streams i.e., for different plain-images different chaotic sequences are produced, which renders their recovering harder. Secondly, the confusion module is based on a bit-level permutation and the generated one-time key-streams using the chosen 1D chaotic system (LTS), this kind of shuffling permits to modify both the pixel's location and value to further attain both confusion and diffusion within just this phase. Thirdly, the diffusion module is separated into two sub modules: in the first one the value of every pixel is modified sequentially by means of the chosen chaotic system (LTS), for accelerating the diffusion process and spread out the influence of a single bit over the others, and the second sub phase, 2D reversible memory cellular automata (RMCA) is associated with quadtree decomposition method (QTD), and performed to the output of the former sub module, to enhance the security and diffusion effect of the proposed cryptosystem.

Random Pixel Overwriting One pixel of the plain image at a random position is overwritten, by inserting the weighted histogram value (Wh) as a new measure that represents all the plain image's pixels except one (i.e., in where we will insert the Wh value), this value handles the plain image's characteristics and further will be employed to ensure the resistance of the proposed cryptosystem to both known/chosen plain image attacks (CPA secure). The proposed cryptosystem utilizes 512 bits as external key K, this later is used to calculate the i^{th} and j^{th} positions of the overwriting pixel using the proposed technique in [98] as follows:

- The 512 bits external key K is divided into 8-bit blocks ki as:

$$k = k_1, k_2, \ldots, k_{64} \tag{3.22}$$

- Extract two numbers from the first half of the external key (128 bits) as follows:

$$V_1 = mod(\frac{1}{512(k_1 \oplus \cdots \oplus k_8)} + \frac{\sum_{k=1}^{64} k_i}{64}, 1) \tag{3.23}$$

$$V_2 = mod(\frac{1}{512(k_9 \oplus \cdots \oplus k_{16})} + \frac{\sum_{k=1}^{64} k_i}{64}, 1) \tag{3.24}$$

- Discretize V_1 and V_2 using the following two equations:

$$\widehat{\{V_1\}} = \lfloor \{V_1\} \times 10^{15} \rfloor mod M \tag{3.25}$$

$$\widehat{\{V_2\}} = \lfloor \{V_2\} \times 10^{15} \rfloor mod N \tag{3.26}$$

- The i^{th} position and the j^{th} position of the overwriting pixel are calculated as follows:

$$i = V_1 \tag{3.27}$$

$$j = V_2 \tag{3.28}$$

- The weighted histogram value (Wh) is included in the plain image P as Val_2 (which will be computed in the next section) as follows:

$$P(i, j) = Val_2 \tag{3.29}$$

Generation of the variable initial value and control parameter In the proposed cipher algorithm, the parameter r and the initial condition x_0 of the improved 1D chaotic system (LTS) are extracted from the external secret key as follows:

$$V_1 = mod(\frac{1}{512(k_{17} \oplus \cdots \oplus k_{32})} + \frac{\sum_{k=1}^{64} k_i}{64}, 1) \tag{3.30}$$

$$V_2 = mod(\frac{1}{512(k_{33} \oplus \cdots \oplus k_{48})} + \frac{\sum_{k=1}^{64} k_i}{64}, 1) \tag{3.31}$$

For updating the values of both the parameter r and the initial condition x_0, the plain image's characteristics are handled by means of the weighted histogram (Wh) value, this new measure represents the distribution of all the plain image's pixels except one pixel (which is used for Wh's value insertion), and it is calculated as follows:

$$Val_1 = \sum_{0}^{255} (h[i]/N \times M) \times h[i] \tag{3.32}$$

Where N and M are the width and the height of image respectively, $h[i]$ is an integer array containing the distribution of the considered pixels in [0,255] range. Then, we calculate Val_2 as follows:

$$Val_2 = Val_1 mod 256 \tag{3.33}$$

Where $Val_2 \in$ [0,255] and mod is the module operation. At the end, the weighted histogram (Wh) value with 10^{-15} decimal precision is given by:

$$Wh = Val_2/255 \tag{3.34}$$

Then, the parameter r and the initial condition x_0 are updated as follows:

$$\acute{r} = r + Wh \tag{3.35}$$

$$\acute{x_0} = x_0 + Wh \tag{3.36}$$

Clearly, the new values of $\acute{r}$ as parameter and $\acute{x_0}$ as initial condition of LTS chaotic map are both secret key/plain image related, and thus they are extremely sensitive to any minor change to either the secret key or the plain image, to further generate different key-streams for different plain images even with the same set of keys.

Confusion module This process is governed by a permutation at a bit level, and controlled by means of the produced one-time key-streams of LTS chaotic map, this type of shuffling is handled, in which not only the pixel's position is changed but its value as well, aiming to achieve both confusion and diffusion within just this phase. First of all, the weighted histogram (Wh) of the plain image, noted by P, is gotten, for the sake of computing the initial values of LTS chaotic map, through equations (3.36) and (3.37). Then, each pixel is divided into its 8 parts, each of which contains 8 bits, and hence the plain image is extended to be $M \times N \times 8$ (where M is the number of image's rows, N is the number of image's columns), so, after iterating LTS chaotic map for 500 times to

avoid the transient effect, the process in continued to iterate it for $M \times N \times 8$ times to obtain two chaotic sequences, namely, $\{X_K\}$, $\{Y_K\}$ which are later discretized as follows:

$$\widehat{\{X_K\}} = \lfloor \{X_K\} \times 10^{15} \rfloor mod M \tag{3.37}$$

$$\widehat{\{Y_K\}} = \lfloor \{Y_K\} \times 10^{15} \rfloor mod N \times 8 \tag{3.38}$$

As a latter part, the bit within each plain pixel is exchanged based on the two above generated chaotic key-streams, so that, $\widehat{\{X_K\}}$ chaotic sequence represents the new i position of the exchanged bit, where i=0, 1, ...,$M-1$, and $\widehat{\{Y_K\}}$ chaotic sequence is employed to generate both the j position of this bit, and the bit to be exchanged itself among the 8 bits of the new pixel, where$j$=0,1,...,$8N-1$.

Diffusion module During this module, the process is subdivided into two sub modules which are iteratively applied to the confused image as follows:

First diffusion sub module within this process, a sequential mode for enciphering pixel values is followed, according to which the encryption of each pixel is related to the sum of all the next pixels, and controlled by means of the produced one time key-streams of LTS chaotic map, aiming to de-correlate the relations among neighboring pixels, and accelerate the diffusion effect of the overall cipher algorithm under just one encryption round. The first sub module of diffusion is described as follows:

- The plain image is transformed from its two dimensional to one dimensional vector format P={ p_1 , p_2 , ... ,$p_{M\times N}$ }.
- Calculate the sum of the plain image pixels according to the following equation :

$$S = \sum_{i=0}^{M\times N-1} P_i \tag{3.39}$$

- Encrypt all the plain image pixels using the following equations :

$$C_i = P_i \oplus (K_i + C_{i-1}) mod 256 \oplus S \tag{3.40}$$

Where C_i is the ith cipher pixel, P_i is the ith plain pixel, k_i is a chaotic sequence generated using LTS chaotic map, in which its initial condition and control parameter are based on the latest two generated values in the previous module, C_{i-1} is the previously encrypted pixel, and S is the sum of all image pixels except the ith one (i.e., S is all the next pixels of the ith pixel). The index i is performed from the first pixel of 0 to the last one of $M \times N - 1$.

Second diffusion sub module This sub module is ruled by the association of 4^{th} order two dimensional reversible memory cellular automata (RMCA) with quadtree decomposition strategy, to further amplify the propagation of each bit alteration over the others by means of MCA evolution mechanism, and enhance the security of the cryptosystem. Three different sub-keys (i.e., transition rules) are needed for every decomposition level, since 4^{th} order MCA is performed, so, the mechanism of sub keys' generation is based on a cryptographically secure pseudorandom bit generator. Since two dimensional cellular automata Moore neighborhood is used in this sub phase, the length of each sub key (i.e., rule) is 29 i.e., 512 bits. The initial configuration of 512 bits for evolving cellular automata and generating sub-keys is based on the use of LTS chaotic map with the initial condition $\acute{\acute{X}}_0$ and the parameter$\acute{\acute{r}}$ extracted from both the external key of 512 bits and the plain-images characteristics as follows:

- Extract two numbers from the last 128 bits of the external key and the plain-image's characteristics using the following equations:

$$\acute{\acute{X}}_0 = (\acute{X}_0 + mod(\frac{1}{512(k_{49} \oplus \cdots \oplus k_{56})} + \frac{\sum_{k=1}^{64} k_i}{64}))mod1 \tag{3.41}$$

$$\acute{\acute{r}} = (\acute{r} + mod(\frac{1}{512(k_{57} \oplus \cdots \oplus k_{64})} + \frac{\sum_{k=1}^{64} k_i}{64}))mod1 \tag{3.42}$$

- Iterate the LTS chaotic map for 500 times to avoid the transient effect, continue the iteration of the chaotic map for 512 times to get the sequence $\{S_K\}$ and discretize it:

$$\widehat{\{S_K\}} = \lfloor \{S_K\} \times 10^{15} \rfloor mod2 \tag{3.43}$$

Then, the second sub module of diffusion is described as follows:

- Quadtree decomposition strategy with two level of decomposition is applied.

- In the first level, the image is decomposed into 4 sub-images, each one is a quarter size of the original image, we denote them as C^0 , C^1 , C^2 and C^3.
- The sub-images of $(C^0)_0$, $(C^1)_0$, $(C^2)_0$ and $(C^3)_0$ form the first configuration of 4^{th} order RMCA , to gather with the generated three sub-keys using any cryptographically secure pseudorandom bit generator, and the evolution of cellular automata is applied according to equation (3.19).
- The resulted 4 sub-images are denoted as $(C^0)_1$, $(C^1)_1$, $(C^2)_1$ and $(C^3)_1$, the last three sub-images ($(C^1)_1$, $(C^2)_1$ and $(C^3)_1$) are directly saved to form the final cipher image C.
- In the second level, the top left corner of $(C^0)_1$ is decomposed again to form $(C^0)_{10}$, $(C^1)_{11}$,$(C^2)_{12}$ and $(C^3)_{13}$ as another configuration of 4^{th} order RMCA , to gather with the generated three sub-images, following any cryptographically secure pseudorandom bit generator, and the evolution of cellular automata is applied according to equation (3.19).
- The resulted 4 sub-images are denoted $(C^0)_{20}$, $(C^1)_{21}$, $(C^2)_{22}$ and $(C^3)_{23}$, they are combined to form the top left corner of $(C^0)_1$ which is saved directly to form the complete final ciphered image.

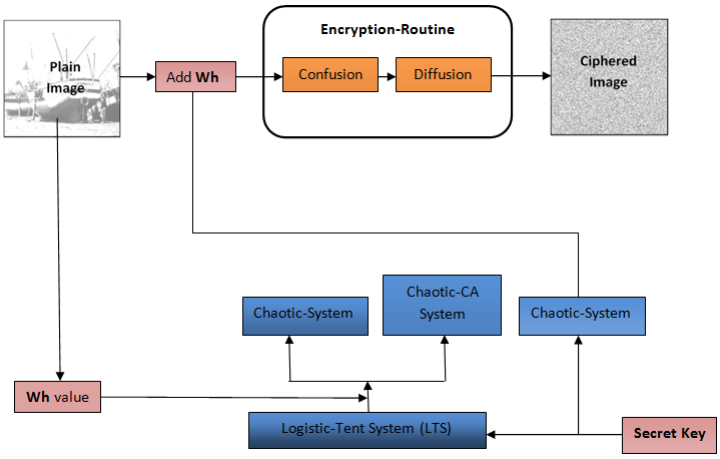


Figure 3.4: Encryption procedure part of cryptosystem-B

3.2.2.2 Decryption procedure

The decryption procedure is the same as the one described above in section 3.2.2.2 (encryption procedure), in which it must be carried out in the reverse order. It should be

noticed that for the sake of decrypting the cipher image C, Wh value is needed otherwise the decryption can't be done successfully. For this reason, the value val_2 is included on the plain-image at a secret local before encryption. The encryption routine is applied to all plain-image's pixels except one pixel in where the val_2 value is added, its location is deduced based on the secret key using equations (3.24-3.25), and Wh value is recalculated using equation (3.35), after all the used chaotic key-streams/sub-keys are regenerated using LTS chaotic map, and cryptographically secure pseudorandom bit generator jointly with LTS chaotic map, respectively, with the correct secret key and Wh value. First of all, the reverse diffusion module is performed to the cipher image, this latter is decomposed into two sub modules, as the first step, the second inverse diffusion sub module must be handled, in which is governed by the quadtree decomposition strategy (QTD) in incorporation with reversible memory cellular automata (RMCA),under only two level of decompositions, to further improve both the security level and the diffusion effect of the proposed cipher algorithm, and as a second step, the first inverse diffusion sub module is adopted, where each pixel value is changed sequentially, and controlled by means of the generated chaotic sequences of 1D LTS chaotic map, aiming to spread out the impact of a single bit over the others and thus speeding up the diffusion process. As a latter part, the reverse permutation at a bit level is performed, and ruled by the one times key-streams of 1D LTS chaotic map, suck kind of shuffling is adopted, for the sake of changing the value of pixel as well as its position, aiming to introduce a certain diffusion within only this module, to further retrieve the original image, which is the same as the plain image, except the altered one pixel that handles the Wh value, such modification is really negligible according to the size of the plain image. As the proposed cipher algorithm belongs to the category of symmetric ciphers, the same sub keys (i.e., chaotic key-streams and transition rules) of the encryption procedure must be employed in the reverse order.

Reverse diffusion module The reverse diffusion module is achieved by the iterative application of its two sub modules in the inverse order as follows:

Second diffusion sub module The process is carried out in a deterministic way to retrieve the output image (which will be used by the next sub module) from the cipher image. The sub module is based on the application of reversible memory cellular automata jointly with quadtree decomposition strategy, under just two decomposition levels, and controlled by any cryptographically secure pseudorandom number generator, in the process of generating the transition rules, in which the initial configuration is relies on LTS chaotic system. First of all, the top left corner block $(C^0)_{20}$ of $(M/4 \times N/4)$ is extracted from the cipher image, jointly with the remained neighborhood blocks, namely, $(C^1)_{21}$, $(C^2)_{22}$ and $(C^3)_{23}$, that are all match to the decomposition depth of 2^{nd} order, the inverse 4^{th} order MCA is carried out, under the use of the three produced transition rules in reverse order, to further recover $(C^0)_1$ first configuration of the 1st level, together with the remained

neighborhood sub blocks, namely, $(C^1)_1$, $(C^2)_1$ and $(C^3)_1$, that are all match to the same decomposition depth (i.e., 1^{st} order), the inverse 4^{th} order MCA is carried out, under the use of three other produced transition rules in reverse order, to further reach the final configurations, namely, $(C^0)_0$, $(C^1)_0$, $(C^2)_0$ and $(C^3)_0$, which are respectively combined to form the final output image.

First diffusion sub module This process is governed by a sequential mode of pixel enciphering, starting from the last pixel to the first, and controlled by the generated key-stream of LTS chaotic map. The steps of such process are defined as follows:

- After transforming the resulted image of the previous sub module from its two dimensional to one dimensional vector format $C=\{C_1, C_2, \ldots, C_{MN}\}$.
- Implement the reverse operations from the last pixel to the first as :

$$p_i = C_i \oplus (k_i + C_{i-1}) mod 256 \oplus S \tag{3.44}$$

$$S = S + p_i \tag{3.45}$$

Where S=0, p_i is the ith recovered plain pixel, C_i is the ith cipher pixel, k_i is a sequence generated using the LTS chaotic map, and C_{i-1} is the previously cipher pixel. The index i is performed from the last pixel of $M \times N - 1$ to the first one of 0.

Reverse confusion module The output of the above explained module (diffusion module), is adopted to the reverse confusion module, for recovering the original image. This module is based on the permutation at a bit level, and controlled by means of the generated chaotic one time key-streams of LTS chaotic map. However, such process is handled by performing the permutation loops at reverse order, this signifies that, we start the procedure of bit shuffling from the last pixel (at the last row position and the last column position), using the same produced chaotic key-streams of the encryption procedure but in the inverse order.

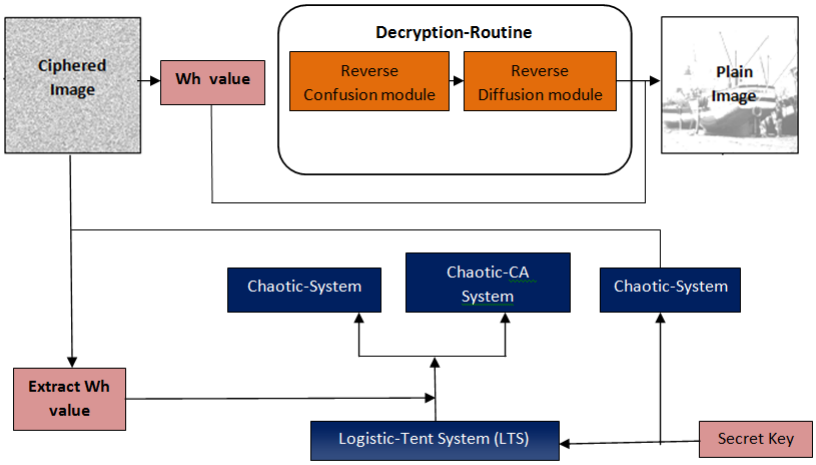


Figure 3.5: Decryption procedure part of cryptosystem-B

3.3 Security and performance analysis

In this section, we aim to evaluate the effectiveness of the realized cryptosystems, in term of the level of security, in which the robustness of our proposals is examined against all the considered types of cryptographic attacks, that are described in detail within chapter 1, besides to the execution time performance, on the other hand, the obtained results are compared with whose of some recent/relevant proposed ciphers in the scientific literature.

3.3.1 Key space analysis

The key space of any cipher algorithm should be large enough, to possess the immunity against exhaustive key search (i.e., brute force attacks). The key space analysis of the proposed cryptosystem-A is relied on the bit length of the employed transition rules (i.e., produced sub keys), for evolving the 4^{th} order MCA mechanism. On the other hand, the key space analysis of the proposed cryptosystem-B is depended on both confusion and diffusion modules, hence, The keys are built of: (1) the initial values of 1D LTS chaotic map which are the initial condition $x_0 \in [0, 1]$ and the parameter $r \in (0, 4]$ that are extracted from val_2 of one byte (i.e., 8 bits) and the external key, and (2) the external used secret key k of 512 bits. So the total key space is calculated as: $2^8 \times 2^{512}{=}2^{520}$. Indeed, with such key space, the proposals are really immune against those types of attacks, with respect to the present computer's computational power. Table 3.1 exhibits the results of key space analysis, for some recent existing methods including ours.

Table 3.1: Comparison of key-space analysis with existing methods

Encryption method	Type	Key space
Cryptosystem-A	CA	2^{128}
Cryptosystem-B	CA combined Chaos	2^{520}
Ref. [90]	CA	2^{128}
Ref. [50]	CA	2^{128}
Ref. [41]	CA combined Chaos	2^{128}
Ref. [42]	CA combined Chaos	2^{128}
Ref. [130]	CA combined Chaos	$> 2^{280}$
Ref. [11]	CA combined Chaos	$10^{44} \times 5$
Ref. [131]	CA combined Chaos	$> 10^{141}$
Ref. [148]	Chaos	10^{84}
Ref. [45]	Chaos	$> 10^{60}$

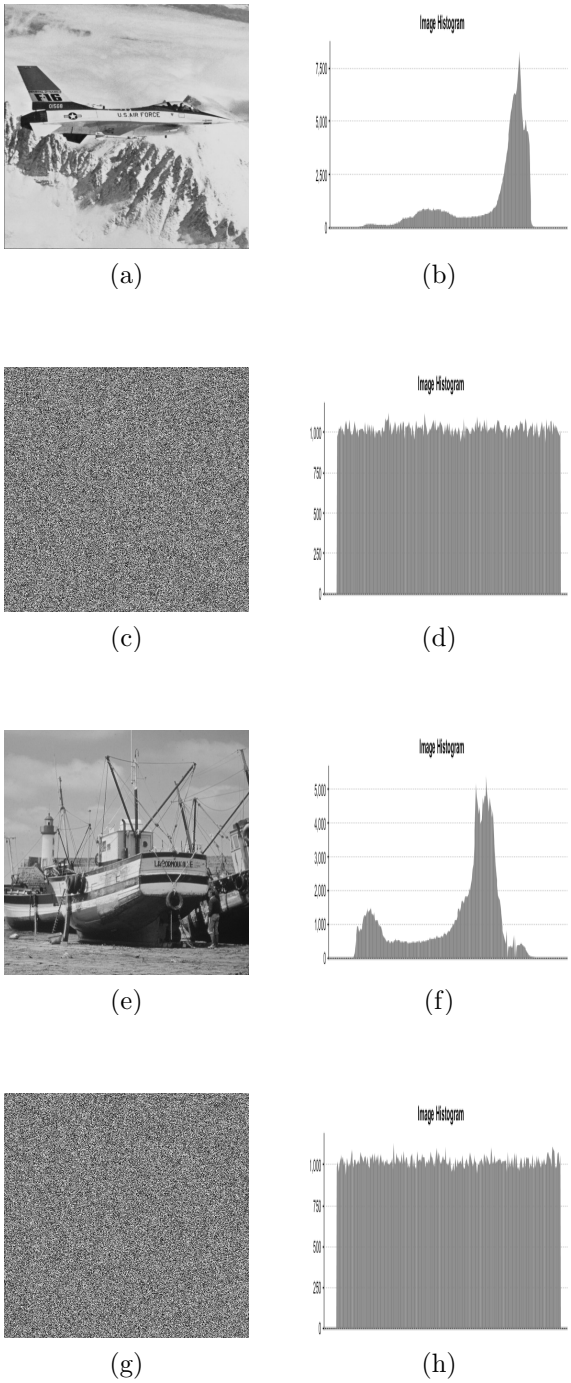
3.3.2 Statistical analysis

3.3.2.1 Uniformity analysis

The histogram of a given image permits clearly to deduce information, about the statistical distribution of its pixel values, according to which the histogram of the plain image can possess an arbitrary form depending on the image content, whereas the histogram of the corresponding cipher image should follow a uniform distribution, that reflects a random behavior, to further avoid any possible information deduction. The histograms of the plain images and their cipher ones are exhibited in Figure 3.6 using cryptosystem-A, and in Figure 3.7 using cryptosystem-B. Indeed, identical results are attained with both proposals, in which for each time the histogram of the cipher image is very close to the uniform distribution, and hence significantly different from that of the matching plain image. The visual analysis is an important tool to show the cipher image uniformity, however it is not enough to confirm such uniformity. To this end, another statistical metric, namely, Chi-square test is handled, see Equation (2.4). A comparison in term of Chi-square test is given in Table 3.2, for some existing methods including ours. All the obtained experimental values of the Chi-square test are less than the critical value (i.e., 293), which reflects the uniformity of the cipher histograms using our proposals.

Table 3.2: Comparison of Chi-square test with existing methods

Encryption method	Image	Image size	Chi-square
Cryptosystem-A	Lena	$512 \times 512 \times 1$	254.23
Cryptosystem-B	Lena	$512 \times 512 \times 1$	249.12
Ref. [146]	Lena	$512 \times 512 \times 1$	254.15
Cryptosystem-A	Lena	$256 \times 256 \times 1$	242.56
Cryptosystem-B	Lena	$256 \times 256 \times 1$	259.39
Ref. [98]	Lena	$256 \times 256 \times 1$	184
Ref. [18]	Lena	$256 \times 256 \times 1$	263
Cryptosystem-A	Peppers	$512 \times 512 \times 1$	271.28
Cryptosystem-B	Peppers	$512 \times 512 \times 1$	283.62
Ref. [146]	Peppers	$512 \times 512 \times 1$	264.92
Cryptosystem-A	Peppers	$256 \times 256 \times 1$	275.64
Cryptosystem-B	Peppers	$256 \times 256 \times 1$	171.32
Ref. [98]	Peppers	$256 \times 256 \times 1$	270
Ref. [18]	Peppers	$256 \times 256 \times 1$	274
Cryptosystem-A	House	$256 \times 256 \times 1$	255.64
Cryptosystem-B	House	$256 \times 256 \times 1$	268.93
Ref. [18]	House	$256 \times 256 \times 1$	260
Cryptosystem-A	Baboon	$512 \times 512 \times 1$	287.64
Cryptosystem-B	Baboon	$512 \times 512 \times 1$	266.75
Ref. [146]	Baboon	$512 \times 512 \times 1$	278.88
Cryptosystem-A	Baboon	$256 \times 256 \times 1$	289.53
Cryptosystem-B	Baboon	$256 \times 256 \times 1$	280.25
Ref. [98]	Baboon	$256 \times 256 \times 1$	259
Ref. [18]	Baboon	$256 \times 256 \times 1$	266
Cryptosystem-A	Airplane	$512 \times 512 \times 1$	264.82
Cryptosystem-B	Airplane	$512 \times 512 \times 1$	261.82
Ref. [146]	Airplane	$512 \times 512 \times 1$	238.50
Cryptosystem-A	Airplane	$256 \times 256 \times 1$	285.54
Cryptosystem-B	Airplane	$256 \times 256 \times 1$	253.79
Ref. [98]	Airplane	$256 \times 256 \times 1$	246
Ref. [18]	Airplane	$256 \times 256 \times 1$	265
Cryptosystem-A	Cameraman	$256 \times 256 \times 1$	276.42
Cryptosystem-B	Cameraman	$256 \times 256 \times 1$	279.04
Ref. [98]	Cameraman	$256 \times 256 \times 1$	234
Ref. [18]	Cameraman	$256 \times 256 \times 1$	257



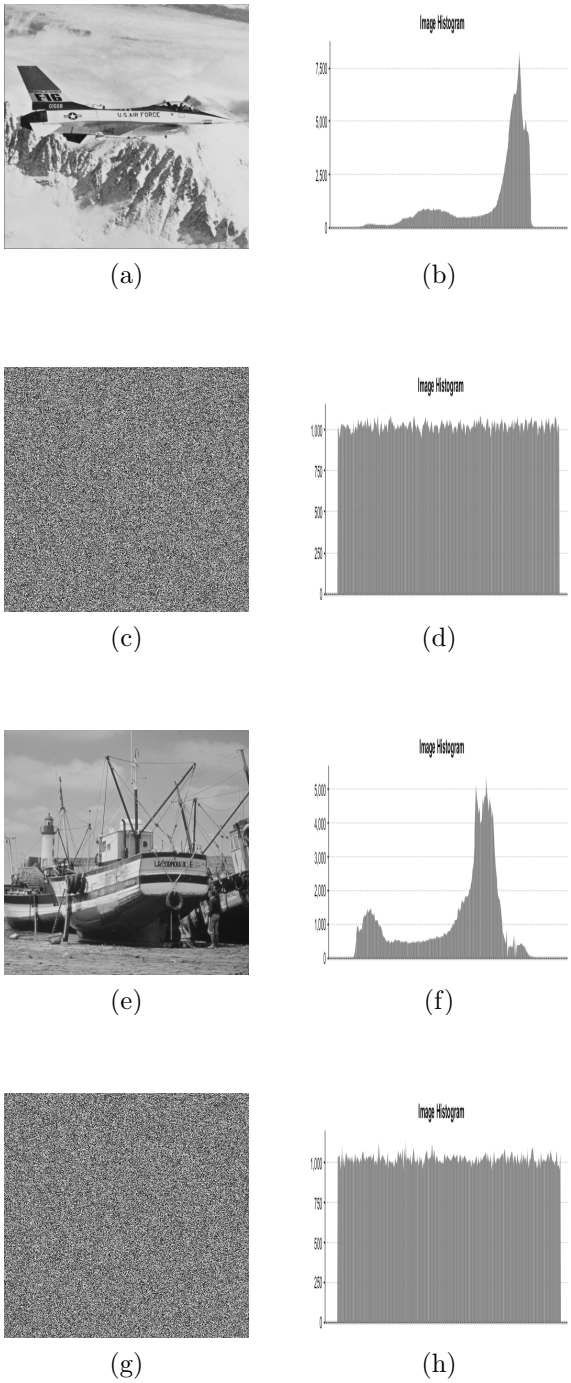
(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figure 3.6: Histogram test of plain/cipher image: (a) Plain Airplane grayscale standard test image 512×512 pixels, (b) its corresponding histogram, (c) Cipher Airplane, (d) its corresponding histogram; (e) Plain Boat grayscale standard test image 512×512 pixels, (f) its corresponding histogram, (g) Cipher Boat, (h) and its corresponding histogram: cryptosystem-A



(a) (b)

(c) (d)

(e) (f)

(g) (h)

Figure 3.7: Histogram test of plain/cipher image: (a) Plain Airplane grayscale standard test image 512×512 pixels, (b) its corresponding histogram, (c) Cipher Airplane, (d) its corresponding histogram; (e) Plain Boat grayscale standard test image 512×512 pixels, (f) its corresponding histogram, (g) Cipher Boat, (h) and its corresponding histogram: cryptosystem-B

3.3.2.2 Entropy analysis

Shannon's entropy is one of the commonly employed metrics of randomness. It is calculated by following the equation (2.5), of section 1.3.1.2 of chapter 1.Table 3.3 presents the obtained results of the entropy test for different cipher images, attained by applying some existing methods with respect to our proposals (i.e., cryptosystem-A, cryptosystem-B). Clearly, the obtained results are very nearby to the theoretical value (i.e., the truly random source entropy which is 8), and hence indicates the unpredictability and the randomness of our cipher algorithms.

Table 3.3: Comparison of Entropy test with existing methods

Encryption method	Image	Image size	Entropy
Cryptosystem-A	Lena	$512 \times 512 \times 1$	7.999303
Cryptosystem-B	Lena	$512 \times 512 \times 1$	7.999287
Ref. [130]	Lena	$512 \times 512 \times 1$	7.9992
Ref. [11]	Lena	$512 \times 512 \times 1$	7.9696
Ref. [131]	Lena	$512 \times 512 \times 1$	7.999317
Ref. [146]	Lena	$512 \times 512 \times 1$	7.999301
Ref. [20]	Lena	$512 \times 512 \times 1$	7.9993
Cryptosystem-A	Peppers	$512 \times 512 \times 1$	7.999253
Cryptosystem-B	Peppers	$512 \times 512 \times 1$	7.999221
Ref. [90]	Peppers	$512 \times 512 \times 1$	7.9987
Ref. [130]	Peppers	$512 \times 512 \times 1$	7.9993
Ref. [11]	Peppers	$512 \times 512 \times 1$	7.9717
Ref. [131]	Peppers	$512 \times 512 \times 1$	7.999297
Ref. [146]	Peppers	$512 \times 512 \times 1$	7.999270
Cryptosystem-A	Peppers	$256 \times 256 \times 1$	7.997128
Cryptosystem-B	Peppers	$256 \times 256 \times 1$	7.997452
Ref. [98]	Peppers	$256 \times 256 \times 1$	7.9970
Cryptosystem-A	Baboon	$512 \times 512 \times 1$	7.999375
Cryptosystem-B	Baboon	$512 \times 512 \times 1$	7.999346
Ref. [146]	Baboon	$512 \times 512 \times 1$	7.999233
Ref. [20]	Baboon	$512 \times 512 \times 1$	7.9993
Cryptosystem-A	Baboon	$256 \times 256 \times 1$	7.997367
Cryptosystem-B	Baboon	$256 \times 256 \times 1$	7.997603
Ref. [98]	Baboon	$256 \times 256 \times 1$	7.9972
Cryptosystem-A	Boat	$512 \times 512 \times 1$	7.997699
Cryptosystem-B	Boat	$512 \times 512 \times 1$	7.999342
Ref. [11]	Boat	$512 \times 512 \times 1$	7.9706
Ref. [131]	Boat	$512 \times 512 \times 1$	7.999296
Cryptosystem-A	Airplane	$512 \times 512 \times 1$	7.999273
Cryptosystem-B	Airplane	$512 \times 512 \times 1$	7.999280
Ref. [146]	Airplane	$512 \times 512 \times 1$	7.999343
Cryptosystem-A	Cameraman	$256 \times 256 \times 1$	7.997675
Cryptosystem-B	Cameraman	$256 \times 256 \times 1$	7.997391
Ref. [20]	Cameraman	$256 \times 256 \times 1$	7.9974

3.3.2.3 Local entropy analysis

The global Shannon entropy is deemed to be inappropriate metric to measure the true randomness of a given image. To this end, the newly proposed measurement by Wu et al. more recently [138], namely, local Shannon entropy is adopted by following all the aforesaid steps of the procedure described in detail in section 1.3.1.3 of chapter 1.Table 3.4 presents the obtained results of the local entropy test for different cipher images, attained by applying some existing methods including our proposed approaches. According to the obtained results, it is obvious that the local entropies fall with the acceptance interval at 5

Table 3.4: Comparison of Local entropy test with existing methods

Encryption method	Image [1]	Local entropy	Local entropy critical value k=30, $T_B^{L=256*}$=1936		
			$h_{left}^{l*0.05}$=7.901901305 $h_{left}^{l*0.01}$=7.901722822 $h_{left}^{l*0.001}$=7.901515698 $h_{right}^{l*0.05}$=7.903037329 $h_{right}^{l*0.01}$=7.903215812 $h_{right}^{l*0.001}$=7.90342293 Results		
			0.05-level	0.01-level	0.001-level
Cryptosystem-A	1	7.902746984	Passed	Passed	Passed
Cryptosystem-B	1	7.902757747	Passed	Passed	Passed
Ref. [45]	1	7.902765431	Passed	Passed	Passed
Ref. [27]	1	7.903007790	Passed	Passed	Passed
Ref. [29]	1	7.902445506	Passed	Passed	Passed
Cryptosystem-A	2	7.902153049	Passed	Passed	Passed
Cryptosystem-B	2	7.902012483	Passed	Passed	Passed
Ref. [45]	2	7.998521546	Passed	Passed	Passed
Ref. [27]	2	7.902512701	Passed	Passed	Passed
Ref. [29]	2	7.903015681	Passed	Passed	Passed
Cryptosystem-A	3	7.902744142	Passed	Passed	Passed
Cryptosystem-B	3	7.902636628	Passed	Passed	Passed
Ref. [27]	3	7.903008003	Passed	Passed	Passed
Ref. [29]	3	7.902186958	Passed	Passed	Passed
Cryptosystem-A	4	7.902536407	Passed	Passed	Passed
Cryptosystem-B	4	7.902121141	Passed	Passed	Passed
Ref. [27]	4	7.902501967	Passed	Passed	Passed
Ref. [29]	4	7.902336465	Passed	Passed	Passed
Cryptosystem-A	5	7.902222999	Passed	Passed	Passed
Cryptosystem-B	5	7.902868651	Passed	Passed	Passed
Ref. [27]	5	7.902818511	Passed	Passed	Passed
Ref. [29]	5	7.902636426	Passed	Passed	Passed
Cryptosystem-A	6	7.902002122	Passed	Passed	Passed
Cryptosystem-B	6	7.902836371	Passed	Passed	Passed
Ref. [27]	6	7.901916948	Passed	Passed	Passed
Ref. [29]	6	7.902582864	Passed	Passed	Passed
Cryptosystem-A	7	7.902026437	Passed	Passed	Passed
Cryptosystem-B	7	7.902449366	Passed	Passed	Passed
Ref. [15]	7	7.903037315	Passed	Passed	Passed
Cryptosystem-A	8	7.902826553	Passed	Passed	Passed
Cryptosystem-B	8	7.902833973	Passed	Passed	Passed
Ref. [15]	8	7.902862586	Passed	Passed	Passed
Cryptosystem-A	9	7.902721743	Passed	Passed	Passed
Cryptosystem-B	9	7.902631970	Passed	Passed	Passed
Ref. [15]	9	7.902689100	Passed	Passed	Passed
Cryptosystem-A	10	7.902036530	Passed	Passed	Passed
Cryptosystem-B	10	7.902081069	Passed	Passed	Passed
Ref. [15]	10	7.902520202	Passed	Passed	Passed
Cryptosystem-A	11	7.902774504	Passed	Passed	Passed
Cryptosystem-B	11	7.902954076	Passed	Passed	Passed
Ref. [15]	11	7.902263797	Passed	Passed	Passed
Cryptosystem-A	12	7.902765303	Passed	Passed	Passed
Cryptosystem-B	12	7.902835265	Passed	Passed	Passed
Ref. [15]	12	7.902502812	Passed	Passed	Passed

3.3.2.4 Correlation analysis

The intention of each secure cipher algorithm is to decrease the high redundancies between adjacent pixels. For the sake of evaluating such desirable property, correlation of adjacent pixels is handled, according to which 10000 pairs of neighboring pixels within the plain image and its matching cipher image are arbitrarily chosen in horizontal, vertical and diagonal directions. The correlation of each pair is computed by means of equations (2.6-2.9), of section 1.3.1.4 of chapter 1. The correlation coefficients of neighboring pixels in horizontal, vertical and diagonal directions for both the standard grayscale Airplane image, and the standard grayscale Boat image are plotted in Figure 3.8 and Figure 3.9, by using cryptosystem-A and cryptosystem-B, respectively. Moreover, the obtained results of correlation coefficient values for different employed cipher images are given in Table 3.5, by applying some existing methods with respect to our proposals. Regarding the obtained results, one can observe that the correlation coefficient, in each direction, of the plain image is very nearby to one, whereas such value of the cipher version is very nearby to the theoretical value of zero. Hence, the performance of the proposed cipher algorithms in term of adjacent pixels analysis is deemed quite sufficient, to conceal the special redundancy with the cipher image's pixel values.

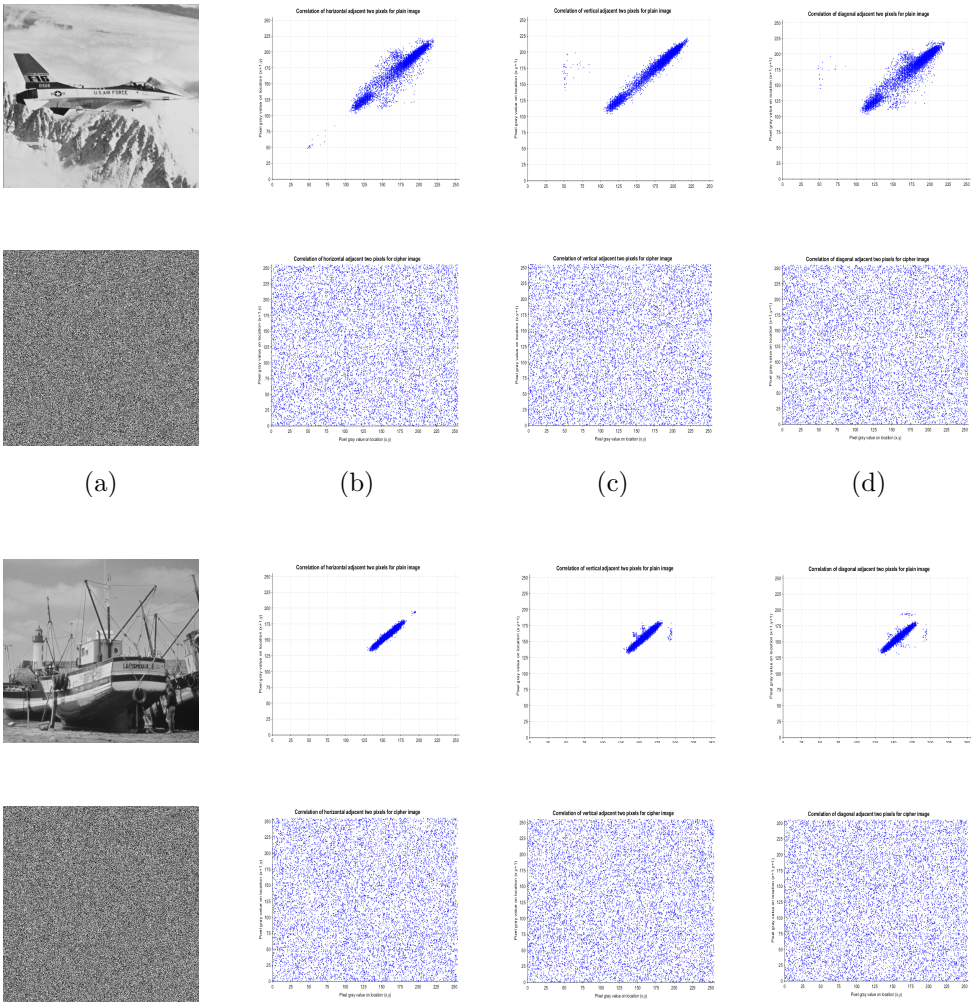
[1]

1=Lena ($512 \times 512 \times 1$)
2=Peppers ($512 \times 512 \times 1$)
3=Baboon ($512 \times 512 \times 1$)
4=Barbara ($512 \times 512 \times 1$)
5=Bridge ($512 \times 512 \times 1$)
6=Couple ($512 \times 512 \times 1$)
7=Lena ($256 \times 256 \times 1$)
8=Cameraman ($256 \times 256 \times 1$)
9=House ($256 \times 256 \times 1$)
10=Barbara ($256 \times 256 \times 1$)
11=Boat ($256 \times 256 \times 1$)
12=Trank ($256 \times 256 \times 1$)

Table 3.5: Comparison of correlation test with existing methods

Encryption method	Image [2]	Plain image correlation results			Cipher image correlation results		
		H	V	D	H	V	D
Cryptosystem-A	1	0.98911	0.98479	0.98133	0.00473	0.01489	0.00487
Cryptosystem-B	1	0.98911	0.98479	0.98133	0.00140	0.00141	-0.00247
Ref. [90]	1	0.9832	0.9725	0.9620	0.0012	0.0031	0.0022
Ref. [131]	1	0.97392	0.98446	0.96065	0.00127	0.00169	-0.00154
Ref. [146]	1	0.98498	0.97187	0.96847	0.00032	-0.00274	-0.00147
Ref. [20]	1	0.9761	0.9626	0.9448	0.0285	0.0014	0.0013
Cryptosystem-A	6	0.97977	0.96402	0.94771	0.01254	0.01006	0.00585
Cryptosystem-B	6	0.97977	0.96402	0.94771	-0.01144	0.00306	-0.00153
Ref. [98]	6	0. 92683	0.96041	0.90680	0.00070	0.02045	-0.00025
Ref. [18]	6	0.8964	0.9549	0.8612	0.0041	0.0308	0.0053
Ref. [15]	6	0.9375	0.9710	0.9257	-0.0294	-0.0014	-0.0180
Cryptosystem-A	2	0.91748	0.97419	0.90470	0.01044	0.01345	0.00984
Cryptosystem-B	2	0.91748	0.97419	0.90470	0.01204	0.00699	0.00681
Ref. [146]	2	0.98263	0.97917	0.96987	0.00187	0.00139	0.00071
Ref. [20]	2	0.9783	0.9737	0.9498	-0.0282	0.0100	-0.0012
Cryptosystem-A	7	0.95520	0.94583	0.90690	0.00678	0.00267	0.00258
Cryptosystem-B	7	0.95520	0.94583	0.90690	0.00908	0.00589	0.01911
Ref. [98]	7	0.94555	0.94074	0.94074	0.00088	-0.01975	-0.00084
Ref. [45]	7	0.9202	0.9417	0.8678	0.0119	0.0064	0.0076
Cryptosystem-A	3	0.61057	0.65975	0.52038	0.01200	0.00453	-0.00222
Cryptosystem-B	3	0.61057	0.65975	0.52038	0.00524	0.00755	0.00827
Ref. [146]	3	0.75870	0.86649	0.71577	-0.00280	-0.00073	0.00119
Ref. [20]	3	0.7142	0.8280	0.6998	0.0013	-0.0281	0.0128
Cryptosystem-A	4	0.97093	0.93652	0.94031	-0.00674	0.00641	0.00495
Cryptosystem-B	4	0.97093	0.93652	0.94031	-0.00293	0.00259	0.01139
Ref. [11]	4	0.9189	0.9028	0.9266	-0.0063	0.0095	0.0089
Cryptosystem-A	5	0.96112	0.95843	0.94326	-0.00316	0.00285	0.01265
Cryptosystem-B	5	0.96112	0.95843	0.94326	0.014460	0.00833	0.01857
Ref. [146]	5	0.96408	0.96629	0.93492	0.00384	-0.00276	0.00051
Cryptosystem-A	8	0.95974	0.95823	0.95363	-0.00293	-0.01627	0.00895
Cryptosystem-B	8	0.95974	0.95823	0.95363	-0.01491	-0.01083	0.00528
Ref. [98]	8	0.90485	0.89408	0.83092	0.00092	0.00592	0.00022
Ref. [18]	8	0.8926	0.8738	0.7996	0.0191	0.0056	0.0055

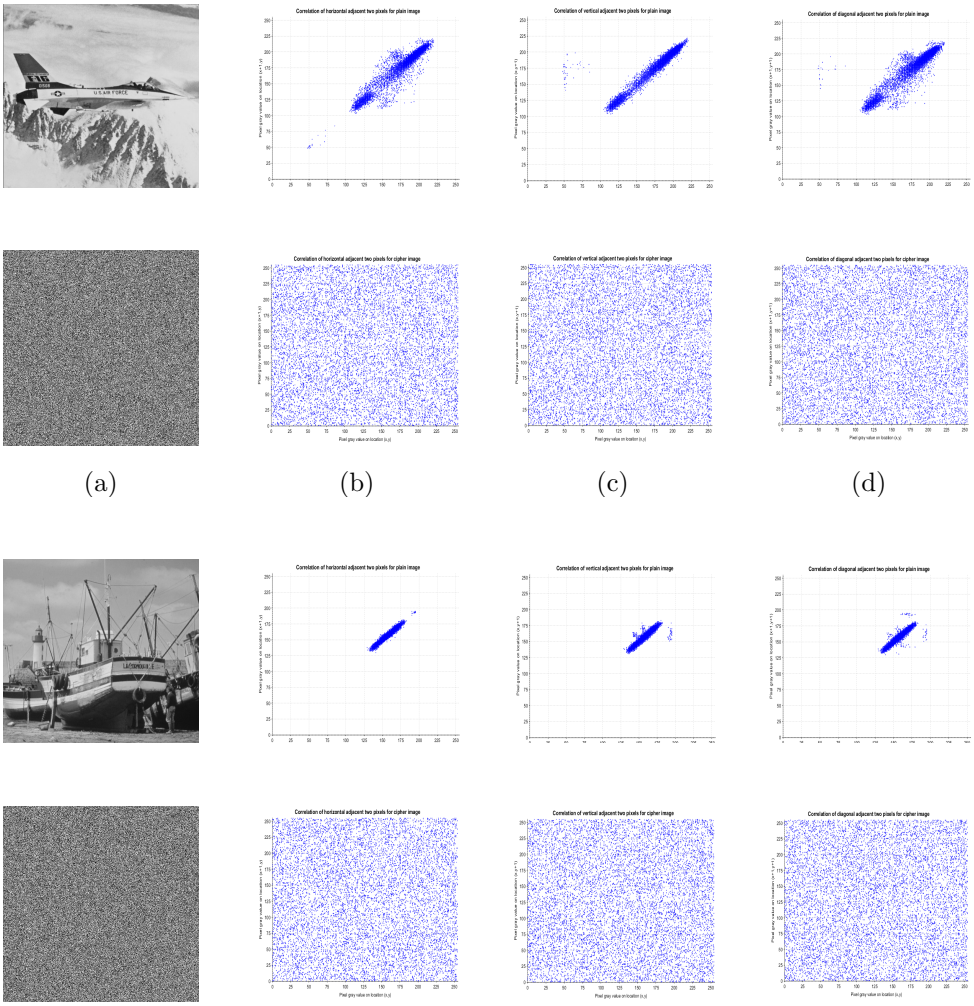
[2] H=Horizontal direction, V=Vertical direction and D=Diagonal direction
1=Lena ($512 \times 512 \times 1$)
2=Peppers ($512 \times 512 \times 1$)
3=Baboon ($512 \times 512 \times 1$)
4=Boat ($512 \times 512 \times 1$)
5=Airplane ($512 \times 512 \times 1$)
6=Lena ($256 \times 256 \times 1$)
7=Peppers ($256 \times 256 \times 1$)
8=Airplane ($256 \times 256 \times 1$)
9=Barbara ($512 \times 512 \times 1$)



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 3.8: Correlation diagrams of plain/cipher image: (a) Airplane grayscale standard test image 512 × 512 pixels, (b) horizontal correlation, (c) vertical correlation, (d) diagonal correlation; (e) Boat grayscale standard test image 512 × 512 pixels, (f) horizontal correlation, (g) vertical correlation, (h) diagonal correlation: cryptosystem-A



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 3.9: Correlation diagrams of plain/cipher image: (a) Airplane grayscale standard test image 512×512 pixels, (b) horizontal correlation, (c) vertical correlation, (d) diagonal correlation; (e) Boat grayscale standard test image 512×512 pixels, (f) horizontal correlation, (g) vertical correlation, (h) diagonal correlation: cryptosystem-B

3.3.2.5 Nist statistical test for cipher image analysis

In order to assess the randomness of the proposed cipher algorithms' output, the NIST statistical test suite [110] is carried out. In this experiment, the significant level α is set to 0.01, hence the p-value should be above 0.01 for every statistical test, in order to accept the randomness of the bit sequences. The obtained results of NIST randomness test for both Airplane and Boat standard test images of 512×512 pixels each, are given in Table

3.6 using cryptosystem-A, whereas the obtained results for the same test and the same standard images using cryptosystem-B are reported in Table 3.7. Regarding the obtained results, it is obvious that the proposed cryptosystems pass all the NIST randomness tests successfully, so that, the produced cipher images are completely stochastic.

Table 3.6: NIST test results for cryptosystem-A

Test name	p-value,(Airplane)	p-value,(Boat)	Results
Frequency	0.161393	0.445851	Success
BlockFrequency (m=128)	0.134707	0.582976	Success
CumulativeSums (Forward)	0.057699	0.445855	Success
CumulativeSums (Reverse)	0.297113	0.734927	Success
Runs	0.049707	0.472012	Success
LongestRun	0.540309	0.297128	Success
Rank	0.109939	0.605173	Success
FFT	0.795990	0.560758	Success
Non Overlapping Template (m=9B=000000001)	0.645987	0.531933	Success
Overlapping Template (m=9)	0.156278	0.312568	Success
Universal	0.930488	0.209220	Success
Approximate Entropy	0.500774	0.798411	Success
Random Excursions (x=+1)	0.528109	0.712863	Success
Random Excursions variant (x=-1)	0.579698	0.449104	Success
Serial (m=16) (1)	0.860210	0.542478	Success
Serial (m=16) (2)	0.827129	0.792958	Success
Linear Complexity	0.161252	0.443029	Success

Table 3.7: NIST test results for cryptosystem-B

Test name	p-value,(Airplane image)	p-value,(Boat image)	Results
Frequency	0.066236	0.375270	Success
BlockFrequency (m=128)	0.901953	0.833891	Success
CumulativeSums (Forward)	0.117149	0.692772	Success
CumulativeSums (Reverse)	0.058206	0.319033	Success
Runs	0.498855	0.403105	Success
LongestRun	0.676403	0.757990	Success
Rank	0.277597	0.421621	Success
FFT	0.940395	0.238037	Success
Non Overlapping Template (m=9B=000000001)	0.495445	0.920064	Success
Overlapping Template (m=9)	0.596649	0.201301	Success
Universal	0.327243	0.686422	Success
Approximate Entropy	0.864691	0.596094	Success
Random Excursions (x=+1)	0.140640	0.675714	Success
Random Excursions variant (x=-1)	0.622782	0.336761	Success
Serial (m=16) (1)	0.716997	0.404124	Success
Serial (m=16) (2)	0.701772	0.155259	Success
Linear Complexity	0.264092	0.149332	Success

3.3.3 Sensitivity test

3.3.3.1 Robustness against differential attacks

In order to withstand differential attacks, a cipher algorithm should be extremely sensitive to a minor alteration at a bit unity, applied to its input herein the plain image, in which such change should conduct to a major transformation on its output herein the cipher version. This influence is commonly measured by means of two metrics, namely, NPCR and UACI, by performing all the aforementioned steps of the procedure described in detail within section 1.3.2.1 of chapter 1.Table 3.8 presents the obtained results of NPCR and UACI values, for different cipher images, attained under the application of certain existing methods including ours. Regarding the shown experimental results, our proposals are highly sensitive to plain image bit alteration, and hence render such type of attacks void.

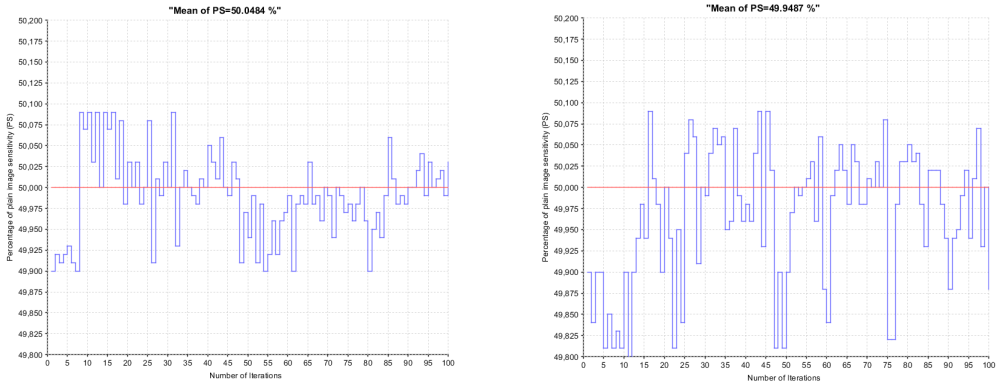
Table 3.8: Comparison of NPCR and UACI values with existing methods

Encryption method	Image	Image size	NPCR	UACI
Cryptosystem-A	Lena	$512 \times 512 \times 1$	99.6089	33.4350
Cryptosystem-B	Lena	$512 \times 512 \times 1$	99.6181	33.4386
Ref. [11]	Lena	$512 \times 512 \times 1$	99.4602	33.2161
Ref. [131]	Lena	$512 \times 512 \times 1$	99.6307	33.5663
Ref. [45]	Lena	$512 \times 512 \times 1$	99.5705	33.4781
Ref. [146]	Lena	$512 \times 512 \times 1$	99.6052	33.4111
Ref. [20]	Lena	$512 \times 512 \times 1$	99.62	33.46
Ref. [27]	Lena	$512 \times 512 \times 1$	99.6044	33.4841
Cryptosystem-A	Lena	$256 \times 256 \times 1$	99.6078	33.4871
Cryptosystem-B	Lena	$256 \times 256 \times 1$	99.6215	33.4091
Ref. [98]	Lena	$256 \times 256 \times 1$	99.5894	33.4645
Ref. [15]	Lena	$256 \times 256 \times 1$	99.6124	33.4734
Cryptosystem-A	Peppers	$512 \times 512 \times 1$	99.6082	33.4722
Cryptosystem-B	Peppers	$512 \times 512 \times 1$	99.6192	33.4236
Ref. [11]	Peppers	$512 \times 512 \times 1$	99.5643	33.5724
Ref. [131]	Peppers	$512 \times 512 \times 1$	99.6196	33.4530
Ref. [45]	Peppers	$512 \times 512 \times 1$	99.5884	33.5134
Ref. [146]	Peppers	$512 \times 512 \times 1$	99.6052	33.4372
Ref. [20]	Peppers	$512 \times 512 \times 1$	99.62	33.44
Cryptosystem-A	Boat	$512 \times 512 \times 1$	99.6204	33.5089
Cryptosystem-B	Boat	$512 \times 512 \times 1$	99.5771	33.4919
Ref. [11]	Boat	$512 \times 512 \times 1$	99.1025	33.1600
Ref. [131]	Boat	$512 \times 512 \times 1$	99.6128	33.4661
Cryptosystem-A	Boat	$256 \times 256 \times 1$	99.6307	33.5748
Cryptosystem-B	Boat	$256 \times 256 \times 1$	99.6276	33.4330
Ref. [15]	Boat	$256 \times 256 \times 1$	99.6215	33.3914
Cryptosystem-A	Baboon	$256 \times 256 \times 1$	99.6292	33.5043
Cryptosystem-B	Baboon	$256 \times 256 \times 1$	99.5956	33.4384
Ref. [98]	Baboon	$256 \times 256 \times 1$	99.6124	33.4891
Cryptosystem-A	Cameraman	$256 \times 256 \times 1$	99.6124	33.5051
Cryptosystem-B	Cameraman	$256 \times 256 \times 1$	99.6246	33.3944
Ref. [98]	Cameraman	$256 \times 256 \times 1$	99.6121	33.4734
Ref. [15]	Cameraman	$256 \times 256 \times 1$	99.6032	33.3954
Cryptosystem-A	Airplane	$256 \times 256 \times 1$	99.5971	33.5044
Cryptosystem-B	Airplane	$256 \times 256 \times 1$	99.6047	33.4415
Ref. [98]	Airplane	$256 \times 256 \times 1$	99.6116	33.4758

3.3.3.2 Plain image sensitivity

In order to confirm the degree of sensitivity of the proposed approaches against a minor change at a bit unity (herein the Least Significant Bit (LSB)) on the plain image, the scenario described in section 1.3.2.2 of chapter 1 is followed. The procedure is iterated for a set of randomly selected standard test images of different sizes. Figure 3.10 exhibits the obtained results, (a) using cryptosystem-A, and (b) using cryptosystem-B. Regarding the obtained results, the mean value of the hamming distance test for each proposed cipher is very nearby to 50% (equal to 50.0484% using cryptosystem-A, and 49.9487% using cryptosystem-B), which indicates that with a small change in the plain image, more

than 50% of transformation is appeared on the cipher version. Therefore, the proposed approaches possess sufficient sensitivity against any alteration on the plain image.

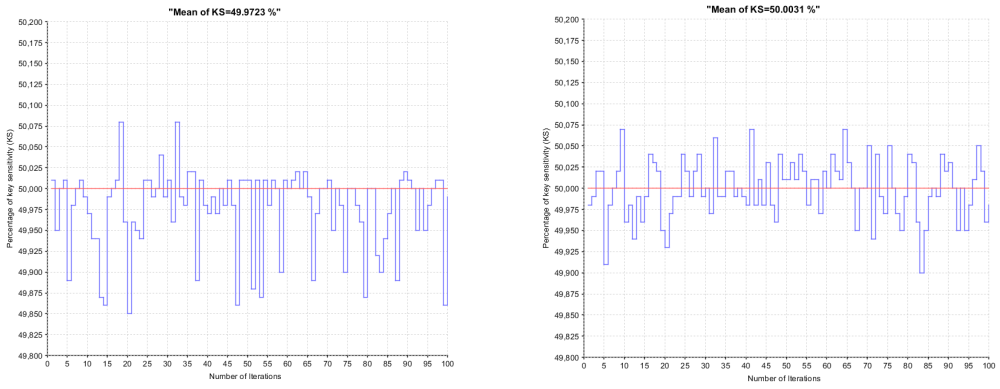


(a) (b)

Figure 3.10: (a) plain image sensitivity test for a set of random test images using cryptosystem-A; (b) plain image sensitivity test for a set of random test images using cryptosystem-B

3.3.3.3 Key sensitivity

Another desirable property for any cipher algorithm is its sensitivity to a slight change at a bit unity, applied to its input herein the secret key, in which such change should lead to a major transformation on its output, herein the cipher version. The influence is commonly computed by means of the percentage value of difference, by performing all the aforementioned steps of the procedure described in detail within section 1.3.2.3 of chapter 1. In cryptosystem-B, the generated keys employed in both confusion and diffusion modules are relied on the initial values of 1D LTS chaotic system, namely, the initial condition $x_0 \in [0, 1]$, and the control parameter $r_0 \in (0, 4]$, extracted and updated by means of the external secret key of 512 bits, and the Wh value of 8 bits that handles the plain images features. To this end, the experiment of key sensitivity is carried out as follows: at first, the cipher image herein C_1 is attained using the key K_1 $(x_0 = 0.53, r_0 = 3.999, k)$ as shown in Figure (a) of Figures 3.12/ Figures 3.13, secondly, the cipher image C_2 is attained using the keyK_2 $(x_0 = 0.53 + \Delta\delta, r_0 = 3.999, k)$ like the one in (b) of Figures

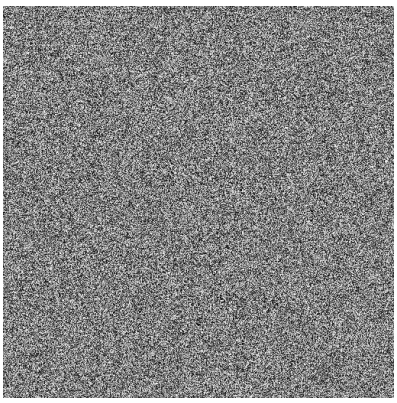


(a) (b)

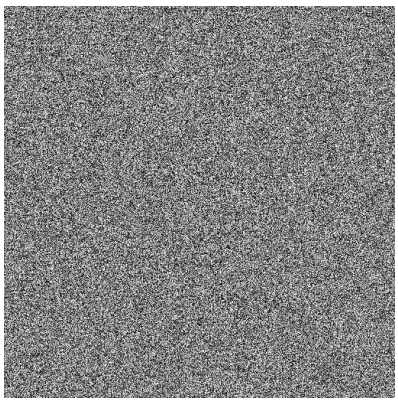
Figure 3.11: (a) Key sensitivity test for a set of random test images using cryptosystem-A; (b) plain image sensitivity test for a set of random test images using cryptosystem-B

3.12/ Figures 3.13, such test is extended to cover the decryption procedure, so that, Figure (c) of Figures 3.12/ Figures 3.13 represents the deciphered image using the correct key i.e., K_1 $(x_0 = 0.53, r_0 = 3.999, k)$, whereas the one of (d) represents the deciphered image using the perturbed key i.e.,K_2 $(x_0 = 0.53 + \Delta\delta, r_0 = 3.999, k)$, where $\Delta\delta$ is a very small value called the perturbing value [11], within our experiment, it is equal to 10^{-15} , we should notice that, it is the only perturbed value and the other parameter values of the key are kept unmodified, at last the percentage value of dissimilarities is measured using the equation (2.14), of section 1.3.2.3 of chapter 1. Table 3.9 presents the obtained results under the employment of certain standard test images of different sizes, for both encryption and decryption procedures.

Moreover, and for the sake of evaluating the degree of sensitivity of the proposed approaches against a little change at a bit unity (herein the Least Significant Bit (LSB)) on the secret key, the scenario described in section 1.3.2.2 of chapter 1 is followed, exactly as it was adapted in section 3.3.3.2. The procedure is iterated for 100 different keys. Figure 3.11 exhibits the obtained results, (a) using cryptosystem-A, and (b) using cryptosystem-B. The obtained results are very nearby to the critical value of 50%, where the resultant mean value is 49.9723% using cryptosystem-A, and 50.0031% using cryptosystem-B, according to which the robustness of our proposals is validated against any minor change in the secret key, and thus the avalanche effect is achieved.

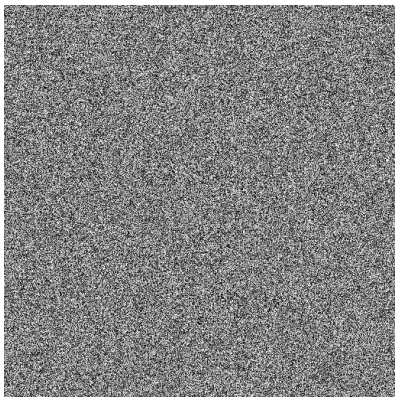


(a) Enciphered with K_1 ($x_0^{'} = 0.53$)



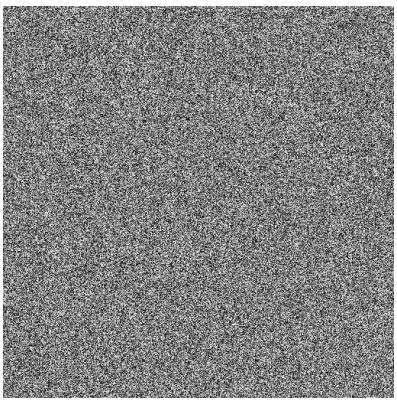
(b) Enciphered with K_2 ($x_0^{'} = x_0 + \Delta\delta$)

(c) Deciphered with correct key

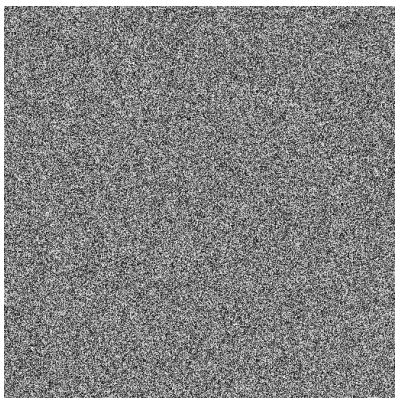


(d) Deciphered with perturbed key)

Figure 3.12: Shows the key sensitivity experiment for Airplane standard test image: cryptosystem-B

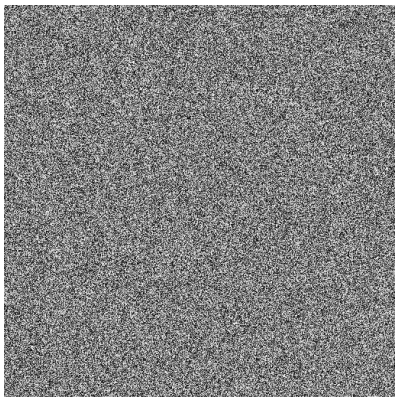


(a) Enciphered with K_1 ($\acute{x_0} = 0.53$)



(b) Enciphered with K_2 ($\acute{x_0} = x_0 + \Delta\delta$)

(c) Deciphered with correct key



(d) Deciphered with perturbed key)

Figure 3.13: Shows the key sensitivity experiment for Boat standard test image: cryptosystem-B

Table 3.9: Key sensitivity test results for standard test images

Encryption method	Secret key	Image	Image size	Difference rates (%)	
				Encryption	Decryption
	ρ_1 ($x'_0 = x_0 + \Delta\delta$)				
Cryptosystem-B		Lena	$512 \times 512 \times 1$	99.6383	99.6047
		Lena	$256 \times 256 \times 1$	99.6261	99.5941
		Peppers	$512 \times 512 \times 1$	99.5853	99.5880
		Peppers	$256 \times 256 \times 1$	99.6627	99.6047
		Boat	$512 \times 512 \times 1$	99.5944	99.6101
		Boat	$256 \times 256 \times 1$	99.6322	99.5986
		Airplane	$512 \times 512 \times 1$	99.6047	99.6128
		Airplane	$256 \times 256 \times 1$	99.6307	99.6109
	ρ_2 ($x'_0 = x_0 - \Delta\delta$)				
		Lena	$512 \times 512 \times 1$	99.6177	99.6013
		Lena	$256 \times 256 \times 1$	99.6261	99.5941
		Peppers	$512 \times 512 \times 1$	99.6376	99.6128
		Peppers	$256 \times 256 \times 1$	99.6627	99.6047
		Boat	$512 \times 512 \times 1$	99.6234	99.6154
		Boat	$256 \times 256 \times 1$	99.6322	99.5986
		Airplane	$512 \times 512 \times 1$	99.6227	99.6034
		Airplane	$256 \times 256 \times 1$	99.6307	99.5925
	ρ_3 ($r'_0 = r_0 + \Delta\delta$)				
		Lena	$512 \times 512 \times 1$	99.6185	99.6082
		Lena	$256 \times 256 \times 1$	99.6139	99.6098
		Peppers	$512 \times 512 \times 1$	99.6040	99.6135
		Peppers	$256 \times 256 \times 1$	99.6185	99.6131
		Boat	$512 \times 512 \times 1$	99.6223	99.6215
		Boat	$256 \times 256 \times 1$	99.5891	99.6227
		Airplane	$512 \times 512 \times 1$	99.6261	99.5964
		Airplane	$256 \times 256 \times 1$	99.6040	99.5967
	ρ_4 ($r'_0 = r_0 - \Delta\delta$)				
		Lena	$512 \times 512 \times 1$	99.6166	99.6242
		Lena	$256 \times 256 \times 1$	99.6144	99.6120
		Peppers	$512 \times 512 \times 1$	99.6040	99.5990
		Peppers	$256 \times 256 \times 1$	99.6002	99.5975
		Boat	$512 \times 512 \times 1$	99.6196	99.6063
		Boat	$256 \times 256 \times 1$	99.6200	99.5975
		Airplane	$512 \times 512 \times 1$	99.6112	99.6208
		Airplane	$256 \times 256 \times 1$	99.6192	99.6212

3.3.4 Performance analysis

3.3.4.1 Computational speed analysis

Besides to the security consideration, some other issues on image encryption methods are also important, including time consuming. The performance in term of execution time of our proposed cipher algorithms (herein cryptosystem-A, cryptosystem-B) is assessed under different test images of different sizes, in which the mean value is reported for both

encryption and decryption procedures. The experiment is handled using C compiler, on PC with 3 GHz processor Intel Core i7-2600, with 8Gb, and windows 7, 64-Bit operating system. The algorithms are executed under 100 times, and then the average encryption/decryption time is computed for every considered test image. The obtained results of the average encryption/decryption times for different employed cipher images of different sizes are presented in Table 3.10, by applying some existing methods with respect to our proposals. Regarding the obtained results, it is obvious that our proposed methods point to the achieved speed of calculations enhancements compared to certain existing methods.

Table 3.10: Comparison of the average encryption/decryption time with existing methods

Encryption method	Image size	Type	Execution time (ms)	
			Encryption	Decryption
Cryptosystem-A	$256 \times 256 \times 1$	CA	81	80
	$512 \times 512 \times 1$		257	257
	$1024 \times 1024 \times 1$		933	933
Cryptosystem-B	$256 \times 256 \times 1$	CA combined chaos	103	97
	$512 \times 512 \times 1$		369	336
	$1024 \times 1024 \times 1$		1303	1184
Ref. [90]	$256 \times 256 \times 1$	CA	189	Not reported
	$512 \times 512 \times 1$		758	Not reported
	$1024 \times 1024 \times 1$		3097	Not reported
Ref. [148]	$256 \times 256 \times 1$	Chaos	178	Not reported
	$512 \times 512 \times 1$		663	Not reported
	$1024 \times 1024 \times 1$		3141	Not reported
Ref. [71]	$256 \times 256 \times 1$	Chaos	120	Not reported
	$512 \times 512 \times 1$		475	Not reported
	$1024 \times 1024 \times 1$		1951	Not reported
Ref. [137]	$256 \times 256 \times 1$	Chaos	7641	Not reported
	$512 \times 512 \times 1$		34463	Not reported
	$1024 \times 1024 \times 1$		151709	Not reported

3.4 Conclusion

This chapter discusses the system design and realization of two cipher algorithms for image content protection. The first proposal herein cryptosystem-A is a novel contribution in the literature of cellular automata (CA) based ciphers, it is based on quadtree decomposition mechanism (QTD) jointly a special class of cellular automata concept, namely, 4^{th} order reversible memory cellular automata. The proposed approach handles a randomized

encryption property, and performed under the application of two iterative modules: mixing module and diffusion module. The second proposal herein cryptosystem-B is relied on the combination of two different dynamical systems means, namely, chaos in combination with cellular automata, aiming to investigate the strongpoint of each concept in terms of security and time efficiency. The proposed approach introduces a new metric to represent the characteristic of the plain image, this latter together with the external secret key contribute in the mechanism of producing one time keys, that are employed overall the cryptosystem, the proposal is based on two iterative modules: confusion module and diffusion module. The robustness and effectiveness of the newly proposed cipher algorithms are tested against all the commonly considered cryptographic attacks which include: key space attacks, key sensitivity attacks, statistical attacks, differential attacks besides to other security and time performance issues, and a comparison with respect to related existing methods is given. Indeed, the obtained results of the proposed approaches point to the achieved security improvements and calculation time reduction compared to certain existing methods.

Chapter 4

Design and Realization of Secure and Efficient Chaos -based cryptosystems

It is required for a good cipher to accomplish some basic cryptographic significance, namely, confusion, diffusion and randomness, these desirable properties can be reached with the specific features of chaotic systems like ergodicity, sensitivity to initial conditions/ system parameters and random behavior, so that, this class of dynamical systems, which has grasped the attention of several researchers during the last two decades, seems to be a good candidate to be investigated as a base to design new proposals, especially for practical use, as regards to their reasonable computational time, high security level and complexity [26, 141].

In this chapter, a new chaotic cipher algorithm for efficient and secure image content preservation is introduced, this method is considered faster than the previous proposed cryptosystems with a higher security level, it is specialized for both standard and medical images, and consists of two modules which are iteratively performed: chaotic confusion and pixel diffusion. An improved 1D chaotic system (i.e., Logistic Tent System (LTS)) is employed in both confusion and diffusion modules, where its initial conditions are dynamically generated and controlled by the external secret key of 256-bit length and SHA-256 hash value of the plain image, conducted to random-like generating key-streams, elevated the sensitivity to small changes on the plain image, and hence ensured the immunity of the proposal against known/chosen plain image attacks. The confusion module is governed by a novel nonlinear bit-shuffling and circular-shifting technique, aiming to achieve bit balancing effect, mixing effect of the pixel value, and certain diffusion mechanism. The diffusion module is ruled by means of an improved XOR operation (eXOR), to further pro-

mote the sensitivity to plain image, and accelerate the diffusion mechanism of the overall cipher algorithm. Given that the diffusion mechanism with respect to pixel value mixing are contributed by the two modules, only one encryption round is needed to make a good combination between computational performance, and sufficient security. The chapter is structured as follows: section 4.1 presents the basic definitions concerning an improved 1D chaotic system and expanded XOR operation. The detailed nonlinear bit-level shuffling and circular shifting based confusion, and pixel diffusion modules are discussed in section 4.2.Section 4.3 exhibits the effectiveness of the newly proposed confusion technique. A comparative study of performance, in terms of security level and execution time, is introduced in section 4.4. Finally, section 4.5 gives a conclusion to this chapter.

4.1 Mathematical background

4.1.1 Chaotic behavior of the improved 1D chaotic system

In [148], three improved 1D chaotic systems, namely, Logistic-Tent system (LTS), Logistic-Sine system (LSS) and Tent-Sine system, were more recently suggested in the scientific literature. Each chaotic system is a nonlinear mixture of two different and existing 1D chaotic maps, i.e., Logistic map, Tent map and Sine map, which are considered as seed maps. Logistic-Tent system (LTS) is arbitrary chosen to be employed in our chaos-based proposals, it is relied on the nonlinear combination of both Logistic map and Tent map as seed maps, and it is describes as follows:

$$\begin{aligned} x_{n+1} &= A_{LT}(r, x_n) = L(r, x_n) + T((4, r), x_n) mod 1 \\ &= \begin{cases} mod(r x_n(1 - x_n) + (r - 4)x_n/2, 1), & x_n < 0.5 \\ mod(r x_n(1 - x_n) + (r - 4)(1 - x_n)/2, 1), & x_n \geq 0.5 \end{cases} \end{aligned} \tag{4.1}$$

where $r \in (0,4]$

Simulations and numerical analysis were carried out by the authors of [148] to demonstrate the excellent chaoticness that characterizes LTS, TSS and TSS. Moreover, these improved 1D chaotic systems own at least three advantages in contrast with their corresponding seed maps: (i) the chaotic sequences of the suggested chaotic systems own a uniform distribution within [0,1], in contrast with their corresponding seed maps with a restricted data ranges within [0,1]; (ii) these 1D improved chaotic systems possess a larger chaotic range; besides to their (iii) larger Lyapunov exponents in comparison with their corresponding seed maps, revealing the better chaoticness behavior.

4.1.2 The improved expanded XOR operation

The improved expanded XOR operation [23, 132] (eXOR, for short) is presented, for the sake of increasing the plain image's sensitivity, and enhancing the overall security level. For two inputs $x=\sum_{i=0}^{7} x_i$ and $r=\sum_{i=0}^{8} r_i$ the eXOR operator is defined as follows:

$$eXOR = \sum_{i=0}^{7} not(x_i \oplus r_i \oplus r_{i+1}) \times 2^i \tag{4.2}$$

Where not (x) flips a single bit x. The operator is featured by the giving property: if $eXOR(x, r)=t$, then $eXOR(t, r)=x$.Table 4.1 shows clearly the deduced property.

Table 4.1: he results of not $(x_i \oplus r_i \oplus r_{i+1})$

x_i	$r_i\ r_{i+1}$			
	00	01	10	11
0	1	0	0	1
1	0	1	1	0

4.2 New proposal

Within this section, a detailed discussion about the methodology of the proposed cipher algorithm, herein cryptosystem-C is covered.

4.2.1 An efficient and secure chaotic cipher algorithm for image content preservation (Cryptosystem-C)

The proposed cipher algorithm is comprised mainly of the iterative application of two modules: chaotic confusion and pixel diffusion. The overall proposal is controlled by means of 1D chaotic system herein Logistic Tent System (LTS). The structure of the cryptosystem is pictorially shown in Figure 4.1 for the encryption procedure part, and Figure 4.4 for the decryption procedure part.

4.2.1.1 Encryption procedure

A new encryption algorithm for efficient and secure image content preservation is presented in this chapter. This method is specialized for both standard and medical images, and it consists of two iterative phases: chaotic confusion and pixel diffusion. An improved 1D chaotic system, namely, Logistic Tent System (LTS) is employed by both of these

phases, where its dynamical initial value and system parameter are produced by means of the external secret key, and 256 bit long hash value of the plain image, for the sake of generating one-time chaotic sequences, increasing the sensitivity to small changes on the plain image, and hence ensuring the immunity of the cryptosystem against known/chosen plain image attacks. The confusion phase is governed by means of a novel nonlinear bit-shuffling and circular shifting technique, in which it composes of two iterative sub phases: in the first sub phase, every pixel's bit is relocated based on the sum of its three composed neighborhood (i.e., the bit considered to be relocated, its immediate left-bit and right-bit, and hence 2^3 possible positions can be appeared), to further introduce the mixing effect of the pixel value; in the later part sub phase, image's rows and columns are rotated, and controlled by the generated chaotic sequences, aiming to handle a certain diffusion mechanism, and achieve the bit balancing effect. The diffusion phase is ruled by means of an improved XOR operation (eXOR), aiming to elevate the sensitivity to plain image, and accelerate the diffusion mechanism of the whole cipher algorithm. A good combination between computational performance and sufficient security is achieved by our proposal under just one encryption round. The detailed description of the proposal is given below.

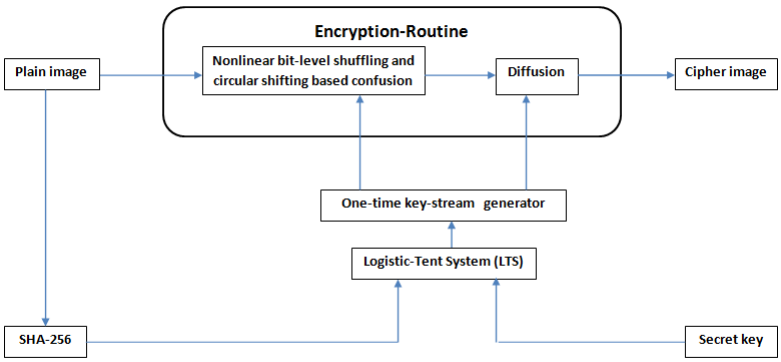


Figure 4.1: Encryption procedure part of cryptosystem-C

Generation of the variable initial value and control parameter In cryptography, SHA-256 is a commonly employed cryptographic hash function with 256-bit hash value [84]. The proposed cryptosystem herein cryptosystem-C uses 256-bit as external secret key, which can be generated by means of any cryptographic secure pseudorandom bit generator, this latter together with the 256-bit hash value of the plain image are Xored to obtain a dynamic secret key K. Hence, a cryptosystem with a total complexity of 2^{256}, is

enormous enough to withstand any kind of brute force Attacks.

- The 256-bit dynamic key is divided into 8-bit blocks (k_i) such as:

$$K = k_1, k_2, \ldots, k_{32} \tag{4.3}$$

- The initial value and the control parameter can be extracted as follows:

$$x_0^{'} = mod(x_0 + \frac{(k_1 \oplus k_2, \ldots, k_{16})}{256}, 1) \tag{4.4}$$

$$r_0^{'} = mod(x_0 + \frac{(k_{17} \oplus k_{18}, \ldots, k_{32})}{256}, 4) \tag{4.5}$$

Where x_0 and r are the given initial values.

Obviously, the new initial values of LTS chaotic system, namely $x_0^{'}$ and $r_0^{'}$ are greatly sensitive to a minor change at a bit-level applied to either the secret key or the plain image, hence, they are both secret key/plain image related, leading to the production of dissimilar chaotic sequences for different plain images even with identical set of keys.

Nonlinear bit-level shuffling and circular-shifting based confusion module In [151], Zhu et al. pointed out their conclusion of that, different information content is carried by bits at different positions in a pixel. As an example, a "1" at the 8^{th} bit's location within a pixel represents 128 (2^7), however at the 1^{st} bit's location it only represents 1 (2^0). The percentage of information $p(i)$ provided by the ith bit is computed using equation (4.7), and listed in Table 4.2.

Table 4.2: The percentage of information provided by each pixel's bit

Bit location	The percentage of information $p(i)$ (%)
0	0.3922
1	0.7843
2	1.5685
3	3.137
4	6.275
5	12.55
6	25.10
7	50.20

$$p(i) = \frac{2^i}{\sum_{i=0}^{7}}, i = \{0, 1, \ldots, 7\} \tag{4.6}$$

From Table 4.2, it is obvious that the higher 4 bits carry 94.125% of the total pixel's information, however with the lower 4 bits, this pixel's information is less than 6%. Based on this conclusion, a permutation method at a bit-level (BLP) is suggested [151], in which the higher 4 bits are permuted individually, whereas the remaining 4 lower bits are considered as a whole and relocated, in order to reduce the computation cost.

On the other hand, the computed information percentage of different pixel's bits using Zhan's equation, can't reflect the real information distinguished by the human eyes, more precisely in case of medical images, in which these later possess more than 70% of 0's bits, and by the way are quite different from the usual standard images [30]. Moreover, the lower bit-planes of medical images should be treated similarly as higher bit-planes in term of security level for the sake of sensitive information content preservation. In this sense, image encryption proposals with elevated concentration to higher bit-planes, and less attention to lower bit-planes [151] are not appropriated for this special kind of images. To address the above-mentioned limitations, a new permutation method is proposed, in which similar level of security is provided for each pixel's bit constitution. Hence, the suggested bit- permutation is well-matched for both standard images and medical images. Figure 4.2 and Figure 4.3 display the set of the employed standard 256 grayscale images of 512×512 size, and medical 256 grayscale images of 512×512 size, respectively.
The steps of the newly proposed confusion strategy are described as follows:

- **Input:** gray-scale image P of size $M \times N$, in which M is the number of rows, N is the number of columns, the computed initial condition $\acute{x_0}$ and control parameter $\acute{r_0}$, using equations (4.4) and (4.5), respectively.

- **Ouput:** the confused image $\acute{\acute{P}}$.

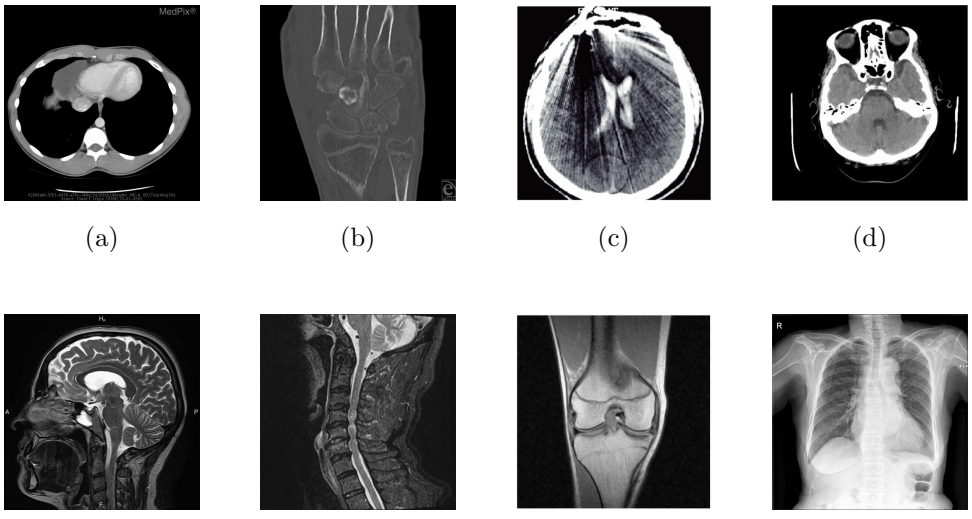
- **Step1:** Get the hash value of the gray-scale image P, together with the utilized 256-bit external secret key are Xored to obtain the dynamic key K, this latter is used to calculate the initial values of equation (4.2) through equations (4.4) and (4.5).

- **Step2:** Iterate equation (4.2) for l ($l \geq 500$) times to avoid the transient effect, using the updated initial condition $\acute{x_0}$ and control parameter $\acute{r_0}$. Continue to iterate the LTS chaotic system for M times, $8 \times M$ times and $8 \times M$ times, to obtain three chaotic sequences with length M, $M \times 8$ and $M \times 8$ respectively i.e., $init - conf$=$\{$ $init - conf_1$, $init - conf_2$, ... ,$init - conf_M$ $\}$, , V^1= $\{$ V_1^1, V_2^1, ..., $V_{M\times 8}^1$ $\}$ and V^2= $\{$ V_1^2, V_2^2, ..., $V_{M\times 8}^2$ $\}$.

(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 4.2: The standard test images: (a) Lena; (b) Peppers; (c) Baboon; (d) Lake; (e) Boats; (f) Bridge; (g) Goldhill; (h) Barbara



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 4.3: The medical test images: (a) CT-Abdomen; (b) CT-Hand; (c) CT-Head; (d) CT-Paranasal-sinus; (e) MR-Brain; (f) MR-Cervital-vertibra; (g) MR-Knee; (h) X-Chest

- **Step3:** In the bit-shuffling process, the plain image P and the shuffled image $\acute{P}$ with size $M \times N$ are viewed as two-dimensional (2D) arrays, and the generated chaotic sequence $init - conf$ is employed to relocate the bits of each plain image's pixel as follows:

1. For i=1 : M

   (a) For j=1 : N , read pixels for each plain image's row,

   $$Row_j = P(i, j) \tag{4.7}$$

   (b) Get the equivalent binary array of Row_j, denoted by Row_{bin}

   (c) Each Row_{bin}'s bit is exchanged based on the neighborhood's sum of the bit considered to be relocated. The neighborhood is composed of three adjacent bits extracted from $init - conf$, and it is consisted of: the bit located at the same position of the bit considered to be relocated $(c - bit)$, its immediate left-bit $(l - bit)$ and right-bit $(r - bit)$, the new position (NB) is calculated as follows:

   $$NB = (l - bit \times 2^2 + c - bit \times 2^1 + r - bit \times 2^0) \tag{4.8}$$

   To solve the problem of boundaries, the bits of the Row_{bin} array are concatenated together in a cyclic form to establish periodic boundary condition.

   (d) Modular addition operation is performed to each P's row as follows:

   $$Row_{\acute{j}} = (Row_j + init - conf) mod 256 \tag{4.9}$$

   Where Row_j is the resulted row after applying Step 3.1.c, $init - conf$ is the generated chaotic sequence, mod is the module operation, and $Row_{\acute{j}}$ is the resulted row after applying Step 3.1.d.

   (e) And the $init - conf$ is updated as follows:

   $$init - conf = Row_j \tag{4.10}$$

- **Step4:** In the circular-shifting process, the shuffled image $\acute{P}_1$ and the confused image $\acute{P}$ with size $M \times N$ are viewed as two-dimensional (2D) arrays. Each shuffled image's row and column are rotated based on the generated chaotic sequences V^1 and V^2 respectively, and it is described as follows:

1. For i=1 : M

   (a) For j=1 : N , read pixels for each shuffled image's row,

   $$Row_j = \acute{P}_1(i, j) \tag{4.11}$$

(b) Get the equivalent binary array of Row_j, denoted by Row_{bin}

(c) Row's circular shifts is performed as follows:

$$Row_{b\acute{i}n} = CircularShift(Row_{bin}, V_k^1) \tag{4.12}$$

Where the value V_k^1 determines the number in which circular shifts of Row_{bin} should be rotated through itself, k is a loop variable ranging from 1 to $8 \times M$, yielding $Row_{b\acute{i}n}$

(d) The direction of row's circular shifts is computed as follows:

$$D_{CS} = mod(V_k^1, 2) \tag{4.13}$$

2. For j=1 : N

(a) For j=1 : M , read each column's pixels from the resulted image of step 4.1, denoted by, $\acute{P}_2$

$$Col_i = \acute{P}_2(i, j) \tag{4.14}$$

(b) Get the equivalent binary array of Col_i, denoted by Col_{bin}

(c) Column's circular shifts is performed as follows:

$$Col_{b\acute{i}n} = CircularShift(Col_{bin}, V_k^2) \tag{4.15}$$

Where the value V_k^2 determines the number in which circular shifts of Col_{bin} should be rotated through itself, k is a loop variable ranging from 1 to $8 \times M$, yielding $Col_{b\acute{i}n}$

(d) The direction of col's circular shifts is computed as follows:

$$D_{CS} = mod(V_k^2, 2) \tag{4.16}$$

If D_{CS}=0 then right circular shifts is performed to image's rows and columns, with V_k^1 and V_k^2 times respectively, else left circular shifts is applied instead.

If the value within V_k^1/V_k^2 is divisible by eight, then row/column rotating procedure is viewed as pixel level permutation i.e., pixels are circularly rotated through the ith row and jth column with $V_k^1/8$ and $V_k^2/8$ steps respectively.

If the value within V_k^1/V_k^2 is not divisible by eight, then row/column rotating procedure is viewed as bit level permutation i.e., bits are circularly rotated from one pixel to another without any limitations.

Diffusion module Every confused image's pixel is subjected to be diffused by means of expanded XOR operation. Aiming to, improve the overall security level, increase the plain image sensitivity for amplifying the resistance to known/chosen plain image attacks and accelerate the diffusion effect within only one encryption round.

The steps of the improved diffusion strategy are described as follows:

- **Input:** the confused image $\acute{\acute{P}}$.
- **Ouput:** the cioher image C
- **Step1:** the confused image with size $M \times N$ is transformed to one dimensional (1D) array, $\acute{\acute{P}}$=$\acute{\acute{P}}_1$,$\acute{\acute{P}}_2$, ...,$\acute{\acute{P}}_{M\times N}$.
- **Step2:** generating one chaotic sequence X_1 using LTS chaotic system, and extracting the other one X_2 based on X_1.

$$X_1^i = \lfloor X_1^i \times 10^{15} \rfloor mod 2^9 \tag{4.17}$$

$$X_2^i = \bar{X_1^i} \oplus RCS(\bar{X_1^i}, 1) \tag{4.18}$$

  Where i is a loop variable, ranging from 1 to $M \times N$, $X_1^i \in X_1$, $X_2^i \in X_2$, $\bar{X_1^i}$ refers to the complement code of X_1^i, $\lfloor x \rfloor$ refers to obtain the nearest integer less than or equal x, $\oplus$ denotes the XOR operation and RCS (a,b) denotes the b-bit Right Circular Shift operation applied on the number a.

- **Step3:** diffuse each confused image's pixel, in which the first pixel should be computed in a specific way as follows:

$$C_1 = (eXOR(\acute{\acute{P}}_1, X_1^{M\times N}) + (\acute{\acute{P}}_0, X_2^1)) mod 2^8 \tag{4.19}$$

$$C_i = (eXOR(\acute{\acute{P}}_i, X_1^i) + (C_{i-1}, X_2^i)) mod 2^8 \tag{4.20}$$

  Where $\acute{\acute{P}}_i \in \acute{\acute{P}}$, $C_i \in C$, and $\acute{\acute{P}}_0 \in$ [0,255] in which it is served as a part of the secret key.

4.2.1.2 Decryption procedure

The decryption procedure is the same as that of the encryption one described above, however it must be performed in the reverse order. First of all, the SHA-256 hash value of the plain image should be transferred with the external secret key to the decryption part,

in order to produce the initial conditions of 1D LTS chaotic system, and hence generate the required chaotic sequences. The decryption starts by performing the diffusion phase as the first step, and nonlinear bit-level shuffling and circular-shifting based confusion phase as the later part step. As the confusion phase consists of two iterative sub phases, they also must be applied reversibly, starting with circular-shifting sub phase as the first step, image's columns and rows are circularly shifted, where the circular shift directions are switched (i.e., If D_{CS}=0 then left circular shifts is performed to image's columns and rows, with V_k^2 and V_k^1 times respectively, else right circular shifts is applied instead); as the later part bit-shuffling sub phase is carried out starting by the last images row to the first image's row. Due to the symmetric nature of encryption and decryption processes, they are essentially similar in their complexity and execution-time.

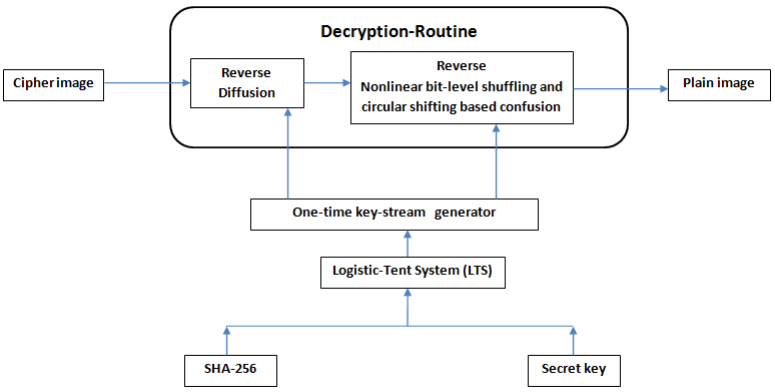


Figure 4.4: Decryption procedure part of cryptosystem-C

Reverse diffusion module Every cipher image's pixel is subjected to the reverse diffusion mechanism, using expanded XOR operation, to further recover the confused image. The steps of the reverse improved diffusion strategy are outlined as follows:

- **Input:** the cioher image C
- **Ontput:** the confused image $\acute{P}$.
- **Step1:** the cipher image with size $M \times N$ is transformed to one dimensional (1D) array, C=C_1, C_2, ..., $C_{M\times N}$.

- **Step2:** Attain the SHA-256 hash value of the original gray-scale image P, together with the utilized 256-bit external secret key are Xored to obtain the dynamic key K, this latter is used to calculate the initial values of equation (4.2) through equations (4.4) and (4.5). After that, all the employed chaotic sequences should be produced and discretized, herein $init - conf$, V^1, V^2, X_1 and X_2.

- **Step3:** the reverse diffusion is carried out from the last cipher image's pixel to the first, in which the first pixel should be computed in a specific way as follows:

$$temp_1 = (C_1 - (\acute{P}_0 \oplus X_2^1))mod2^8 \tag{4.21}$$

$$temp_i = (C_i - (C_{i-1} \oplus X_2^i))mod2^8 \tag{4.22}$$

$$\acute{P}_1 = eXOR(temp_1, X_1^{M\times N}) \tag{4.23}$$

$$\acute{P}_i = eXOR(temp_2, X_1^i) \tag{4.24}$$

Reverse nonlinear bit-level shuffling and circular-shifting based confusion module The reverse confusion module is achieved by the iterative application of its two sub modules in the reverse order as follows:

Circular-shifting sub module The process is governed by the circular rotation operation, controlled by means of the produced chaotic sequences herein V^1 and V^2, and it is essentially performed as the one described in detail within the encryption procedure, except in two points, the former one is that the confused image's columns are circularly shifted first, and then the same operation is applied to the confused images rows as well, the later part is that the direction of the circular rotation mechanism should be inverted to attain the shuffled image $\acute{P}_1$.

Bit-shuffling sub module The process is ruled by bit-level permutation, modular subtraction operation (i.e., the modular addition within the encryption procedure should be replaced by a modular subtraction), controlled by means of the produced chaotic sequence herein $init - conf$, and it is essentially carried out as the one described in detail within the encryption procedure, we have just to start from the last shuffled image's row to the first one, and perform the modular subtraction operation first, and then the bit level permutation, which is exactly as the one handled in the encryption procedure, to further recover the plain image.

4.3 Effectiveness of the proposed confusion strategy

4.3.1 The uniformity of bit distribution within each pixel's bit

The uniformity distribution of each bit-plane within a pixel is a needed property that should be accomplished by the permutation technique [145]. To this end, the bit distribution of different bit-planes for both standard and medical images is experimented. Table 4.3 and Table 4.4 clarify the obtained results using the two testing images, namely, the standard 256 grayscale Lena image 512×512 under one permutation round, and the 256 grayscale medical CT image of Abdomen (i.e., CT-Abdomen) 512×512 under two permutation rounds, respectively. One can conclude that the suggested permutation technique is very effective, to balance the percentage of "0" for both kind of images.

Table 4.3: The percentage of "0" of Lena plain vs. permuted standard image

Lena	8^{th} bit	7^{th} bit	6^{th} bit	5^{th} bit	4^{th} bit	3^{rd} bit	2^{nd} bit	1^{st} bit
Plain (%)	48.8830	57.9910	49.3618	49.7234	50.1136	50.1579	49.9458	49.9114
Permuted (%)	49.9816	49.8458	49.9176	49.8592	49.9027	49.8847	49.8668	49.9191

Table 4.4: The percentage of "0" of CT-Abdomen plain vs. permuted medical image

CT-Abdomen	8^{th} bit	7^{th} bit	6^{th} bit	5^{th} bit	4^{th} bit	3^{rd} bit	2^{nd} bit	1^{st} bit
Plain (%)	80.3260	86.5848	86.8686	86.1663	82.7411	96.0250	72.9679	76.1497
Permuted (%)	50.0785	50.1136	50.1247	50.1434	50.1209	50.1022	50.1228	49.9729

4.3.2 Pixel correlation and diffusion effect performance

One of the major roles of the permutation technique is to reduce the high redundancies between adjacent pixels. To evaluate such property, correlation of adjacent pixels is handled, in which: 3000 pairs of neighboring pixels in the plain image and its corresponding cipher image are randomly selected (in horizontal, vertical and diagonal directions). The correlation coefficient for each pair is computed by means of equations (2.6-2.9) of section 1.3.1.4 of chapter 1.

Another desirable property that should be satisfied by the permutation technique is that, not only the pixel's position should be modified but also its value [145], to further accomplish both confusion and diffusion within just this step. To assess the diffusion effect of the

proposed permutation strategy, two commonly metrics, namely, $NPCR$ (number of pixels change rate) and $UACI$ (unified average changing intensity), are handled to examine the influence of a minor change (i.e., at a bit-level) applied to the plain image on the whole cipher image. The $NPCR$ and $UACI$ values are computed by means of equation (2.10) and equation (2.12) of section 1.3.2.1 of chapter 1.

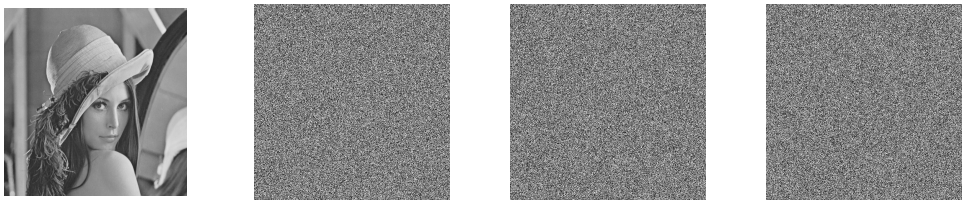
The two experiments have been conducted for a variety of standard and medical images with different sizes using the suggested permutation technique.Table 4.5 and 4.6 illustrate the simulation results for both the suggested permutation, and some other existing permutation techniques in the scientific literature. For the sake of simplicity, two testing images are selected: the standard 256 gray scale Lena image 512×512, and the medical image 256 gray scale CT-Abdomen 512×512, respectively. Figure 4.5 and Figure 4.6 show the obtained permuted images using one round (a), two rounds (b) and three rounds (c), for both the standard Lena image and medical CT-Abdomen image, respectively.

Table 4.5: Simulations of the proposed permutation and other permutation techniques using standard Lena image

Permutation technique	Rounds	Pixel correlation			NPCR (%)	UACI (%)
		Horizontal	Vertical	Diagonal		
Plain image	-	0.9891	0.9847	0.9813	-	-
Proposed	1	0.0111	0.0076	-0.0097	41.13	10.40
Proposed	2	-0.0206	0.0100	0.0110	99.50	33.10
Proposed	3	-0.0219	0.0149	-0.0025	99.60	33.46
Ref. [30]	1	-0.0032	0.0029	-0.0019	73.38	15.87
Cat map	3	0.0276	0.0226	0.0199	3.8147e-006	1.4960e-008

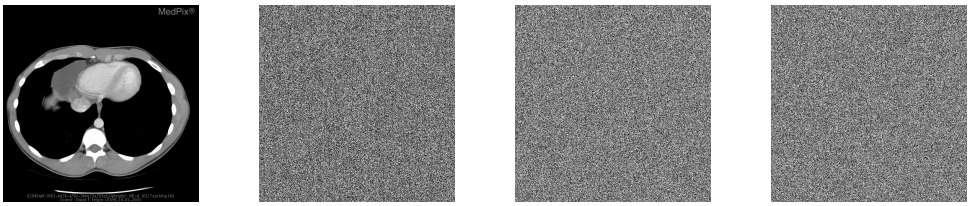
Table 4.6: Simulations of the proposed permutation and other permutation techniques using medical CT-Abdomen image

Permutation technique	Rounds	Pixel correlation			NPCR (%)	UACI (%)
		Horizontal	Vertical	Diagonal		
Plain image	-	0.8615	0.6870	0.6512	-	-
Proposed	1	0.1020	0.0192	-0.0049	6.22	1.45
Proposed	2	0.0098	0.0134	0.0048	98.63	32.64
Proposed	3	0.0169	0.0058	0.0180	99.61	33.50
BLP [151]	1	-0.0032	0.0029	-0.0019	3.8147e-006	1.4960e-008
Ref. [30]	1	-0.0134	0.0024	-0.0170	7.90	2.62
Ref. [30]	2	-0.0164	0.0083	0.0080	99.22	32.72
ES [145]	1	0.0551	0.1720	0.0538	3.8147e-006	1.4960e-008



(a) (b) (c) (d)

Figure 4.5: The application of the proposed permutation technique: (a) Lena grayscale standard test image 512×512 pixels; (b) the permuted image after one round; (c) the permuted image after two rounds; (d) the permuted image after three rounds



(a) (b) (c) (d)

Figure 4.6: The application of the proposed permutation technique: (a) CT-Abdomen grayscale medical test image 512×512 pixels; (b) the permuted image after one round; (c) the permuted image after two rounds; (d) the permuted image after three rounds

With regard to the obtained results, the effectiveness and security performance of the

suggested permutation technique can be proved in three aspects: (1) not only the pixel's location is modified but also its value as well, as a consequent, the bit distribution of the confused images exhibits a good performance of 0-1 ratio; (2) the confused images are totally indistinguishable after only one permutation round, and the relations among adjacent pixels are significantly de-correlated; (3) both confusion and diffusion are achieved within just this phase, in which the influence of a minor change by unity of one bit flipping applied to the plain image, can be extended to a larger scale on the corresponding cipher image using the proposed permutation technique, this difference is expressed by means of NPCR and UACI values. In case of standard images, these values are how about 41% $NPCR$ and 10% $UACI$, whereas they are how about 6% $NPCR$ and 1% $UACI$ in case of medical images by using only one permutation round. These values can further be improved by increasing the number of permutation rounds, where three rounds are quite enough to satisfy the expected level of $NPCR > 99.6\%$ and $UACI > 33.4\%$, for both standard and medical test images.

4.4 Security and performance analysis of the proposed cipher algorithm

This section aims to assess the performance of the proposed chaotic cipher algorithm, with regard to the level of security, where the robustness of our proposal is tested against all the considered types of cryptographic attacks, that are presented in detail within chapter 1, besides to the speed of calculation performance, on the other hand, the obtained results are compared with whose of some recent/relevant proposed ciphers in the scientific literature.

4.4.1 Key space analysis

A good cipher algorithm is one in which the best attack is an exhaustive search (i.e., brute force attacks) [74]. Owing to the remarkable growth in computational power, the key space has to be no smaller than 2^{128} [51]. In the proposed cryptosystem, the keys are built of:

1. The bit length of the external secret key of 256 bits.
2. The given initial values of x and r for LTS chaotic system.
3. The 256-bit long hash value

As for the initial values of x and r, 10^{-15} is considered as the used precision of floating point numbers, to conform with IEEE floating point standard. Furthermore, the security of SHA-256 with complexity of best attack is given as $SHA-256{=}2^{128}$ [84], besides to the employed external secret key with total complexity of 2^{256}. So, the overall key space

can be computed by the multiplication of the aforementioned possibilities as: $10^{30} \times 2^{128} \times 2^{256}=2^{384} \times 10^{30}$, hence, with this sufficiently enormous key space, all types of attacks are rendered difficult and infeasible in practical time. Moreover, Table 4.7 presents the results of key-space analysis, for some recent methods including ours.

Table 4.7: Comparison of key-space analysis with existing methods

Encryption method	Type	Key space
Cryptosystem-C	Chaos	$2^{384} \times 10^{30}$
Ref. [15]	Chaos	$> 2^{208}$
Ref. [89]	Chaos	2^{296}
Ref. [117]	Chaos	$> 2^{100}$
Ref. [10]	Chaos	10^{84}
Ref. [66]	Chaos	2^{232}
Ref. [81]	Chaos	$\approx 2^{273}$
Ref. [139]	Chaos	$\approx 2^{300}$
Ref. [30]	Chaos	$\approx 2^{197}$
Ref. [141]	Chaos	$\approx 2^{582}$

4.4.2 Statistical analysis

4.4.2.1 Uniformity analysis

Image histogram is one of the commonly used metrics for evaluating the robustness of the cipher algorithm against statistical attacks. It shows the distribution of pixel values within an image, by plotting the amount number of pixels within each gray level value. To realize such experiment, several standards and medical images have been examined with their corresponding cipher images under different secret keys. Each pair of them reveals the same result, and for each time the histogram of the cipher image is very close to the uniform distribution, and significantly different from that of the matching plain image.Figure 4.7 shows the histograms of both the standard grayscale Lena image and the medical grayscale CT-Abdomen image, using cryptosystem-C. Moreover, to demonstrate such obtained uniformity, the Chi-square is carried out, and it is calculated by means of equation (2.4), of section 1.3.1.1 of chapter 1.Table 4.8 gives the obtained results of Chi-square test, performed to the histograms of a set of medical grayscale images ($512\times512\times1$), whereas a comparison in terms of such test is performed to the cipher histograms of a set of standard grayscale images, and introduced in Table 4.9, for some existing methods including ours. All the obtained experimental values of Chi-square test are less than the critical value (i.e., 293), reflecting the efficiency of the proposed cipher to conceal the

spatial redundancy of the plain image, and hence, no detectable clue can be found to apply statistical attacks.

Table 4.8: The Chi-square test results for medical images

Test image	X^2-TEST	
	Plain image	Cipher image
CT_Abdomen	31382757.26	263.11
CT_Hand	15363981.14	235.37
CT_Head	5852617.54	266.91
CT_Paranasal_sinus	25012277.10	286.68
MR_Brain	5978910.51	253.70
MR_Cervical_Vertibra	7675854.60	209.25
MR_Knee	7088705.81	257.56
X_Chest	2439249.25	283.52

Table 4.9: Comparison of Chi-square test with existing methods

Encryption method	Image	Image size	Chi-square
Cryptosystem-C	Lena	$512 \times 512 \times 1$	240.91
Ref. [146]	Lena	$512 \times 512 \times 1$	254.15
Cryptosystem-C	Lena	$256 \times 256 \times 1$	277.53
Ref. [98]	Lena	$256 \times 256 \times 1$	184
Ref. [18]	Lena	$256 \times 256 \times 1$	263
Cryptosystem-C	Peppers	$512 \times 512 \times 1$	276.79
Ref. [146]	Peppers	$512 \times 512 \times 1$	264.92
Cryptosystem-C	Peppers	$256 \times 256 \times 1$	277.41
Ref. [98]	Peppers	$256 \times 256 \times 1$	270
Ref. [18]	Peppers	$256 \times 256 \times 1$	274
Cryptosystem-C	House	$256 \times 256 \times 1$	272.42
Ref. [18]	House	$256 \times 256 \times 1$	260
Cryptosystem-C	Baboon	$512 \times 512 \times 1$	235.93
Ref. [146]	Baboon	$512 \times 512 \times 1$	278.88
Cryptosystem-C	Baboon	$256 \times 256 \times 1$	261.60
Ref. [98]	Baboon	$256 \times 256 \times 1$	259
Ref. [18]	Baboon	$256 \times 256 \times 1$	266
Cryptosystem-C	Airplane	$512 \times 512 \times 1$	242.28
Ref. [146]	Airplane	$512 \times 512 \times 1$	238.50
Cryptosystem-C	Airplane	$256 \times 256 \times 1$	240.26
Ref. [98]	Airplane	$256 \times 256 \times 1$	246
[18]	Airplane	$256 \times 256 \times 1$	265
Cryptosystem-C	Cameraman	$256 \times 256 \times 1$	269.20
Ref. [98]	Cameraman	$256 \times 256 \times 1$	234
Ref. [18]	Cameraman	$256 \times 256 \times 1$	257

4.4.2.2 Entropy analysis

Information entropy is the commonly employed metric to express the unpredictability and randomness of information [113]. As for image information, the distribution of its grayscale values is computed, so that, the closer entropy to its theoretical value, reflects the more uniform the distribution of image grayscale values is. It is computed by following the equation (2.5), of section 1.3.1.2 of chapter 1.Table 4.10 gives the obtained results of entropy test, for medical grayscale images ($512 \times 512 \times 1$) attained by our proposal, while Table 4.11 presents the obtained experimental values for different standard cipher images, attained by applying some existing methods with respect to our proposal (i.e., cryptosystem-C). Thus, it is obvious that these values are extremely nearby to the maximum value of 8, rendering the information leakage from the proposed cipher algorithm insignificant.

Table 4.10: Information entropy test results for medical images

Test image	Plain images	Cipher images
CT_Abdomen	2.270036	7.999277
CT_Hand	2.570225	7.999352
CT_Head	5.478837	7.999263
CT_Paranasal_sinus	2.618263	7.999212
MR_Brain	3.991414	7.999299
MR_Cervical_Vertibra	3.706131	7.999424
MR_Knee	4.073966	7.999291
X_Chest	4.778157	7.999219

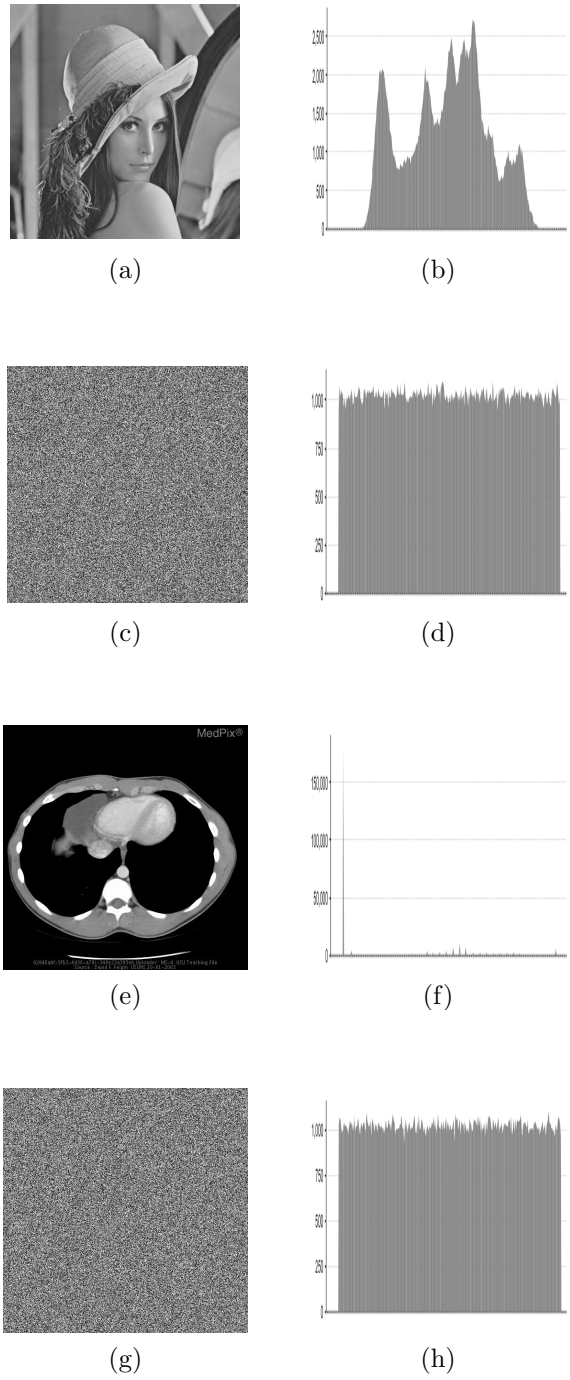


Figure 4.7: Histogram test of plain/cipher image: (a) Plain Lena grayscale standard test image 512×512 pixels, (b) its corresponding histogram, (c) Cipher Lena, (d) its corresponding histogram; (e) Plain CT-Abdomen grayscale medical test image 512×512 pixels, (f) its corresponding histogram, (g) Cipher CT-Abdomen, (h) and its corresponding histogram

Table 4.11: Comparison of Entropy test with existing methods

Encryption method	Image	Image size	Entropy
Cryptosystem-C	Lena	$512 \times 512 \times 1$	7.999338
Ref. [27]	Lena	$512 \times 512 \times 1$	7.999275
Ref. [151]	Lena	$512 \times 512 \times 1$	7.999309
Ref. [141]	Lena	$512 \times 512 \times 1$	7.999324
Ref. [28]	Lena	$512 \times 512 \times 1$	7.999319
Ref. [99]	Lena	$512 \times 512 \times 1$	7.9952
Cryptosystem-C	Lena	$256 \times 256 \times 1$	7.996951
Ref. [117]	Lena	$256 \times 256 \times 1$	7.997
Ref. [81]	Lena	$256 \times 256 \times 1$	7.9972
Ref. [139]	Lena	$256 \times 256 \times 1$	7.9973
Cryptosystem-C	Peppers	$512 \times 512 \times 1$	7.999240
Ref. [27]	Peppers	$512 \times 512 \times 1$	7.999275
Cryptosystem-C	Peppers	$256 \times 256 \times 1$	7.99694
Ref. [117]	Peppers	$256 \times 256 \times 1$	7.9973
Ref. [139]	Peppers	$256 \times 256 \times 1$	7.9975
Cryptosystem-C	Barbara	$512 \times 512 \times 1$	7.999357
Ref. [27]	Barbara	$512 \times 512 \times 1$	7.999211
Ref. [28]	Barbara	$512 \times 512 \times 1$	7.999321
Cryptosystem-C	Barbara	$256 \times 256 \times 1$	7.997047
Ref. [117]	Barbara	$256 \times 256 \times 1$	7.9971
Cryptosystem-C	Baboon	$512 \times 512 \times 1$	7.999350
Ref. [27]	Baboon	$512 \times 512 \times 1$	7.999345
Ref. [151]	Baboon	$512 \times 512 \times 1$	7.999265
Ref. [28]	Baboon	$512 \times 512 \times 1$	7.999399
Cryptosystem-C	Bridge	$512 \times 512 \times 1$	7.999424
Ref. [27]	Bridge	$512 \times 512 \times 1$	7.999268
Ref. [141]	Bridge	$512 \times 512 \times 1$	7.999380
Ref. [28]	Bridge	$512 \times 512 \times 1$	7.999254
Cryptosystem-C	Cameraman	$256 \times 256 \times 1$	7.997012
Ref. [117]	Cameraman	$256 \times 256 \times 1$	7.997
Ref. [139]	Cameraman	$256 \times 256 \times 1$	7.9973

4.4.2.3 Local entropy analysis

The global Shannon entropy is a quantitative measurement, which may fail to test the true randomness of a given image [138]. To this end, the newly proposed qualitative metric by the authors of [138], more recently, namely, local Shannon entropy is adopted by following all the aforementioned steps of the procedure described in detail in section 1.3.1.3 of chapter 1. Table 4.12 gives the obtained results of local entropy test, for medical grayscale images ($512 \times 512 \times 1$) attained by our proposal, whereas table 4.13 presents the obtained experimental values for different standard cipher images, obtained by applying some existing methods with respect to our proposed approach herein cryptosystem-C.

Table 4.12: Local entropy test results for medical images

Encryption method	Image	Local entropy	Local entropy critical value k=30, $T_B^{L=256*}$=1936		
			$h_{left}^{l*0.05}$=7.901901305 $h_{left}^{l*0.01}$=7.901722822 $h_{left}^{l*0.001}$=7.901515698 $h_{right}^{l*0.05}$=7.903037329 $h_{right}^{l*0.01}$=7.903215812 $h_{right}^{l*0.001}$=7.90342293 Results		
			0.05-level	0.01-level	0.001-level
Cryptosystem-C	1	7.902538389	Passed	Passed	Passed
Cryptosystem-C	2	7.902743781	Passed	Passed	Passed
Cryptosystem-C	3	7.902118621	Passed	Passed	Passed
Cryptosystem-C	4	7.901988273	Passed	Passed	Passed
Cryptosystem-C	5	7.902247648	Passed	Passed	Passed
Cryptosystem-C	6	7.902351692	Passed	Passed	Passed
Cryptosystem-C	7	7.902651685	Passed	Passed	Passed
Cryptosystem-C	8	7.902428283	Passed	Passed	Passed

Table 4.13: Comparison of Local entropy test with existing methods

Encryption method	Image [1]	Local entropy	Local entropy critical value k=30, $T_B^{L=256*}$=1936		
			$h_{left}^{l*0.05}$=7.901901305 $h_{left}^{l*0.01}$=7.901722822 $h_{left}^{l*0.001}$=7.901515698 $h_{right}^{l*0.05}$=7.903037329 $h_{right}^{l*0.01}$=7.903215812 $h_{right}^{l*0.001}$=7.90342293 Results		
			0.05-level	0.01-level	0.001-level
Cryptosystem-C	1	7.902256898	Passed	Passed	Passed
Ref. [45]	1	7.902765431	Passed	Passed	Passed
Ref. [27]	1	7.903007790	Passed	Passed	Passed
Ref. [29]	1	7.902445506	Passed	Passed	Passed
Cryptosystem-C	2	7.902450061	Passed	Passed	Passed
Ref. [45]	2	7.998521546	Passed	Passed	Passed
Ref. [27]	2	7.902512701	Passed	Passed	Passed
Ref. [29]	2	7.903015681	Passed	Passed	Passed
Cryptosystem-C	3	7.901988289	Passed	Passed	Passed
Ref. [45]	3	7.901877890	Passed	Passed	Passed
Ref. [27]	3	7.903008003	Passed	Passed	Passed
Ref. [29]	3	7.902186958	Passed	Passed	Passed
Cryptosystem-C	4	7.902177628	Passed	Passed	Passed
Ref. [27]	4	7.902501967	Passed	Passed	Passed
Ref. [29]	4	7.902336465	Passed	Passed	Passed
Cryptosystem-C	5	7.902995758	Passed	Passed	Passed
Ref. [27]	5	7.902818511	Passed	Passed	Passed
Ref. [29]	5	7.902636426	Passed	Passed	Passed
Cryptosystem-C	6	7.902066266	Passed	Passed	Passed
Ref. [27]	6	7.901916948	Passed	Passed	Passed
Ref. [29]	6	7.902582864	Passed	Passed	Passed
Cryptosystem-C	7	7.902793779	Passed	Passed	Passed
Ref. [15]	7	7.903037315	Passed	Passed	Passed
Cryptosystem-C	8	7.902740951	Passed	Passed	Passed
Ref. [15]	8	7.902862586	Passed	Passed	Passed
Cryptosystem-C	9	7.902995703	Passed	Passed	Passed
Ref. [15]	9	7.902689100	Passed	Passed	Passed
Cryptosystem-C	10	7.902409218	Passed	Passed	Passed
Ref. [15]	10	7.902520202	Passed	Passed	Passed
Cryptosystem-C	11	7.902098289	Passed	Passed	Passed
Ref. [15]	11	7.902263797	Passed	Passed	Passed
Cryptosystem-C	12	7.902036183	Passed	Passed	Passed
Ref. [15]	12	7.902502812	Passed	Passed	Passed

[1]
1=Lena ($512 \times 512 \times 1$)
2=Peppers ($512 \times 512 \times 1$)
3=Baboon ($512 \times 512 \times 1$)
4=Barbara ($512 \times 512 \times 1$)
5=Bridge ($512 \times 512 \times 1$)
6=Couple ($512 \times 512 \times 1$)
7=Lena ($256 \times 256 \times 1$)

4.4.2.4 Correlation analysis

One of the main features of an image with its meaningful visual content, is the high correlation and redundancy among its neighboring pixels, either in horizontal, vertical or diagonal directions. An efficient cipher algorithm should conceal such relations between adjacent pixels, and exhibit a good performance of balanced 0-1 ratio and zero correlation [43]. For the sake of evaluating such desirable property, correlation of adjacent pixels is handled, according to which 10000 pairs of neighboring pixels within the plain image and its matching cipher image are arbitrarily chosen in horizontal, vertical and diagonal directions. The correlation of each pair is computed by means of equations (2.6-2.9), of section 1.3.1.4 of chapter 1. The correlation coefficients of neighboring pixels in every direction, for both the standard grayscale Lena image and the medical grayscale CT-Abdomen image are plotted in Figure 4.8, by using cryptosystem-C. Furthermore, Table 4.14 gives the obtained results of correlation coefficient values, for medical grayscale images ($512 \times 512 \times 1$) attained by our proposal, whereas Table 4.15 presents the obtained experimental values for different standard cipher images, obtained by applying some existing methods including ours (i.e., cryptosystem-C).

Table 4.14: Correlation test results for medical images

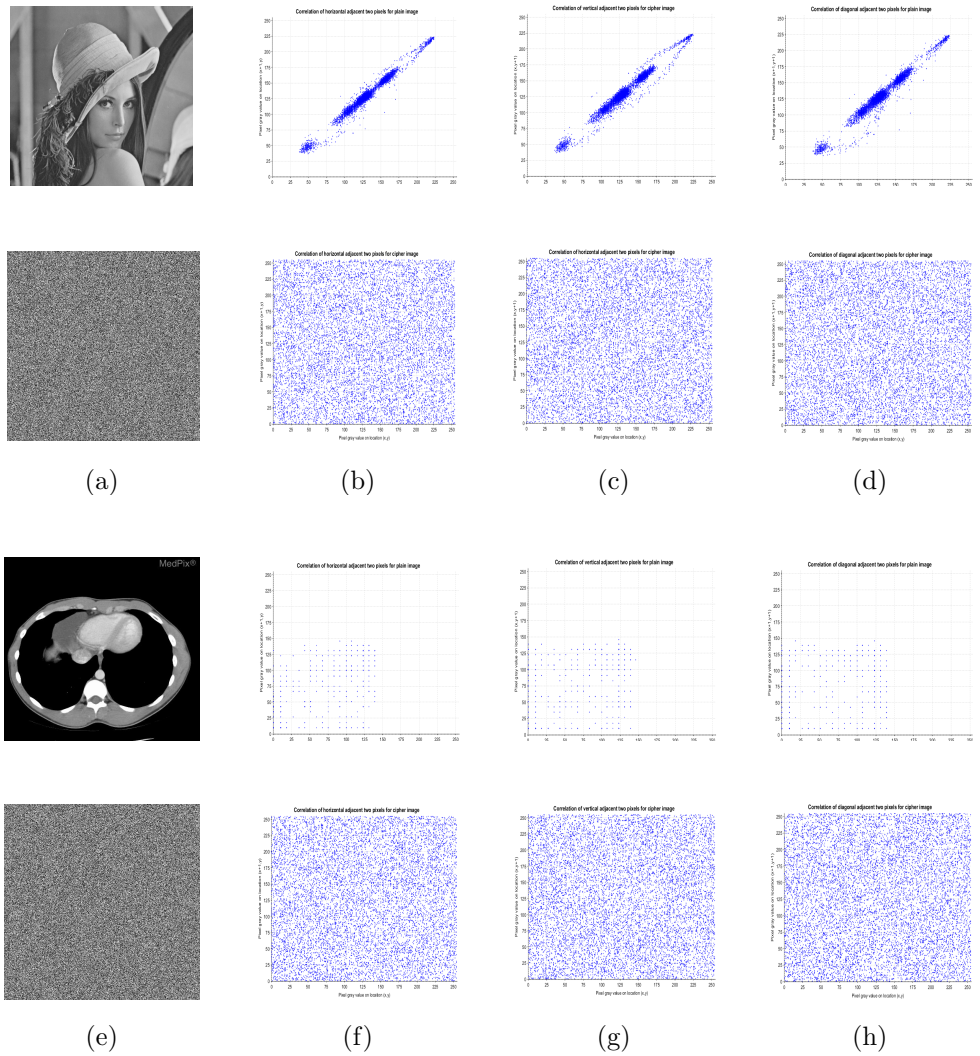
Test image	Plain			Ciphered		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
CT_Abdomen	0.86153	0.68702	0.65124	0.01919	0.00636	0.00628
CT_Hand	0.99677	0.97542	0.97226	0.01205	-0.00350	-0.00676
CT_Head	0.96784	0.98902	0.95485	-0.00613	0.00970	0.01914
CT_Paranasal_sinus	0.47818	0.77222	0.33431	0.00848	-0.00321	-0.01085
MR_Brain	0.90131	0.85195	0.82648	0.00235	0.01072	0.00286
MR_Cervical_Vertibra	0.96306	0.98312	0.95068	0.01457	-0.00453	0.00243
MR_Knee	0.96260	0.95777	0.94135	0.00337	0.00921	-0.00826
X_Chest	0.97266	0.98359	0.96500	-0.00291	0.00162	-0.00190

8=Cameraman ($256 \times 256 \times 1$)
9=House ($256 \times 256 \times 1$)
10=Barbara ($256 \times 256 \times 1$)
11=Boat ($256 \times 256 \times 1$)
12=Trank ($256 \times 256 \times 1$)

Table 4.15: Comparison of correlation test with existing methods

Encryption method	Image [2]	Plain image correlation results			Cipher image correlation results		
		H	V	D	H	V	D
Cryptosystem-C	1	0.98911	0.98479	0.98133	0.01191	0.00921	0.00132
Ref. [90]	1	0.9832	0.9725	0.9620	0.0012	0.0031	0.0022
Ref. [131]	1	0.97392	0.98446	0.96065	0.00127	0.00169	-0.00154
Ref. [146]	1	0.98498	0.97187	0.96847	0.00032	-0.00274	-0.00147
Ref. [20]	1	0.9761	0.9626	0.9448	0.0285	0.0014	0.0013
Cryptosystem-C	6	0.97977	0.96402	0.94771	0.00430	-0.00551	-0.00330
Ref. [98]	6	0. 92683	0.96041	0.90680	0.00070	0.02045	-0.00025
Ref. [18]	6	0.8964	0.9549	0.8612	0.0041	0.0308	0.0053
Ref. [15]	6	0.9375	0.9710	0.9257	-0.0294	-0.0014	-0.0180
Ref. [81]	6	0.9422	0.9682	0.9320	0.0015	0.0032	0.0008
Ref. [139]	6	0.9503	0.9755	0.9275	0.0226	0.0041	0.0368
Cryptosystem-C	2	0.91748	0.97419	0.90470	0.01155	0.01094	-0.01011
Ref. [146]	2	0.98263	0.97917	0.96987	0.00187	0.00139	0.00071
Ref. [20]	2	0.9783	0.9737	0.9498	-0.0282	0.0100	-0.0012
Ref. [117]	2	0.96682	0.93444	0.92067	0.01142	0.004505	0.00872
Cryptosystem-C	7	0.95520	0.94583	0.90690	-0.00704	0.00568	0.00257
Ref. [98]	7	0.94555	0.94074	0.94074	0.00088	-0.01975	-0.00084
Ref. [45]	7	0.9202	0.9417	0.8678	0.0119	0.0064	0.0076
Cryptosystem-C	3	0.61057	0.65975	0.52038	0.02011	-0.03262	0.00971
Ref. [146]	3	0.75870	0.86649	0.71577	-0.00280	-0.00073	0.00119
Ref. [20]	3	0.7142	0.8280	0.6998	0.0013	-0.0281	0.0128
Cryptosystem-C	4	0.97093	0.93652	0.94031	0.00233	0.01864	0.00998
Ref. [11]	4	0.9189	0.9028	0.9266	-0.0063	0.0095	0.0089
Ref. [117]	4	0.96241	0.94630	0.90249	0.00779	0.00860	0.01716
Cryptosystem-C	5	0.96112	0.95843	0.94326	0.00526	0.00754	0.00298
Ref. [146]	5	0.96408	0.96629	0.93492	0.00384	-0.00276	0.00051
Ref. [117]	5	0.96840	0.93377	0.92234	0.004492	0.00054	0.00322
Cryptosystem-C	8	0.95974	0.95823	0.95363	0.00686	0.01427	-0.01112
Ref. [98]	8	0.90485	0.89408	0.83092	0.00092	0.00592	0.00022
Ref. [18]	8	0.8926	0.8738	0.7996	0.0191	0.0056	0.0055
Cryptosystem-C	9	0.94978	0.90340	0.85259	0.01110	0.00322	0.00473
Ref. [117]	9	0.96840	0.93377	0.91247	0.01818	0.009108	0.007296

[2] H=Horizontal direction, V=Vertical direction and D=Diagonal direction
1=Lena ($512 \times 512 \times 1$)
2=Peppers ($512 \times 512 \times 1$)
3=Baboon ($512 \times 512 \times 1$)
4=Boat ($512 \times 512 \times 1$)
5=Airplane ($512 \times 512 \times 1$)
6=Lena ($256 \times 256 \times 1$)
7=Peppers ($256 \times 256 \times 1$)
8=Airplane ($256 \times 256 \times 1$)
9=Barbara ($512 \times 512 \times 1$)



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 4.8: Correlation diagrams of plain/cipher image : (a) Lena grayscale standard test image 512×512 pixels, (b) horizontal correlation, (c) vertical correlation, (d) diagonal correlation ; (e) CT-Abdomen grayscale medical test image 512×512 pixels, (f) horizontal correlation, (g) vertical correlation, (h) diagonal correlation.

4.4.2.5 Nist statistical test for cipher image analysis

A good cipher algorithm is one in which has the ability to map plain images into random cipher ones [132]. To this end, the randomness of the output cipher images is evaluated by means of the NIST statistical test suite [110]. In this experiment, the significant level α is set to 0.01, hence the p-value should be above 0.01 for every statistical test, in order to accept the randomness of the bit sequences. The obtained results of NIST randomness

test for both the standard grayscale Lena image and the medical grayscale CT-Abdomen image of 512×512 pixels each, are reported in Table 4.16 using cryptosystem-C. Regarding the obtained results, it is obvious that the proposed cryptosystem pass all the NIST randomness tests successfully, and hence verifies the hypothesis of randomness.

Table 4.16: NIST test results for cryptosystem-C

Test name	p-value,(Lena)	p-value,(CT-Abdomen)	Results
Frequency	0.822965	0.801540	Success
BlockFrequency (m=128)	0.403435	0.545148	Success
CumulativeSums (Forward)	0.969410	0.470773	Success
CumulativeSums (Reverse)	0.937696	0.690182	Success
Runs	0.408853	0.507414	Success
LongestRun	0.413831	0.431330	Success
Rank	0.853334	0.734695	Success
FFT	0.522988	0.372276	Success
Non Overlapping Template (m=9B=000000001)	0.288661	0.880150	Success
Overlapping Template (m=9)	0.970970	0.114830	Success
Universal	0.201688	0.332507	Success
Approximate Entropy	0.910882	0.887096	Success
Random Excursions (x=+1)	0.752013	0.690385	Success
Random Excursions variant (x=-1)	0.110488	0.487416	Success
Serial (m=16) (1)	0.564450	0.962215	Success
Serial (m=16) (2)	0.408515	0.718528	Success
Linear Complexity	0.451255	0.377700	Success

4.4.3 Sensitivity test

4.4.3.1 Robustness against differential attacks

As stated in section 4.2, two metrics, namely, $NPCR$ and $UACI$ are handled to evaluate the degree of the plain image's sensitivity by means of the proposed cipher algorithm. For the sake of ensuring the effectiveness and robustness against differential attacks, all the aforementioned steps of the procedure described in detail within section 1.3.1.4 of chapter 1 should be performed. The obtained results of $NPCR$ and $UACI$ values, for medical grayscale images ($512 \times 512 \times 1$) are presented in Table 4.17, using our proposal, while Table 4.18 introduces the obtained results of such experimental values, for different standard cipher images, attained under the application of certain existing methods including ours. As regards to the exhibited experimental results, our proposal is highly sensitive to plain image bit modification, and hence render such type of attacks void.

Table 4.17: $NPCR$ and $UACI$ tests results for cipher medical images

Test image	NPCR(%)	UACI(%)
CT_Abdomen	99.7920	33.5661
CT_Hand	99.5956	33.4046
CT_Head	99.6086	33.4911
CT_Paranasal_sinus	99.5903	33.4944
MR_Brain	99.6696	33.3811
MR_Cervical_Vertibra	99.6170	33.3992
MR_Knee	99.6860	33.5320
X_Chest	99.5986	33.4658

4.4.3.2 Plain image sensitivity

For the sake of revealing the degree of sensitivity of the proposed cipher's input (i.e., plain image), and how much of dissimilarities can be achieved by its output, after a minor change on its input, the scenario described in section 1.3.2.2 of chapter 1 is handled. The experiment is carried out for a set of random standard and medical images as shown in Figure 4.11(a). All of them exhibit identical results, in which the hamming distance between two cipher images C_1 and C_2 , is very close to 50%, and the resultant mean value is 50.0211%, which signifies that with a minor change by unity of one bit flipping, more than 50% of the corresponding cipher image is changed. Hence, the proposed cipher overcomes the plain image sensitivity attacks.

4.4.3.3 Key sensitivity

Another searched property for any proposed cipher algorithm is its sensitivity to secret key, and in order to evaluate the degree of such sensitivity, all the aforementioned steps of the procedure described in detail within section 1.3.2.3 of chapter 1 should be carried out. In cryptosystem-C, the produced chaotic sequences employed in both confusion and diffusion modules are relied on the initial values of 1D LTS chaotic system, namely, the initial condition $x_0 \in [0,1]$, and the control parameter $r_0 \in (0,4]$, and updated using the dynamic secret key K, which handles both the features of the external secret key of 256 bits, and the plain image by means of its 256-bit hash value. The sensitivity to the secret key for Lena standard image and CT-Abdomen medical image are exhibited in Figure 4.9 and Figure 4.10, respectively, in which Figure 4.9 (a) / Figure 4.10 (a) are the attained cipher images using the key K_1 $(x_0 = 0.53, r_0 = 3.999, k)$, whereas Figure 4.9(b)/Figure 4.10 (b) are the attained cipher images using the key K_2 $(x_0 = 0.53+, r_0 = 3.999, k)$, where is a very small value called the perturbing value [11], within our experiment, it is equal to 10^{-15} , we should notice that, it is the only perturbed value and the other parameter values of the key are kept unmodified. In the same sense, the experiment is extended to be performed for the decryption process. Figure 4.9 (c)/ Figure 4.10 (c) give the decipher images using the correct key, whereas Figure 4.9(d)/Figure 4.10(d) give the decipher images using the perturbing key. Table 4.19 gives the obtained results of secret key sensitivity

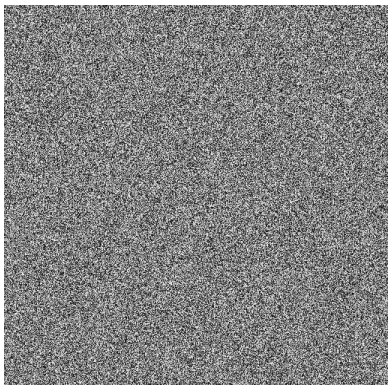
Table 4.18: Comparison of $NPCR$ and $UACI$ values with existing methods

Encryption method	Image	Image size	NPCR	UACI
Cryptosystem-C	Lena	$512 \times 512 \times 1$	99.6452	33.6152
Ref. [11]	Lena	$512 \times 512 \times 1$	99.4602	33.2161
Ref. [131]	Lena	$512 \times 512 \times 1$	99.6307	33.5663
Ref. [45]	Lena	$512 \times 512 \times 1$	99.5705	33.4781
Ref. [146]	Lena	$512 \times 512 \times 1$	99.6052	33.4111
Ref. [20]	Lena	$512 \times 512 \times 1$	99.62	33.46
Ref. [27]	Lena	$512 \times 512 \times 1$	99.6044	33.4841
Ref. [47]	Lena	$512 \times 512 \times 1$	99.607	33.463
Ref. [141]	Lena	$512 \times 512 \times 1$	99.62	33.41
Cryptosystem-C	Lena	$256 \times 256 \times 1$	99.5941	33.5052
Ref. [98]	Lena	$256 \times 256 \times 1$	99.5894	33.4645
Ref. [15]	Lena	$256 \times 256 \times 1$	99.6124	33.4734
Ref. [117]	Lena	$256 \times 256 \times 1$	99.655	33.516
Ref. [81]	Lena	$256 \times 256 \times 1$	99.61	33.46
Ref. [139]	Lena	$256 \times 256 \times 1$	99.61	33.53
Cryptosystem-C	Peppers	$512 \times 512 \times 1$	99.6315	33.5073
Ref. [11]	Peppers	$512 \times 512 \times 1$	99.5643	33.5724
Ref. [131]	Peppers	$512 \times 512 \times 1$	99.6196	33.4530
Ref. [45]	Peppers	$512 \times 512 \times 1$	99.5884	33.5134
Ref. [146]	Peppers	$512 \times 512 \times 1$	99.6052	33.4372
Ref. [20]	Peppers	$512 \times 512 \times 1$	99.62	33.44
Ref. [27]	Peppers	$512 \times 512 \times 1$	99.6391	33.5128
Cryptosystem-C	Peppers	$256 \times 256 \times 1$	99.5849	33.4641
Ref. [10]	Peppers	$256 \times 256 \times 1$	99.593	33.635
Ref. [139]	Peppers	$256 \times 256 \times 1$	99.63	33.58
Cryptosystem-C	Barbara	$256 \times 256 \times 1$	99.6368	33.5152
Ref. [47]	Barbara	$512 \times 512 \times 1$	99.607	33.463
Cryptosystem-C	Baboon	$512 \times 512 \times 1$	99.6154	33.4354
Ref. [27]	Baboon	$512 \times 512 \times 1$	99.6101	33.4354
Cryptosystem-C	Boat	$512 \times 512 \times 1$	99.6284	33.5407
Ref. [11]	Boat	$512 \times 512 \times 1$	99.1025	33.1600
Ref. [131]	Boat	$512 \times 512 \times 1$	99.6128	33.4661
Ref. [66]	Boat	$512 \times 512 \times 1$	99.6154	33.4654
Cryptosystem-C	Boat	$256 \times 256 \times 1$	99.6139	33.4751
Ref. [15]	Boat	$256 \times 256 \times 1$	99.6215	33.3914
Ref. [117]	Boat	$256 \times 256 \times 1$	99.625	33.453
Ref. [47]	Boat	$256 \times 256 \times 1$	99.596	33.448
Cryptosystem-C	Baboon	$256 \times 256 \times 1$	99.6017	33.6287
Ref. [98]	Baboon	$256 \times 256 \times 1$	99.6124	33.4891
Cryptosystem-C	Cameraman	$256 \times 256 \times 1$	99.6215	33.3489
Ref. [98]	Cameraman	$256 \times 256 \times 1$	99.6121	33.4734
Ref. [15]	Cameraman	$256 \times 256 \times 1$	99.6032	33.3954
Ref. [139]	Cameraman	$256 \times 256 \times 1$	99.60	33.53
Cryptosystem-C	Airplane	$256 \times 256 \times 1$	99.6093	33.5133
Ref. [98]	Airplane	$256 \times 256 \times 1$	99.6116	33.4758
Ref. [117]	Airplane	$256 \times 256 \times 1$	99.608	33.574

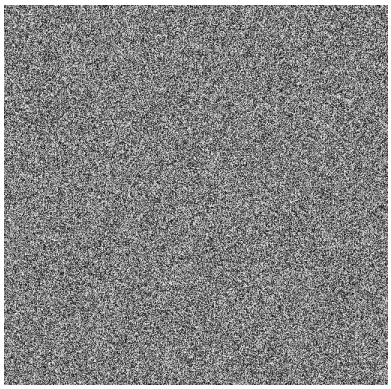
test, for medical grayscale images ($512 \times 512 \times 1$), whereas table 4.20 presents the obtained

experimental values for different standard cipher images, both obtained by applying our proposal (i.e., cryptosystem-C). It should be noticed that a small change is handled for just one key at a time, in the original key set ρ_i, hence, it is obvious that our proposal has enough sensitivity against any change on the secret key.

On the other side, and for demonstrating the degree of sensitivity of the proposed cipher's input (i.e., the used external secret key), and how much of difference can be achieved by its output, after a minor change by unity of one bit flipping (at a Least Significant Bit (LSB)) on its input, the same experiment described in section 4.4.3.2 is carried out for 100 different keys, and the hamming distance for each pair of corresponding cipher images is computed and shown in Figure 4.11 (b). The obtained values are very close to the optimal value of 50%, in which the resultant mean value is 50.0097%, reflecting the robustness of our proposal against any minor change in its secret external key, and thus the avalanche effect is achieved.

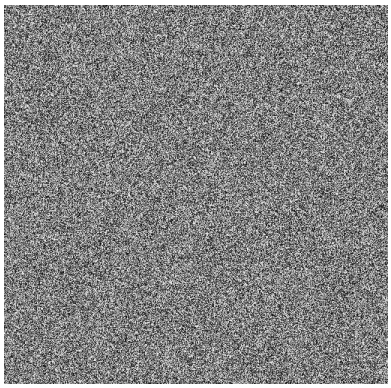


(a) Enciphered with K_1 ($x_0 = 0.53$)



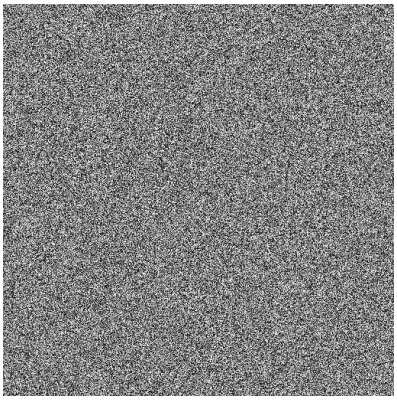
(b) Enciphered with K_2 ($x_0 = x_0 + \Delta\delta$)

(c) Deciphered with correct key

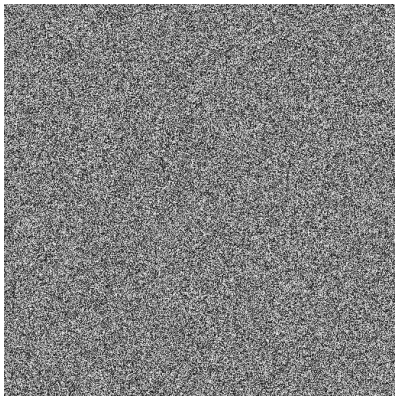


(d) Deciphered with perturbed key)

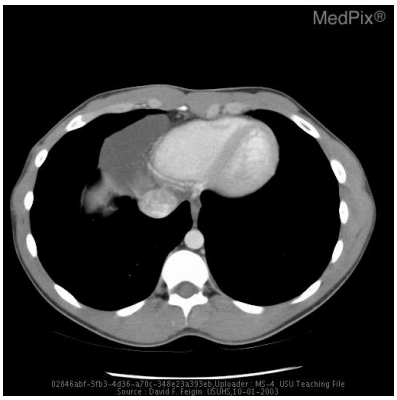
Figure 4.9: Shows the key sensitivity experiment for Lena standard image



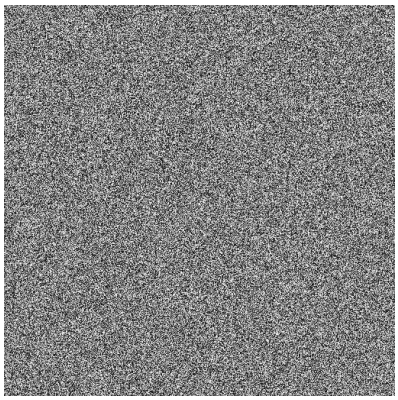
(a) Enciphered with K_1 ($x_0 = 0.53$)



(b) Enciphered with K_2 ($x_0 = x_0 + \Delta\delta$)



(c) Deciphered with correct key



(d) Deciphered with perturbed key)

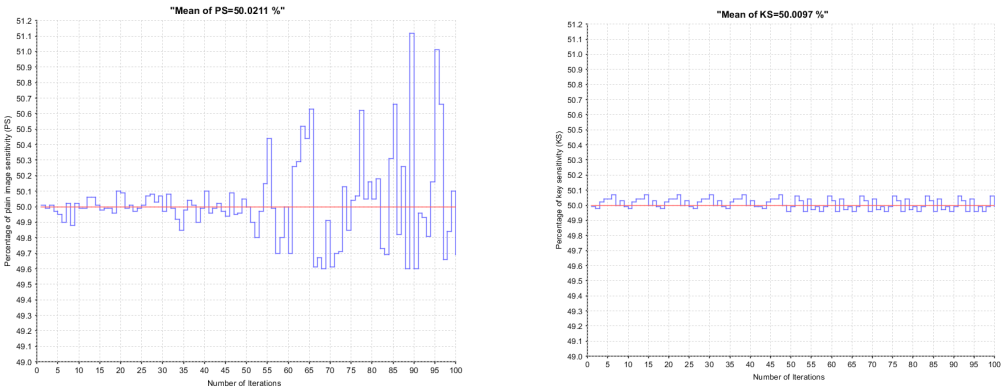
Figure 4.10: Shows the key sensitivity experiment for CT-Abdomen medical image

Table 4.19: Key sensitivity test results for medical images

Test image	Secret keys	Difference rates (%)	
		Encryption	Decryption
CT_Abdomen	ρ_1 ($x'_0 = x_0 + \Delta\delta$)	99.6128	99.6059
CT_Hand		99.6189	99.6185
CT_Head		99.5956	99.6223
CT_Paranasal_sinus		99.6047	99.6192
MR_Brain		99.6231	99.5941
MR_Cervical_Vertibra		99.6055	99.6044
MR_Knee		99.5971	99.6089
X_Chest		99.6372	99.6204
CT_Abdomen	ρ_2 ($x'_0 = x_0 - \Delta\delta$)	99.6009	99.5834
CT_Hand		99.5975	99.5990
CT_Head		99.6170	99.5941
CT_Paranasal_sinus		99.6059	99.6334
MR_Brain		99.6055	99.6318
MR_Cervical_Vertibra		99.6021	99.6204
MR_Knee		99.6173	99.6032
X_Chest		99.6322	99.6170
CT_Abdomen	ρ_3 ($r'_0 = r_0 + \Delta\delta$)	99.6196	99.5910
CT_Hand		99.6238	99.6009
CT_Head		99.6139	99.6109
CT_Paranasal_sinus		99.5971	99.6131
MR_Brain		99.5994	99.6002
MR_Cervical_Vertibra		99.6105	99.6250
MR_Knee		99.5960	99.6074
X_Chest		99.6223	99.6047
CT_Abdomen	ρ_4 ($r'_0 = r_0 - \Delta\delta$)	99.6196	99.6067
CT_Hand		99.6238	99.6131
CT_Head		99.5826	99.6166
CT_Paranasal_sinus		99.6162	99.6246
MR_Brain		99.6044	99.5952
MR_Cervical_Vertibra		99.6093	99.5887
MR_Knee		99.5944	99.6074
X_Chest		99.5948	99.6074

Table 4.20: Key sensitivity test results for standard images

Test image	Secret keys	Difference rates (%)	
		Encryption	Decryption
Lena	ρ_1 ($x'_0 = x_0 + \Delta\delta$)	99.5937	99.5964
Pepper		99.6086	99.5994
Baboon		99.6006	99.6208
Lake		99.6013	99.6196
Boats		99.6131	99.6032
Bridge		99.5899	99.6086
Goldhill		99.6322	99.5937
Barbara		99.6128	99.6040
Lena	ρ_2 ($x'_0 = x_0 - \Delta\delta$)	99.5967	99.6212
Pepper		99.6276	99.5903
Baboon		99.6036	99.5903
Lake		99.5800	99.6025
Boats		99.6170	99.6089
Bridge		99.6006	99.6322
Goldhill		99.6112	99.5922
Barbara		99.6177	99.6025
Lena	ρ_3 ($r'_0 = r_0 + \Delta\delta$)	99.5944	99.6154
Pepper		99.6078	99.6395
Baboon		99.6253	99.6124
Lake		99.6139	99.6185
Boats		99.6070	99.5975
Bridge		99.6166	99.6021
Goldhill		99.6158	99.6109
Barbara		99.6097	99.6112
Lena	ρ_4 ($r'_0 = r_0 - \Delta\delta$)	99.6082	99.6036
Pepper		99.6101	99.5998
Baboon		99.5906	99.6131
Lake		99.6212	99.5807
Boats		99.6192	99.6150
Bridge		99.6128	99.6002
Goldhill		99.5990	99.5971
Barbara		99.6009	99.6181



(a) (b)

Figure 4.11: (a) plain image sensitivity test for a set of random standard and medical images; (b) key sensitivity test for 100 different dynamic key

4.4.4 Performance analysis

4.4.4.1 Computational speed analysis

Time-consuming is also an important factor, with respect to security level. The performance in term of execution time of our proposed cipher algorithm herein cryptosystem-C is tested by means of different test images of different sizes, where the mean value is reported for both encryption and decryption procedures. The experiment is conducted using C compiler, on PC with 3 GHz processor Intel Core i7-2600, with 8Gb, and windows 7, 64-Bit operating system. The algorithm is run under 100 times, and then the average encryption/decryption time is computed for every considered test image. The obtained results of the average encryption/decryption times for different employed cipher images of different sizes are introduced in table 4.21, by applying some existing methods including ours. Regarding the obtained results, it is obvious that our proposed method point to the achieved speed of calculations improvements compared to certain existing methods.

4.4.4.2 Computational complexity analysis

The whole computational complexity of the cipher algorithm herein cryptosystem-C is mainly depended on the permutation module i.e., nonlinear bit-level shuffling and circular-shifting, this latter consumes as a time complexity Θ $(5 \times M \times N)$, whereas only Θ $(M \times N)$ is done by the diffusion module. Moreover, the time-consuming part in the number of floating point operations for the production of chaotic sequences is $\Theta(8 \times M)$ and

Table 4.21: Comparison of the average encryption/decryption time with existing methods

Encryption method	Image size	Type	Execution time (ms)	
			Encryption	Decryption
Cryptosystem-C	$256 \times 256 \times 1$	Chaos	43	46
	$512 \times 512 \times 1$		108	121
	$1024 \times 1024 \times 1$		250	268
Ref. [90]	$256 \times 256 \times 1$	CA	189	Not reported
	$512 \times 512 \times 1$		758	Not reported
	$1024 \times 1024 \times 1$		3097	Not reported
Ref. [148]	$256 \times 256 \times 1$	Chaos	178	Not reported
	$512 \times 512 \times 1$		663	Not reported
	$1024 \times 1024 \times 1$		3141	Not reported
Ref. [71]	$256 \times 256 \times 1$	Chaos	120	Not reported
	$512 \times 512 \times 1$		475	Not reported
	$1024 \times 1024 \times 1$		1951	Not reported
Ref. [137]	$256 \times 256 \times 1$	Chaos	7641	Not reported
	$512 \times 512 \times 1$		34463	Not reported
	$1024 \times 1024 \times 1$		151709	Not reported

$\Theta(3 \times M \times N)$. Hence, the total O-complexity of the proposal can be easily approximated to $\Theta(M \times N)$.

4.5 Conclusion

This chapter discusses the system design and realization of the newly proposed chaotic cipher algorithm for image content preservation, well-suited for both standard and medical images. The proposal herein cryptosystem-C aims to address both the unsuitability problem of existing bit-level proposals for image encryption, where the specific features of medical images in not considered, and the efficiency problem encountered by several image ciphers that have been suggested in the scientific literature. So, a new approach is based on the iterative application of two modules: chaotic confusion and pixel diffusion, and controlled by means of an improved 1D chaotic system (i.e., Logistic Tent System (LTS)), in which its initial conditions are dynamically produced and relied on both the external secret key of 256-bit length and the SHA-256 hash value of the plain image, that lead to generate one-time key-streams, promote the sensitivity to minor alterations applied to plain image, and hence withstand to known/chosen plain image attacks. In the confusion module, a novel nonlinear bit-shuffling and circular shifting technique is handled, to further meet the bit balancing effect, pixel value mixing effect, and certain diffusion mechanism. In the diffusion phase, every confused pixel is diffused by means of an improved XOR operation (eXOR), aiming to elevate the sensitivity to plain image, and accelerate the diffusion mechanism of the whole cipher algorithm. As the diffusion mechanism with respect to pixel level mixing are introduced by the two modules, a good trade-off between computational performance and sufficient security, can be achieved with just one

encryption round. The robustness and effectiveness of the newly proposed chaotic cipher algorithm is assessed against all the commonly considered cryptographic attacks which include: key space attacks, key sensitivity attacks, statistical attacks, differential attacks besides to other security and time performance issues, and a comparison with respect to related existing methods is introduced. Indeed, the extensive analysis and tests have validated the robustness of our method against the commonly known cryptographic attacks, and pointed to the achieved security enhancements and speed of calculation reduction compared to certain existing methods.

Chapter 5

Conclusions and future directions

5.1 Conclusions of this Thesis

The ever-growing demand of secure image storage and transmissions has become more prevalent under the rapid enlargement and development of public networks. Moreover, real-time multimedia applications are also made possible with the advanced progress in communication technologies. This scenario opens challenging problems of how to preserve sensitive information from unauthorized interceptions from a part, and then investigate a secure and efficient cryptographic mean that made a good tradeoff between sufficient level of security and time-consuming, especially in online-communications. So that, whenever a digital image is needed to be used within any communication tools, its content protection turns to be a critical issue.

Along with this thesis the objective has been to advocate the possibility of achieving the needs of a well-designed cryptographic mean through the virtues of dynamical systems (herein cellular automata and chaos).

An overview of this thesis was provided. In this latter, the context of the study was introduced, the bridge between cryptography and the theory of dynamical systems was pointed out, a brief discussion about the theory of CA-based dynamical systems with respect to chaos-based dynamical systems were covered. Then, the motivations of this thesis were introduced, and the main contributions on the navigation issue were reported.

Chapter 1 aimed to give a preliminary knowledge concerning the context of study herein cryptography, and the investigated techniques on which the contributions of this thesis are based, these contributions are supported as possible solutions to the navigation concern. As a latter part, the common and typical security assessment tools that are employed to evaluate the performance of the designed cryptosystems in terms of security level and

time-consuming were covered.

Chapter 2 presented a comprehensive and up-to-date review on image encryption methods based on cellular automata, cellular automata jointly chaos, and chaos dynamical systems. The review also provided a comparative study in terms of the commonly employed cryptographic attacks to break the security of cryptosystems.

It was observed that various existing image encryption methods for image confidentiality preservation, especially based on either chaos or chaos jointly CA, have been broken under known/chosen plaintext attacks [62], by exploiting the low NPCR and UACI values, and mainly the only key-related in the mechanism of key-stream/sub keys production (i.e., there is no incorporation of the plain image features) [13, 67, 69, 107, 147, 149]. Another observed fact is that most of existing proposals are less efficient in term of time-consuming. These security failings were the leading factors behind our contributions within this thesis.

In chapter 3, we designed, implemented and evaluated two proposed contributions in the field of digital image cryptography. The proposals are sufficiently efficient in terms of security degrees and time consuming, under just one encryption round, and hence are best suited for real time applications. The first contribution herein cryptosystem-A proposes for the first time in the literature of CA based cipher design, the application of quadtree decomposition mechanism (QTD) in incorporation with a special class of CA, namely 4^{th} order 1D reversible memory cellular automata (RMCA), and comprises two iterative modules: mixing module and diffusion module. The proposal achieves a good diffusion effect, this latter was exploited to render the system performs a randomized encryption (RE), which leads to its immunity against known/chosen plaintext attacks. The second contribution herein cryptosystem-B is based on chaos in combination with cellular automata (CA), for the sake of benefiting from the strongpoint of the two dynamical system concepts. The proposal consists mainly of two iterative modules: confusion module and diffusion module. A new metric to handle the plain image features is introduced (i.e., weighted histogram (Wh)), this latter together with the external secret key contribute in the mechanism of generating one-time keys employed overall the cryptosystem, and hence ensures its resistance to known/chosen plaintext attacks. Throughout this chapter the mathematical background behind the investigated classes of CA were presented.

In chapter 4, a new chaotic cipher algorithm for efficient and secure image content preservation was introduced, the method is considered faster than the previous proposed cryptosystems with a higher security level reached under just one encryption round. The contribution herein cryptosystem-C consists of two modules which are iteratively performed: chaotic confusion and pixel diffusion, and specializes for both standard and medical images, hence is best suited for real-time teleradiology and other telehealth applications. An im-

proved 1D chaotic system (i.e., Logistic Tent System (LTS)) proposed in [148] is employed in both confusion and diffusion modules, the chaotic behavior of this latter is studied in detail in [148], where excellent chaotic properties are obtained, and the well-known limitations of 1D chaotic systems are overcome, hence, the computational performance of the proposed approach is enhanced by evading the use of higher-dimensional chaotic systems. The dynamical initial conditions of the employed 1D chaotic system are produced by means of the external secret key of 256 bit-length, and the 256-bit long hash value of the plain image, such dependency conducted to random-like generating key-streams, promoted the sensitivity to minor changes of the plain image, and guaranteed the resistance to known/chosen plain image attacks (CPA secure). Throughout this chapter the mathematical background of the work was paved.

A comparative study in terms of security tests and time performance with respect to related existing methods was presented in chapter 3 and chapter 4. Indeed, the reported experimental results are promising and point to the advocacy of the proposed cipher algorithms.

5.2 Future directions

The essential points to be investigated as future directions, and extensions of the research work devoted within this thesis, are:

- A further investigation in the theory of cellular automata is needed. In this regard, the focus will be in exploiting the dynamics of new families of cellular automata. In particularly, reversible memory cellular automata (RMCA) whose state set is F_2^8 instead of F_2 will be the scope.
- A further investigation in the theory of chaos is required. In this regard, new chaotic systems of higher chaoticness will be the scope.
- Instead of applying the encryption process on the whole plain image, partial encryption gives the opportunity to select only the portions of interest to handle the encryption routine. This latter, can significantly reduce the time processing consumed by encryption and decryption routines, while preserving satisfactory level of security. Partial encryption will be the extension of our third contribution (cryptosystem-C), in which only the portions of interest within the medical image will handle the encryption process, aiming to meet real-time medical applications requirements.
- Design and realization of joint encryption-compression cryptosystems.
- Another pivotal concern is to develop cryptographic means that not only get interested by image confidentiality but its authenticity as well (i.e., copyright protection

of digital image). In other words, it is very important to check whether the given image is authentic or has been altered during transmissions over open networks.

Bibliography

[1] AA Abdo, Shiguo Lian, IA Ismail, M Amin, and H Diab. A cryptosystem based on elementary cellular automata. *Communications in Nonlinear Science and Numerical Simulation*, 18(1):136–147, 2013.

[2] Abdel Latif Abu Dalhoum, Basel Ali Mahafzah, Aiman Ayyal Awwad, Ibraheem Aldhamari, Alfonso Ortega, and Manuel Alfonseca. Digital image scrambling using 2d cellular automata. *IEEE Multimedia*, 2012.

[3] Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda. Image encryption by novel cryptosystem using matrix transformation. In *Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on*, pages 77–81. IEEE, 2008.

[4] Andrew Adamatzky, Ramón Alonso-Sanz, Anna T. Lawniczak, Genaro Juárez Martínez, Kenichi Morita, and Thomas Worsch, editors. *Automata 2008: Theory and Applications of Cellular Automata, Bristol, UK, June 12-14, 2008*. Luniver Press, Frome, UK, 2008.

[5] Kathleen T. Alligood, Tim Sauer, and James A. Yorke. *Chaos : an introduction to dynamical systems*. Textbooks in mathematical sciences. Springer, New York, 1996.

[6] Ramón Alonso-Sanz. One-dimensional r= 2 cellular automata with memory. *International Journal of Bifurcation and Chaos*, 14(09):3217–3248, 2004.

[7] Gonzalo Alvarez and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(08):2129–2151, 2006.

[8] David Arroyo, Gonzalo Alvarez, and Veronica Fernandez. A basic framework for the cryptanalysis of digital chaos-based cryptography. In *Systems, Signals and Devices, 2009. SSD'09. 6th International Multi-Conference on*, pages 1–6. IEEE, 2009.

[9] David Arroyo, Rhouma Rhouma, Gonzalo Alvarez, Veronica Fernandez, and Safya Belghith. On the skew tent map as base of a new image chaos-based encryption scheme. In *Second Workshop on Mathematical Cryptology*, pages 113–117, 2008.

[10] Tariq Shah Attaullah. An algorithm based on 1d chaotic system and substitution box (retraction of vol 117, pg 219, 2015). *SIGNAL PROCESSING*, 127:288–288, 2016.

[11] Atieh Bakhshandeh and Ziba Eslami. An authenticated image encryption scheme based on chaotic maps and memory cellular automata. *Optics and Lasers in Engineering*, 51(6):665–673, 2013.

[12] Long Bao, Yicong Zhou, CL Philip Chen, and Hongli Liu. A new chaotic system for image encryption. In *System Science and Engineering (ICSSE), 2012 International Conference on*, pages 69–73. IEEE, 2012.

[13] Rabei Bechikh, Houcemeddine Hermassi, Ahmed A Abd El-Latif, Rhouma Rhouma, and Safya Belghith. Breaking an image encryption scheme based on a spatiotemporal chaotic system. *Signal Processing: Image Communication*, 39:151–158, 2015.

[14] Akram Belazi, Ahmed A Abd El-Latif, and Safya Belghith. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, 128:155–170, 2016.

[15] Akram Belazi, Ahmed A Abd El-Latif, Adrian-Viorel Diaconu, Rhouma Rhouma, and Safya Belghith. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, 88:37–50, 2017.

[16] N. Boccara, E. Goles, S. Martínez, and P. Picco. *Cellular Automata and Cooperative Systems*. Nato Science Series C:. Springer Netherlands, 2012.

[17] Radu Boriga, Ana Cristina Dăscălescu, and Iustin Priescu. A new hyperchaotic map and its application in an image encryption scheme. *Signal Processing: Image Communication*, 29(8):887–901, 2014.

[18] Shahram Etemadi Borujeni and Mohammad Eshghi. Chaotic image encryption system using phase-magnitude transformation and pixel substitution. *Telecommunication Systems*, 52(2):525–537, 2013.

[19] Ünal Çavuşoğlu, Sezgin Kaçar, Ihsan Pehlivan, and Ahmet Zengin. Secure image encryption algorithm design using a novel chaos based s-box. *Chaos, Solitons & Fractals*, 95:92–101, 2017.

[20] Xiuli Chai. An image encryption algorithm based on bit level brownian motion and new chaotic systems. *Multimedia Tools and Applications*, 76(1):1159–1175, 2017.

[21] Xiuli Chai, Zhihua Gan, Kang Yang, Yiran Chen, and Xianxing Liu. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and dna sequence operations. *Signal Processing: Image Communication*, 52:6–19, 2017.

[22] Santosh Chapaneri and Radhika Chapaneri. Chaos based image encryption using latin rectangle scrambling. In *India Conference (INDICON), 2014 Annual IEEE*, pages 1–6. IEEE, 2014.

[23] Santosh Chapaneri, Radhika Chapaneri, and Tanuja Sarode. Evaluation of chaotic map lattice systems for image encryption. In *Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014 International Conference on*, pages 59–64. IEEE, 2014.

[24] Savvas A Chatzichristofis, Dimitris A Mitzias, Georgios Ch Sirakoulis, and Yiannis S Boutalis. A novel cellular automata based technique for visual multimedia content encryption. *Optics Communications*, 283(21):4250–4260, 2010.

[25] S Cheepchol, W San-Um, S Kiattisin, and A Leelasantitham. Digital biometric facial image encryption using chaotic cellular automata for secure image storages. In *Information and Communication Technology, Electronic and Electrical Engineering (JICTEE), 2014 4th Joint International Conference on*, pages 1–5. IEEE, 2014.

[26] Guanrong Chen, Yaobin Mao, and Charles K Chui. A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals*, 21(3):749–761, 2004.

[27] Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Hai Yu, and Li-bo Zhang. An efficient image encryption scheme using gray code based permutation approach. *Optics and Lasers in Engineering*, 67:191–204, 2015.

[28] Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Hai Yu, and Li-bo Zhang. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. *Communications in Nonlinear Science and Numerical Simulation*, 20(3):846–860, 2015.

[29] Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Li-bo Zhang, and Yushu Zhang. An efficient image encryption scheme using lookup table-based confusion and diffusion. *Nonlinear Dynamics*, 81(3):1151–1166, 2015.

[30] Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Li-bo Zhang, and Yushu Zhang. An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. *Communications in Nonlinear Science and Numerical Simulation*, 23(1):294–310, 2015.

[31] Rong-Jian Chen and Jui-Lin Lai. Image security system using recursive cellular automata substitution. *Pattern Recognition*, 40(5):1621–1631, 2007.

[32] Rong-Jian Chen, Yi-Te Lai, and Jui-Lin Lai. Architecture design and vlsi hardware implementation of image encryption/decryption system using re-configurable 2d von neumann cellular automata. In *Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on*, pages 4–pp. IEEE, 2006.

[33] Rong-Jian Chen, Wen-Kai Lu, and Jui-Lin Lai. Image encryption using progressive cellular automata substitution and scan. In *Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on*, pages 1690–1693. IEEE, 2005.

[34] Tinghuan Chen, Meng Zhang, Jianhui Wu, Chau Yuen, and You Tong. Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling. *Optics & Laser Technology*, 84:118–133, 2016.

[35] Abdel Latif Abu Dalhoum, Alia Madain, and Hazem Hiary. Digital image scrambling based on elementary cellular automata. *Multimedia Tools and Applications*, 75(24):17019–17034, 2016.

[36] Debasis Das. A survey on cellular automata and its applications. In *Global trends in computing and communication systems*, pages 753–762. Springer, 2012.

[37] Debasis Das. A survey on cellular automata and its applications. In *Global trends in computing and communication systems*, pages 753–762. Springer, 2012.

[38] Debasis Das and Abhishek Ray. A parallel encryption algorithm for block ciphers based on reversible programmable cellular automata. *arXiv preprint arXiv:1006.2822*, 2010.

[39] A Martín del Rey, JL Hernández Pastora, and G Rodríguez Sánchez. 3d medical data security protection. *Expert Systems with Applications*, 54:379–386, 2016.

[40] Ángel Martín del Rey. A protocol to provide assurance of images integrity using memory cellular automata. In *Cellular Automata, 7th International Conference on Cellular Automata, for Research and Industry, ACRI 2006, Perpignan, France, September 20-23, 2006, Proceedings*, pages 627–635. Springer, 2006.

[41] Ángel Martín del Rey, Gerardo Rodríguez Sánchez, and A. de la Villa Cuenca. A protocol to cipher digital images based on cat maps and cellular automata. In *Pattern Recognition and Image Analysis, Third Iberian Conference, IbPRIA 2007, Girona, Spain, June 6-8, 2007, Proceedings, Part I*, pages 571–578. Springer, 2007.

[42] Ángel Martín del Rey, Gerardo Rodríguez Sánchez, and A. de la Villa Cuenca. Encrypting digital images using cellular automata. In *Hybrid Artificial Intelligent Systems - 7th International Conference, HAIS 2012, Salamanca, Spain, March 28-30th, 2012. Proceedings, Part II*, pages 78–88. Springer, 2012.

[43] Ángel Martín del Rey, Gerardo Rodríguez Sánchez, and A. de la Villa Cuenca. A protocol to encrypt digital images using chaotic maps and memory cellular automata. *Logic Journal of the IGPL*, 23(3):485–494, 2015.

[44] Robert L. Devaney. *An introduction to chaotic dynamical systems.* Advanced book program. Addison-Wesley, Reading (Mass.), 1989. 9e impression, aot 1995.

[45] Adrian-Viorel Diaconu. Circular inter–intra pixels bit-level permutation and chaos-based image encryption. *Information Sciences*, 355:314–327, 2016.

[46] Manoj Diwakar, Pratibha Sharma, Sandip Swarnakar, and Pardeep Kumar. Image security using cellular automata rules. In *Proceedings of the Third International Conference on Soft Computing for Problem Solving*, pages 403–412. Springer, 2014.

[47] Safwan El Assad and Mousa Farajallah. A new chaos-based image encryption system. *Signal Processing: Image Communication*, 41:144–157, 2016.

[48] Safwan El Assad and Hassan Noura. Generator of chaotic sequences and corresponding generating system, July 15 2014. US Patent 8,781,116.

[49] Rasul Enayatifar, Hossein Javedani Sadaei, Abdul Hanan Abdullah, Malrey Lee, and Ismail Fauzi Isnin. A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. *Optics and Lasers in Engineering*, 71:33–41, 2015.

[50] Kamel Mohamed Faraoun. Design of fast one-pass authenticated and randomized encryption schema using reversible cellular automata. *Communications in Nonlinear Science and Numerical Simulation*, 19(9):3136–3148, 2014.

[51] Michael François, Thomas Grosges, Dominique Barchiesi, and Robert Erra. Image encryption algorithm based on a chaotic iterative process. *Applied Mathematics*, 3:1910–1920, 2012.

[52] Michael François, Thomas Grosges, Dominique Barchiesi, and Robert Erra. A new image encryption scheme based on a chaotic function. *Signal Processing: Image Communication*, 27(3):249–259, 2012.

[53] Edward Fredkin. An informational process based on reversible universal cellular automata. *Physica D: Nonlinear Phenomena*, 45(1-3):254–270, 1990.

[54] Jiri Fridrich. Image encryption based on chaotic maps. In *Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on*, volume 2, pages 1105–1110. IEEE, 1997.

[55] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, 8(06):1259–1284, 1998.

[56] Chong Fu, Wen-Jing Li, Zhao-Yu Meng, Tao Wang, and Pei-Xuan Li. A symmetric image encryption scheme using chaotic baker map and lorenz system. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on*, pages 724–728. IEEE, 2013.

[57] Chong Fu, Wei-hong Meng, Yong-feng Zhan, Zhi-liang Zhu, Francis CM Lau, K Tse Chi, and Hong-feng Ma. An efficient and secure medical image protection scheme based on chaotic maps. *Computers in biology and medicine*, 43(8):1000–1010, 2013.

[58] Tiegang Gao and Zengqiang Chen. A new image encryption algorithm based on hyper-chaos. *Physics Letters A*, 372(4):394–400, 2008.

[59] Jesus D Terrazas Gonzalez and Witold Kinsner. A modular dynamical cryptosystem based on continuous cellular automata. In *Cognitive Informatics & Cognitive Computing (ICCI* CC), 2011 10th IEEE International Conference on*, pages 203–215. IEEE, 2011.

[60] Jesus D Terrazas Gonzalez and Witold Kinsner. Comparison of cryptosystems using a single-scale statistical measure. In *Electrical and Computer Engineering (CCECE), 2013 26th Annual IEEE Canadian Conference on*, pages 1–5. IEEE, 2013.

[61] Djamal Eddine Goumidi and Fella Hachouf. Hybrid chaos-based image encryption approach using block and stream ciphers. In *Systems, Signal Processing and their Applications (WoSSPA), 2013 8th International Workshop on*, pages 139–144. IEEE, 2013.

[62] Ramzi Guesmi, Mohamed Amine Ben Farah, Abdennaceur Kachouri, and Mounir Samet. Hash key-based image encryption using crossover operator and chaos. *Multimedia tools and applications*, 75(8):4753–4769, 2016.

[63] Maryam Habibipour, Mehdi Yaghobi, Saeed Rahati-Q, et al. An image encryption system by indefinite cellular automata and chaos. In *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*, volume 3, pages V3–23. IEEE, 2010.

[64] Seyed Alireza Hosseini and Seyed Reza Kamel. Fast encryption of rgb color digital images based on elementary cellular automata using three processors. In *Technology, Communication and Knowledge (ICTCK), 2015 International Congress on*, pages 241–246. IEEE, 2015.

[65] Seyed Alireza Hosseini, Iman Mohammadi, and Seyed Reza Kamel. A parallel image encryption based on elementary cellular automata using two processors. In *Technology, Communication and Knowledge (ICTCK), 2014 International Congress on*, pages 1–5. IEEE, 2014.

[66] Zhongyun Hua and Yicong Zhou. Image encryption using 2d logistic-adjusted-sine map. *Information Sciences*, 339:237–253, 2016.

[67] Fuh-Gwo Jeng, Wei-Lun Huang, and Tzung-Her Chen. Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes. *Signal Processing: Image Communication*, 34:45–51, 2015.

[68] Jun Jin. An image encryption based on elementary cellular automata. *Optics and Lasers in Engineering*, 50(12):1836–1843, 2012.

[69] Saeideh Kabirirad and Hamideh Hajiabadi. Cryptanalysis of an authenticated image encryption scheme based on chaotic maps and memory cellular automata. *IACR Cryptology ePrint Archive*, 2015:326, 2015.

[70] D. Kahn. *The Codebreakers: The Story of Secret Writing*. Signet book. New American Library, 1973.

[71] A Kanso and M Ghebleh. A novel image encryption algorithm based on a 3d chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 17(7):2943–2959, 2012.

[72] Jonathan Katz and Yehuda Lindell. Introduction to modern cryptography. *AMC*, 10:12, 2006.

[73] Jan Sher Khan, Atique ur Rehman, Jawad Ahmad, and Zeeshan Habib. A new chaos-based secure image encryption scheme using multiple substitution boxes. In *Information Assurance and Cyber Security (CIACS), 2015 Conference on*, pages 16–21. IEEE, 2015.

[74] Lars Knudsen and Matthew Robshaw. *The block cipher companion*. Information security and cryptography. Springer, Heidelberg, London, 2011. AU@.

[75] Ljupco Kocarev. Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*, 1(3):6–21, 2001.

[76] Ljupco Kocarev and Shiguo Lian, editors. *Chaos-Based Cryptography - Theory, Algorithms and Applications*, volume 354 of *Studies in Computational Intelligence*. Springer, 2011.

[77] Manish Kumar, Sunil Kumar, Rajat Budhiraja, MK Das, and Sanjeev Singh. Intertwining logistic map and cellular automata based color image encryption model. In *Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on*, pages 618–623. IEEE, 2016.

[78] Y. Kuznetsov. *Elements of Applied Bifurcation Theory*, volume 112 of *Applied Mathematical Sciences*. Springer New York, 2004.

[79] Xiao Wei Li, Sung Jin Cho, and Seok Tae Kim. A 3d image encryption technique using computer-generated integral imaging and cellular automata transform. *Optik-International Journal for Light and Electron Optics*, 125(13):2983–2990, 2014.

[80] XW Li, DH Kim, SJ Cho, and ST Kim. Integral imaging based 3-d image encryption algorithm combined with cellular automata. *Journal of applied research and technology*, 11(4):549–558, 2013.

[81] Yueping Li, Chunhua Wang, and Hua Chen. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*, 90:238–246, 2017.

[82] Zhongqin Li and Zongwang Lv. A method for image encryption based on high dimensional chaotic system. In *Measurement, Information and Control (ICMIC), 2013 International Conference on*, volume 2, pages 1302–1306. IEEE, 2013.

[83] Shiguo Lian, Jinsheng Sun, and Zhiquan Wang. Security analysis of a chaos-based image encryption algorithm. *Physica A: Statistical Mechanics and its Applications*, 351(2):645–661, 2005.

[84] Hongjun Liu and Xingyuan Wang. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. *Journal of Systems and Software*, 86(3):826–834, 2013.

[85] Edward N Lorenz. Deterministic nonperiodic flow. *Journal of the atmospheric sciences*, 20(2):130–141, 1963.

[86] Bruno Martin. Damage spreading and μ-sensitivity on cellular automata. In *IFIP International Conference on Theoretical Computer Science*, pages 226–241. Springer, 2000.

[87] James L Massey. Cryptography: Fundamentals and applications. In *Copies of transparencies, Advanced Technology Seminars*, volume 109, page 119, 1993.

[88] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications. CRC Press, 1996.

[89] Omid Mirzaei, Mahdi Yaghoobi, and Hassan Irani. A new image encryption method: parallel sub-image encryption with hyper chaos. *Nonlinear Dynamics*, 67(1):557–566, 2012.

[90] Faraoun Kamel Mohamed. A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science and Technology, an International Journal*, 17(2):85–94, 2014.

[91] A. Moonis, P. Chung, and C. Hinde. *Developments in Applied Artificial Intelligence: 16th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems, IEA/AIE 2003, Laughborough, UK, June 23-26, 2003, Proceedings*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2003.

[92] Rinaldi Munir. Security analysis of selective image encryption algorithm based on chaos and cbc-like mode. In *Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on*, pages 142–146. IEEE, 2012.

[93] MA Murillo-Escobar, F Abundiz-Pérez, C Cruz-Hernández, and RM López-Gutiérrez. A novel symmetric text encryption algorithm based on logistic map. In *Proceedings of the International Conference on Communications, Signal Processing and Computers (ICNC14)*, 2014.

[94] MA Murillo-Escobar, César Cruz-Hernández, F Abundiz-Pérez, RM López-Gutiérrez, and OR Acosta Del Campo. A rgb image encryption algorithm based on total plain image characteristics and chaos. *Signal Processing*, 109:119–131, 2015.

[95] Abolfazl Yaghouti Niyat, Reza Mohammad Hei Hei, and Majid Vafaei Jahan. Chaos-based image encryption using a hybrid cellular automata and a dna sequence. In *Technology, Communication and Knowledge (ICTCK), 2015 International Congress on*, pages 247–252. IEEE, 2015.

[96] Abolfazl Yaghouti Niyat, Mohammad Hossein Moattar, and Masood Niazi Torshiz. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Optics and Lasers in Engineering*, 90:225–237, 2017.

[97] Jean De Dieu Nkapkop, Joseph Yves Effa, Andrei Toma, Florentina Cociota, and Monica Borda. Chaos-based image encryption using the rsa keys management for an efficient web communication. In *Electronics and Telecommunications (ISETC), 2016 12th IEEE International Symposium on*, pages 59–62. IEEE, 2016.

[98] Benyamin Norouzi, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, and Mohammad Reza Mosavi. A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. *Multimedia Tools and Applications*, 74(3):781–811, 2015.

[99] Narendra K Pareek, Vinod Patidar, and Krishan K Sud. Diffusion–substitution based gray image encryption scheme. *Digital signal processing*, 23(3):894–901, 2013.

[100] Fabio Pareschi, Riccardo Rovatti, and Gianluca Setti. On statistical tests for randomness included in the nist sp800-22 test suite and based on the binomial distribution. *IEEE Transactions on Information Forensics and Security*, 7(2):491–505, 2012.

[101] Carmen Pellicer-Lostao and Ricardo Lopez-Ruiz. Notions of chaotic cryptography: Sketch of a chaos based cryptosystem. *arXiv preprint arXiv:1203.4134*, 2012.

[102] Chuan Peng and Yuanxiang Li. A new algorithm for image encryption based on couple chaotic system and cellular automata. In *Mechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 International Conference on*, pages 1645–1648. IEEE, 2013.

[103] Jun Peng, Shangzhu Jin, Liang Lei, and Qi Han. Research on a novel image encryption algorithm based on the hybrid of chaotic maps and dna encoding. In *Cognitive Informatics & Cognitive Computing (ICCI* CC), 2013 12th IEEE International Conference on*, pages 403–408. IEEE, 2013.

[104] Ahmed G Radwan, Sherif H AbdElHaleem, and Salwa K Abd-El-Hafiz. Symmetric encryption algorithms using chaotic and non-chaotic generators: a review. *Journal of advanced research*, 7(2):193–208, 2016.

[105] Amitesh Singh Rajput, Nishchol Mishra, and Sanjeev Sharma. Towards the growth of image encryption and authentication schemes. In *Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference On*, pages 454–459. IEEE, 2013.

[106] Iman Ranaee, Mahdi Majidi Nia, Reza Jahantigh, and Amirhossein Gharib. Introducing a new algorithm for medical image encryption based on chaotic feature of cellular automata. In *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*, pages 582–587. IEEE, 2013.

[107] Rhouma Rhouma and Safya Belghith. Cryptanalysis of a new image encryption algorithm based on hyper-chaos. *Physics Letters A*, 372(38):5973–5978, 2008.

[108] Andrius Rickus, Eckhard Pfluegel, and Nigel Atkins. Chaos-based image encryption using an aont mode of operation. In *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on*, pages 1–5. IEEE, 2015.

[109] Jörg Rothe. *Complexity Theory and Cryptology. An Introduction to Cryptocomplexity.* Texts in Theoretical Computer Science. An EATCS Series. Springer, 2005.

[110] Andrew Rukhin, Juan Soto, James Nechvatal, Elaine Barker, Stefan Leigh, Mark Levenson, David Banks, Alan Heckert, James Dray, San Vo, et al. Statistical test suite for random and pseudorandom number generators for cryptographic applications, nist special publication. 2010.

[111] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C.* Wiley, 1996.

[112] Claude E Shannon. Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4):656–715, 1949.

[113] Claude Elwood Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

[114] SIMON SINGH. *The code book : the science of secrecy from ancient Egypt to quantum cryptography.* NEW YORK : ANCHOR BOOKS, 2000.

[115] Ercan Solak, Cahit Çokal, Olcay Taner Yildiz, and TÜRKER BIYIKOĞLU. Cryptanalysis of fridrich's chaotic image encryption. *International Journal of Bifurcation and Chaos*, 20(05):1405–1413, 2010.

[116] Sukalyan Som and Atanu Kotal. Confusion and diffusion of grayscale images using multiple chaotic maps. In *Computing and Communication Systems (NCCCS), 2012 National Conference on*, pages 1–5. IEEE, 2012.

[117] Chun-Yan Song, Yu-Long Qiao, and Xing-Zhou Zhang. An image encryption scheme based on new spatiotemporal chaos. *Optik-International Journal for Light and Electron Optics*, 124(18):3329–3334, 2013.

[118] Amina Souyah and Kamel Mohamed Faraoun. Fast and efficient randomized encryption scheme for digital images based on quadtree decomposition and reversible memory cellular automata. *Nonlinear Dynamics*, 84(2):715–732, 2016.

[119] Amina Souyah and Kamel Mohamed Faraoun. An image encryption scheme combining chaos-memory cellular automata and weighted histogram. *Nonlinear Dynamics*, 86(1):639–653, 2016.

[120] Amina Souyah and Kamel Mohamed Faraoun. A review on different image encryption approaches. In *Modelling and Implementation of Complex Systems*, pages 3–18. Springer, 2016.

[121] Ahmad Pahlavan Tafti and Safoura Janosepah. Digital images encryption in frequency domain based on dct and one dimensional cellular automata. In *International Conference on Informatics Engineering and Information Science*, pages 421–427. Springer, 2011.

[122] M Tahghighi, S Turaev, R Mahmod, A Jafaar, and M Md Said. The cryptanalysis and extension of the generalized golden cryptography. In *Open Systems (ICOS), 2011 IEEE Conference on*, pages 65–68. IEEE, 2011.

[123] Tommaso Toffoli and Norman H Margolus. Invertible cellular automata: A review. *Physica D: Nonlinear Phenomena*, 45(1-3):229–253, 1990.

[124] Cesar Torres-Huitzil. Hardware realization of a lightweight 2d cellular automata-based cipher for image encryption. In *Circuits and Systems (LASCAS), 2013 IEEE Fourth Latin American Symposium on*, pages 1–4. IEEE, 2013.

[125] Selman Uguz, Hasan Akin, Irfan Siap, and Ugur Sahin. On the irreversibility of moore cellular automata over the ternary field and image application. *Applied Mathematical Modelling*, 40(17):8017–8032, 2016.

[126] John R. Vacca and John R. Vacca. *Computer and Information Security Handbook, Second Edition*. Morgan Kaufmann Publishers Inc., 2nd edition, 2013.

[127] Henk C.A. van Tilborg. *Fundamentals of cryptology : a professional reference and interactive tutorial*. Kluwer international series in engineering and computer science. Kluwer Academic Publ., Boston, Dordrecht, London, 2000.

[128] John Von Neumann, Arthur W Burks, et al. Theory of self-reproducing automata. *IEEE Transactions on Neural Networks*, 5(1):3–14, 1966.

[129] Xingyuan Wang, Chuanming Liu, Dahai Xu, and Chongxin Liu. Image encryption scheme using chaos and simulated annealing algorithm. *Nonlinear Dynamics*, 84(3):1417–1429, 2016.

[130] Xingyuan Wang and Dapeng Luan. A novel image encryption algorithm using chaos and reversible cellular automata. *Communications in Nonlinear Science and Numerical Simulation*, 18(11):3075–3085, 2013.

[131] Xingyuan Wang and Dahai Xu. A novel image encryption scheme using chaos and langtons ant cellular automaton. *Nonlinear Dynamics*, 79(4):2449–2456, 2015.

[132] Xingyuan Wang and Hui-li Zhang. A color image encryption with heterogeneous bit-permutation and correlated chaos. *Optics Communications*, 342:51–60, 2015.

[133] Stephen Wolfram. Cryptography with cellular automata. In *Advances in Cryptology*, CRYPTO '85, pages 429–432. Springer-Verlag, 1986.

[134] Stephen Wolfram. *A new kind of science*. Wolfram Media, 2002.

[135] Kwok-Wo Wong. Image encryption using chaotic maps. In *Intelligent Computing Based on Chaos*, pages 333–354. Springer, 2009.

[136] Yue Wu, Joseph P Noonan, and Sos Agaian. Npcr and uaci randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, pages 31–38, 2011.

[137] Yue Wu, Gelan Yang, Huixia Jin, and Joseph P Noonan. Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging*, 21(1):013014–1, 2012.

[138] Yue Wu, Yicong Zhou, George Saveriades, Sos Agaian, Joseph P Noonan, and Premkumar Natarajan. Local shannon entropy measure with statistical tests for image randomness. *Information Sciences*, 222:323–342, 2013.

[139] Lu Xu, Xu Gou, Zhi Li, and Jian Li. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Optics and Lasers in Engineering*, 91:41–52, 2017.

[140] Yu-Guang Yang, Ju Tian, He Lei, Yi-Hua Zhou, and Wei-Min Shi. Novel quantum image encryption using one-dimensional quantum cellular automata. *Information Sciences*, 345:257–270, 2016.

[141] Erdem Yavuz, Rifat Yazıcı, Mustafa Cem Kasapbaşı, and Ezgi Yamaç. A chaos-based image encryption algorithm with simple logical functions. *Computers & Electrical Engineering*, 54:471–483, 2016.

[142] JKMS Zaman and Ranjan Ghosh. Review on fifteen statistical tests proposed by nist. *J. Theoretical Physics and Cryptography*, 1:18–31, 2012.

[143] Samaneh Zamani, Mahdi Javanmard, Nima Jafarzadeh, and Mostafa Zamani. A novel image encryption scheme based on hyper chaotic systems and fuzzy cellular automata. In *Electrical Engineering (ICEE), 2014 22nd Iranian Conference on*, pages 1136–1141. IEEE, 2014.

[144] Ebrahim Zarei Zefreh, Sara Rajaee, and Meysam Farivary. Image security system using recursive cellular automata substitution and its parallelization. In *Computer Science and Software Engineering (CSSE), 2011 CSI International Symposium on*, pages 77–86. IEEE, 2011.

[145] Wei Zhang, Kwok-wo Wong, Hai Yu, and Zhi-liang Zhu. A symmetric color image encryption algorithm using the intrinsic features of bit distributions. *Communications in Nonlinear Science and Numerical Simulation*, 18(3):584–600, 2013.

[146] Xuanping Zhang and Zhongmeng Zhao. Chaos-based image encryption with total shuffling and bidirectional diffusion. *Nonlinear Dynamics*, 75(1-2):319–330, 2014.

[147] Ying-Qian Zhang and Xing-Yuan Wang. Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. *Nonlinear Dynamics*, 77(3):687–698, 2014.

[148] Yicong Zhou, Long Bao, and CL Philip Chen. A new 1d chaotic system for image encryption. *Signal processing*, 97:172–182, 2014.

[149] Congxu Zhu, Siyuan Xu, Yuping Hu, and Kehui Sun. Breaking a novel image encryption scheme based on brownian motion and pwlcm chaotic system. *Nonlinear Dynamics*, 79(2):1511–1518, 2015.

[150] Hegui Zhu, Xiaojun Lu, Qingsong Tang, Xiangde Zhang, and Cheng Zhao. A new chaos-based image encryption scheme using quadratic residue. In *Systems and Informatics (ICSAI), 2012 International Conference on*, pages 1800–1804. IEEE, 2012.

[151] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong, and Hai Yu. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*, 181(6):1171–1186, 2011.