REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supèrieur et de la Recherche Scientifique

جامعة فرحات عباس سطيف

Ferhat ABBAS University of Setif

Université Ferhat Abbas Sétif 1

Faculté de Technologie

Département d'Elecrtonique

Implémentation et développement d'algorithmes avancés dédiés à la sécurité et à l'identification

---

Thèse présentée par : **Imane KOUADRA**

En vue de l'obtention du diplôme de Doctorat 3ème cycle LMD en *Reseaux de Telecommunications*

Soutenue devant le jury composé de :

Pr. Naceur-eddine BOUKEZZOULA	Université Ferhat Abbas Sétif 1	Président
Pr.Lahcene ZIET	Université Ferhat Abbas Sétif 1	Directeur
Pr.Tewfik BEKKOUCHE	Université Bachir El-ibrahimi BBA	Co-directeur
Pr. Abd-elhak hamida FERHAT	Université Ferhat Abbas Sétif 1	Examinateur
Pr. Ammar SOUKKOU	Université M.S. Benyahia Jijel	Examinateur
Pr. Riadh REMOUCHE	Université M.S. Benyahia Jijel	Examinateur
Pr. Walid EL-SHAFAI	Université Prince Soultane KSA	Invité

2024 / 2025

PEOPLES' DEMOCRATIC REPUBLIC OF ALGERIA

Ministry of Higher Education and Scientific Research

Ferhat Abbas University of Setif

Faculty of Technology

Department of Elictronics

Implementation and Development of Advanced Algorithms Dedicated to Security and Identification

---

Thesis presented by: **Imane KOUADRA**

As a requirement to aim for the degree of 3^{rd} cycle Doctorate in *Telecommunications Networks*

Approved by the supervisory committee :

Prof. Naceur-eddine BOUKEZZOULA	Ferhat Abbas University, Sétif 1	President
Prof. Lahcene ZIET	Ferhat Abbas University, Sétif 1	Supervisor
Prof. Tewfik BEKKOUCHE	Bachir El-Ibrahimi University, BBA	Co-supervisor
Prof. Abd-elhak Hamida FERHAT	Ferhat Abbas University, Sétif 1	Examiner
Prof. Ammar SOUKKOU	M.S. Benyahia University, Jijel	Examiner
Prof. Riadh REMOUCHE	M.S. Benyahia University, Jijel	Examiner
Prof. Walid EL-SHAFAI	Prince Sultan University, KSA	Invited

2024 / 2025

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ:

يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ،
وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ.

سورة المجادلة: ١١

Declaration

I, Imane KOUADRA, declare that this dissertation titled "Implementation and Development of Advanced Algorithms Dedicated to Security and Identification" of Ferhat Abbas University; I confirm that:

- The date supplied in the dissertation, together with the material and documents, has been acquired in accordance with academic and ethical standards.
- All material, documentation, assessments, and findings adhere to scientific ethics and morality.
- I have provided references for all publications used in this dissertation.
- I use the data acquired from the tests without alteration or modification.
- I affirm that the work provided in this dissertation is original.

I accept that any rights and advantages granted by this dissertation may be revoked if any aspects of the claims mentioned above are shown to be untrue.

Signed :

Date : 04/10/2025

Dedications

I dedicate this work **To my beloved parents**. Your love, sacrifices, and unwavering support have been the foundation of my journey. May Allah reward you for every prayer and every effort.

وَوَصَّيْنَا ٱلْإِنسَـٰن بِوَٰلِدَيْهِ حَمَلَتْهُ أُمُّهُ وَهْنًا عَلَىٰ وَهْنٍ وَفِصَـٰلُهُ فِى عَامَيْنِ أَنِ ٱشْكُرْ لِى وَلِوَٰلِدَيْكَ إِلَىَّ ٱلْمَصِيرُ.

Surah Luqman, 14

To my dear sisters and brothers. You are my lifelong companions and my first friends. Thank you for always standing by me through hardships and joys.

وَاجْعَل لِّي وَزِيرًا مِّنْ أَهْلِي، هَارُونَ أَخِي، ٱشْدُدْ بِهِ أَزْرِي، وَأَشْرِكْهُ فِي أَمْرِي.

Surah Al-Hujurat, 29-32

To my cherished friends: Irsel, Imane, Ines, and Abderrahim. Your friendship, kindness, and support have been among the greatest blessings in my life.

ٱلْأَخِلَّآءُ يَوْمَئِذٍ بَعْضُهُمْ لِبَعْضٍ عَدُوٌّ إِلَّا ٱلْمُتَّقِينَ.

Surah Az-Zukhruf, 67

To all my professors in the Electronics Department. Thank you for your dedication, patience, and the knowledge you have imparted. Your efforts have been a source of inspiration.

قُلْ هَلْ يَسْتَوِى ٱلَّذِينَ يَعْلَمُونَ وَ ٱلَّذِينَ لَا يَعْلَمُونَ إِنَّمَا يَتَذَكَّرُ أُولُوا ٱلْأَلْبَـٰب.

Surah Az-Zumar, 9

To everyone I've met in my life or known, whether through good or bad experiences, I am genuinely thankful and wish you all the best.

يَا أَيُّهَا النَّاسُ إِنَّا خَلَقْنَاكُم مِّن ذَكَرٍ وَأُنثَىٰ وَجَعَلْنَـٰكُمْ شُعُوبًا وَقَبَآئِلَ لِتَعَارَفُوٓا إِنَّ أَكْرَمَكُمْ عِندَ ٱللَّهِ أَتْقَىٰكُمْ إِنَّ ٱللَّهَ عَلِيمٌ خَبِيرٌ

Surah Al-Hujurat, 13

Imane Kouadra

Acknowledgments

All praise is due to Almighty **ALLAH**, who facilitated the successful completion of this assignment.

ٱلْحَمْدُ لِلَّهِ رَبِّ ٱلْعَٰلَمِينَ.

I would like to express my deepest gratitude to my supervisor **and** co-supervisor, **Professors: Lahcene ZIET, Tewfik BEKKOUCHE**, for their tremendous academic support. I appreciate all their time and advice to make my research experience substantial and efficient. Thank you so much for your dedication, guidance, and valuable contributions.
I also would like to express my heartfelt appreciation for the thoughtful feedback and constructive criticism the **Jury Committee professors:** Pr. Naceur-eddine BOUKEZZOULA Président , Pr. Abd-elhak hamida FERHAT Pr. Ammar SOUKKOU, Pr. Riadh REMOUCHE Examiners provided. I am very grateful for the opportunity to present my research to such a distinguished panel of experts and for your unwavering support throughout the process.

Additionally, I am deeply grateful to Professor **Walid El-Shafai** at Sultan University in Saudi Arabia, who has consistently provided insightful feedback, scholarly expertise, and encouragement that have greatly enriched my research. His commitment to academic excellence and his mentorship have not only shaped my work but have also inspired me to strive for a deeper understanding of the subject. This work wouldn't have reached its current form without his profound influence and contributions.

Lastly, I would like to express my heartfelt gratitude to my dear **Family**, **Friends**, and **Colleagues**. Your love and unwavering support. Thank you for always being there for me, through thick and thin. You are the most valuable thing in my life.

Imane Kouadra

04/10/2025

Abstract

This doctoral thesis focuses on the development and implementation of advanced chaotic algorithms to enhance information security and identification systems. Using the inherent unpredictability of chaotic systems, the research proposes novel algorithmic models tailored for robust data encryption, particularly in the context of digital and biomedical imaging. A central contribution is the Improved Composite Chaotic Map (ICCM), a dynamic model that integrates classical quadratic and cubic chaotic behaviors, augmented by an additional control parameter to expand the keyspace and enhance flexibility. The chaotic properties of the ICCM are validated through Lyapunov exponent analysis and bifurcation diagrams, achieving a Lyapunov exponent of 21.42, which surpasses that of previous models. Incorporated into a hybrid optodigital image encryption scheme, ICCM demonstrates strong resistance to statistical, differential, and brute-force attacks. Its effectiveness is measured using performance metrics such as a high mean square error ($MSE > 10$), low correlation coefficients ($Cr < 0.0001 - 0.0028$), and a low peak signal-to-noise ratio ($PSNR < 10dB$), confirming its ability to obscure and protect sensitive data. In addition to general data encryption, the thesis addresses medical image security through a customized Pre-processing encryption-decryption technique for retinal images. This method utilizes dual chaotic sequences derived from the logistic map and integrates biometric information, such as fingerprints, to generate dynamic encryption keys. Comprehensive testing, including histogram analysis, sensitivity analysis, PSNR, and correlation evaluation, confirms the method's ability to maintain image integrity while ensuring privacy and resistance to common cryptographic attacks.

In general, this work contributes significantly to the field of chaos-based cryptography by introducing adaptable and secure encryption mechanisms suitable for general-purpose and domain-specific applications. It also paves the way for further innovations in data protection and biometric security.

Keywords: image processing, Biometric-based encryption, Chaotic systems, Information security, composite chaotic map.

Résumé

Cette thèse de doctorat porte sur le développement et la mise en œuvre d'algorithmes chaotiques avancés visant à renforcer la sécurité de l'information et les systèmes d'identification. En exploitant l'imprévisibilité inhérente des systèmes chaotiques, cette recherche propose de nouveaux modèles algorithmiques adaptés à un chiffrement robuste des données, notamment dans les domaines de l'imagerie numérique et biomédicale. L'apport central de ce travail est la carte chaotique composite améliorée (ICCM), un modèle dynamique intégrant les comportements chaotiques quadratiques et cubiques classiques, enrichi par un paramètre de contrôle supplémentaire permettant d'élargir l'espace de clés et d'améliorer la flexibilité. Les propriétés dynamiques de l'ICCM sont validées à travers l'analyse des exposants de Lyapunov et des diagrammes de bifurcation, avec un exposant atteignant 21,42, surpassant les modèles antérieurs. Intégré dans un schéma hybride de chiffrement opto-numérique, l'ICCM montre une forte résistance aux attaques statistiques, différentielles et par force brute. Son efficacité est confirmée par des indicateurs tels qu'une erreur quadratique moyenne élevée (MSE $>$ 10), des coefficients de corrélation faibles (Cr 0.0001–0.0028), et un rapport signal sur bruit de crête bas (PSNR $<$ 10 dB). Par ailleurs, la thèse propose un procédé de prétraitement de chiffrement-déchiffrement adapté à la protection des images rétiniennes. Cette méthode utilise deux séquences chaotiques dérivées de la carte logistique, combinées à des données biométriques (empreintes digitales) pour générer des clés dynamiques. Les tests approfondis confirment la robustesse de ce système à préserver l'intégrité des images tout en assurant leur confidentialité face aux attaques cryptographiques. Ce travail apporte ainsi une contribution notable à la cryptographie chaotique, en introduisant des mécanismes de sécurité adaptables, applicables aussi bien aux systèmes généraux qu'aux domaines spécialisés comme la biométrie médicale.

Mots-clés : Traitement d'image, Chiffrement biométrique, Systèmes chaotiques, Sécurité de l'information, Carte chaotique composite.

الملخص

تركز هذه الأطروحة على تطوير وتنفيذ خوارزميات فوضوية متقدمة تهدف إلى تعزيز أمن المعلومات وأنظمة التحقق منتركز هذه الأطروحة على تطوير وتنفيذ خوارزميات فوضوية متقدمة تهدف إلى تعزيز أمن المعلومات وأنظمة التحقق من الهوية. وبالاعتماد على الطبيعة غير المتوقعة والحساسة للأنظمة الفوضوية، تقترح هذه الدراسة نماذج خوارزمية جديدة مصممة لتحقيق تشفير قوي للبيانات، مع تركيز خاص على الصور الرقمية والطبية الحيوية. ومن أبرز المساهمات في هذا العمل تطوير خريطة فوضوية مركبة محسّنة (ICCM) ، وهي نموذج ديناميكي يدمج السلوك الفوضوي الكلاسيكي من النوع التربيعي والتكعيبي، مع إضافة معامل تحكم جديد يوسّع مجال المفاتيح ويزيد من مرونة الخوارزم. تمت المصادقة على الخصائص الديناميكية لـ ICCM من خلال تحليل مؤشرات ليابونوف ومخططات التفرع، حيث بلغ مؤش ليابونوف 21.42 ، متفوقًا على النماذج السابقة. وعند دمجه في نظام تشفير بصريرقمي هجين، أثبت النموذج مقاومته الكبيرة للهجمات الإحصائية والتفاضلية وهجمات القوة الغاشمة. وتم تقييم أدائه باستخدام مؤشرات مثل متوسط الخطأ التربيعي العالي ($MSE > 10$) ، ومعاملات الارتباط المنخفضة (Cr 0.0001–0.0028) ، ونسبة الإشارة إلى الضوضاء المنخفضة ($PSNR < 10$ dB) . إلى جانب التشفير العام للبيانات، تقدم الأطروحة أيضًا طريقة مبتكرة لمعالجة التشفير وفك التشفير مصممة خصيصًا لحماية صور شبكية العين. وتعتمد هذه الطريقة على توليد مفاتيح ديناميكية باستخدام سلسلتين فوضويتين مستخرجتين من خريطة لوغستية، مع تضمين بيانات حيوية مثل بصمات الأصابع. وتؤكد التحاليل التجريبية والإحصائية فعالية هذا النظام في الحفاظ على سلامة الصور الطبية وضمان الخصوصية والحماية من الهجمات.

الكلمات المفتاحية: معالجة الصور، التشفير القائم على البيانات البيومترية، الأنظمة الفوضوية، أمن المعلومات، الخريطة الفوضوية المركبة.

Scientific Productions

Journal Papers

- Imane Kouadra, Tewfik Bekkouche, Lahcene Ziet, Imane Mehidi, Samah Alshathri, Walid El-Shafai. *"New Composite Chaotic Map Applied To An Image Encryption Scheme in Cybersecurity Applications."*
  IEEE Access, 2025. https://doi.org/10.1109/ACCESS.2025.3558948.

Conference Proceedings

Scopus Indexed Conferences

- Imane Kouadra, Imane Mehidi, Lahcene Ziet, Tewfik Bekkouche, Ines Hammou. *"Chaotic Retinal Image Encryption Pre-processing Based on Biometric Key."* In 2024 International Conference on Electrical Engineering and Control Applications (ICEEAC). IEEE, May 2024. https://doi.org/10.1109/ICEEAC61226.2024.10576302.

Non-Indexed Conferences

- Imane Kouadra, Ines Hammou, Tewfik Bekkouche, Lahcene Ziet. *"A Comparative Study of Chaotic Map and Nonlinear Post-Processing Approaches Applied to Image Encryption."* 1st National Conference on Emergent Technologies in Electrical Engineering (NCETEE'23), Sétif, Algeria, December 2023.

- Imane Kouadra, Imane Mehidi, Lahcene Ziet. *"Chaotic Encryption-Based Multi Biometric Recognition through an Improved Nonlinear Function."* 4th National Conference of Mathematics and Applications (CNMA–2024), Mila, Algeria, December 2024.

Contents

List of Figures

List of Tables

List of abbreviations

A

AES Advanced Encryption Standard

AFIS Automatic Fingerprint Identification System

AI Artificial Intelligence

ANN Artificial Neural Network

AMD Age-related Macular Degeneration

B

BLH Bowler-Hat

BTH Bottom-Hat

C

CLAHE Contrast Limited Adaptive Histogram Equalization

CPU Central Processing Unit

CNN Convolutional Neural Network

CVD Circular Vessel Ratio

Cr Correlation Coefficient

D

DES Data Encryption Standard

DR Diabetic Retinopathy

DRIVE Digital Retinal Image for Vessel Extraction

DRPE Double Random Phase Encoding

F

FN False Negative

FOV Field Of View

FCM Fuzzy C-Means

FRFT Fractional Fourier Transform

FP False Positive

G

GPU Graphics Processing Unit

GT Ground Truth

H

HRF High-Resolution Fundus

HMAC Hash-Based Message Authentication Code

HTTPS HyperText Transfer Protocol Secure

I

ICA Independent Component Analysis

ICCM Improved Composite Chaotic Map

IoT Internet of Things

J

JPEG Joint Photographic Experts Group image format

K

KNN K-Nearest Neighbors

L

LBP Local Binary Patterns

LLBP Local Line Binary Patterns

M

MAC Message Authentication Code

MATLAB MATrix LABoratory

MCC Matthews Correlation Coefficient

MF Matched Filter

MSE Mean Square Error

MRI Magnetic Resonance Imaging

N

NIR Near-Infrared

NIST National Institute of Standards and Technology

O

OD Optic Disc

P

PBBM Pattern-Based Binary Mapping

PCA Principal Component Analysis

PHI Personal Health Information

PMM Portable Pixmap Format

PSNR Peak Signal-to-Noise Ratio

Q

QR Quick Response

R

RGB Red, Green and Blue

ROI Region Of Interest

RSA Rivest–Shamir–Adleman Algorithm

S

SSFCA Spatially Smooth Fuzzy C-Means Algorithm

STARE Structured Analysis of the Retina

SHA Secure Hash Algorithm

Se Sensitivity

Sp Specificity

SVM Support Vector Machine

T

TN True Negative

TP True Positive

V

VPN Virtual Private Network

General introduction

In the modern digital landscape, the protection of information and identity has become an increasingly critical concern. With the proliferation of connected devices, cloud services, and biometric applications, securing data is not merely a technical challenge but a fundamental necessity in safeguarding personal privacy, national security, and institutional integrity. From encrypted communication in banking systems to biometric access in healthcare and surveillance, the demand for intelligent and adaptive security models continues to escalate.

Traditional cryptographic techniques such as RSA, AES, and DES, although robust in many domains, are increasingly vulnerable to evolving threats. These methods rely heavily on computational complexity, making them susceptible to brute-force attacks as processing power increases, especially with the emergence of quantum computing paradigms. Consequently, the field of cryptography has seen a paradigm shift toward more nonlinear, dynamic, and biologically inspired approaches. One such promising direction is chaos-based cryptography, a discipline that exploits the mathematical properties of chaotic systems to develop more secure encryption algorithms [1, 2].

Chaotic systems are inherently deterministic yet appear random due to their extreme sensitivity to initial conditions and system parameters. This sensitivity, known as the "butterfly effect," makes them particularly suitable for encryption tasks where unpredictability and sensitivity to key changes are essential [3]. Chaotic maps such as the logistic map, Henon map, tent map, and cubic maps have been employed in various encryption algorithms due to their ability to generate pseudorandom sequences that are hard to predict or reproduce without exact initial conditions. These features not only increase the entropy of the encrypted data but also reinforce resistance to statistical and differential attacks.

This thesis builds upon this foundation by proposing a more powerful chaotic construct: the Improved Composite Chaotic Map (ICCM). Unlike single chaotic maps, which often exhibit limited chaotic range or degeneracy at certain parameters, the ICCM fuses quadratic and cubic behaviors into a composite structure. A tunable control parameter is introduced to adjust the complexity and span of the chaotic domain dynamically. This innovation significantly expands the encryption keyspace, ensuring higher sensitivity and security [4]. To rigorously validate the chaotic behavior of ICCM, techniques such as Lyapunov exponent analysis and bifurcation diagrams are employed. The system achieves a Lyapunov exponent of 21.42, exceeding benchmarks from prior works and confirming its

enhanced chaotic dynamics.

The cryptographic potential of the ICCM is realized through its integration into an opto-digital image encryption system. Images are particularly vulnerable to various forms of cryptanalysis due to their high redundancy and pixel correlation. To counter these vulnerabilities, the thesis leverages Double Random Phase Encoding (DRPE) and the Fractional Fourier Transform (FrFT), two powerful optical tools that introduce multi-domain transformation and complex phase masking into the encryption process. The resulting encryption scheme shows a substantial improvement in resilience against common attacks. Empirical evaluations report high Mean Square Error (MSE $> 10^4$), low Peak Signal-to-Noise Ratio (PSNR < 10 dB), and correlation coefficients close to zero, all of which indicate the robustness of the approach [5, 6].

Beyond general-purpose encryption, this thesis places special emphasis on biometric image security, with a focus on retinal image encryption. Biometric data, while providing a convenient method of authentication, also presents unique challenges in terms of privacy, irrevocability, and data integrity. Retinal and fingerprint images, in particular, are highly sensitive and must be protected during storage and transmission. The proposed method incorporates biometric information such as the original fingerprint to generate dynamic, user-specific keys. These keys are then utilized to seed chaotic sequences in a dual chaotic encryption framework, enhancing the randomness and binding the encryption process to the individual identity [7].

This hybrid approach, which combines biometric-based key generation, chaos theory, and optical transforms, addresses several critical aspects of secure identification. First, it ensures that the encryption is non-reversible without biometric validation, reinforcing access control. Second, it introduces temporal and user-specific variability, preventing replay or substitution attacks. Third, the system is designed to resist chosen-plaintext and known-plaintext attacks, which are common in biometric applications. This comprehensive security makes this approach ideal for protecting medical images, national identification systems, border control, and other high-stakes identification applications [8].

To validate the effectiveness of the system, standard datasets such as DRIVE and STARE are used to test encryption performance on retinal images. A full suite of cryptographic evaluations is applied, including entropy analysis, histogram uniformity, key sensitivity, noise attack tolerance, and the NIST statistical test suite. Results confirm that the proposed scheme not only achieves high security standards but also maintains the structural integrity and clinical usability of the encrypted images—an essential feature in medical contexts [9].

Furthermore, this thesis aligns with global trends in privacy-preserving computing, where data must remain encrypted not only in transit and at rest, but also during processing. Techniques such as homomorphic encryption, federated learning, and zero-knowledge proofs share a common goal with this work: securing data without compro-

mising its utility. The proposed models complement these broader security frameworks by offering high-speed, lightweight encryption systems suitable for real-time applications, particularly in edge computing and Internet of Things (IoT) environments [10].

In summary, this research aims to bridge theoretical cryptographic innovation with practical deployment in biometric and medical security. By introducing an enhanced chaotic model (ICCM), integrating it with optical transformations (FrFT, DRPE), and anchoring the encryption process in biometric identity, the work delivers a comprehensive security solution. As cybersecurity threats grow in scale and sophistication, these adaptable, user-specific, and chaos-driven methods provide a promising path forward in protecting personal identity and sensitive data across sectors.

Contributions

This dissertation lies at the intersection of chaotic cryptography, biometric security, and advanced image encryption. It addresses current cybersecurity challenges by developing novel mathematical models and applying them in real-world scenarios, especially in the medical imaging and biometric identification domains. The work is structured around two main contributions, each supported by published or submitted research articles and conference presentations.

Dissertation outline

All the chapters in this dissertation are based on our peer-reviewed publications and submitted articles. Together, they form a coherent and cumulative body of work, advancing the design and implementation of chaotic systems for cryptographic applications and biometric identification. The structure of the dissertation mirrors the chronological and thematic progression of these contributions.

First Part: Theoretical Foundations and Framework

Chapter 1: Entitled "State of the Art in Information Security", this chapter provides a comprehensive overview of fundamental principles and modern challenges in digital security. It introduces the key concepts of confidentiality, integrity, authentication, and availability, and discusses the limitations of classical cryptographic methods in the face of emerging technologies. The chapter also explores the evolution of information security frameworks and the rise of biometric and chaos-based approaches as alternatives to traditional encryption systems.

Chapter 2: Entitled "Cryptographic and Biometric Security Systems", this chapter delves into the theoretical underpinnings of modern cryptographic mechanisms, including symmetric and asymmetric encryption, hash functions, and hybrid systems. It further analyses the growing role of biometric traits, such as fingerprints, retinal patterns, and voiceprints, in secure identification systems. The chapter also lays the mathematical foundation for chaotic systems and their application in cryptography, highlighting the relevance of nonlinear dynamics, sensitivity to initial conditions, and pseudo-random behaviour in secure key generation.

Second Part: Original Contributions

Chapter 3: Titled "Chaotic Retinal Image Encryption Pre-processing Based on Biometric Key", this chapter presents the first contribution of the thesis. It proposes a novel encryption-decryption scheme tailored for protecting retinal images using a dual chaotic system seeded by biometric fingerprint data. The approach binds encryption keys to individual identity, enhancing both privacy and authentication. The system is evaluated using standard retinal image datasets and demonstrates high performance across security metrics such as PSNR, MSE, entropy, and correlation analysis. This work addresses the critical need for secure medical data storage and transmission in healthcare applications.

Chapter 4: Titled "New Composite Chaotic Map Applied to an Image Encryption Scheme in Cybersecurity Applications", this chapter presents the second contribution of the dissertation. It introduces the Improved Composite Chaotic Map (ICCM), a new chaotic model combining quadratic and cubic behaviors with an adjustable control parameter. The ICCM is embedded into a hybrid opto-digital encryption system that uses Double Random Phase Encoding (DRPE) and the Fractional Fourier Transform (FrFT). Experimental validation confirms the method's high security level, key sensitivity, and resistance to statistical and differential attacks, positioning it as a strong candidate for modern cyber-protection systems.

Framework

Chapter 1

State of the Art in Information Security

1.1 Introduction

In an era of escalating cyber threats, the protection of digital assets has become a critical priority for governments, corporations, and individuals alike. The continuous expansion of interconnected systems, the proliferation of smart devices, and the increasing reliance on digital services have significantly elevated the importance of robust information security frameworks [11]. As adversaries become more sophisticated, so too must the mechanisms designed to safeguard data confidentiality, integrity, and availability.

This chapter provides a comprehensive overview of the foundational and emerging approaches in information security. It begins by examining classical cryptographic systems, which form the backbone of secure digital communication. These systems are broadly categorized into three types: symmetric encryption, which relies on a shared secret key; asymmetric encryption, which uses a mathematically linked public-private key pair; and hybrid encryption, which combines the efficiency of symmetric methods with the security of asymmetric systems [12].

Following this, the chapter addresses the limitations of traditional encryption methods when applied to non-textual data, particularly digital images. Image encryption has become essential in various applications, including telemedicine, surveillance, cloud storage, and remote sensing. Conventional cryptographic algorithms struggle with large file sizes and high redundancy in images. Therefore, specialized methods such as pixel permutation, diffusion techniques, and chaos-based encryption are explored for their capacity to obscure image structure and enhance security [13].

A key innovation discussed in this chapter is the application of **chaotic systems** in encryption. These systems leverage properties such as sensitivity to initial conditions, nonlinearity, and pseudo-randomness to provide a high level of unpredictability in the encrypted output. Their lightweight computational cost and resistance to brute-force

attacks make them especially attractive for image and multimedia data protection [14].

In addition to cryptographic techniques, this chapter explores **biometric security systems**, which authenticate users based on physiological and behavioral traits, including fingerprints, facial features, iris patterns, voice, and gait. Biometric authentication offers several advantages over traditional methods, including enhanced user convenience and a reduced risk of identity theft. However, it also introduces challenges related to spoofing attacks, sensor variability, and privacy concerns [15].

To mitigate these challenges, the chapter also reviews advanced countermeasures such as liveness detection, template protection, and multimodal biometric systems, as well as future trends involving artificial intelligence, edge computing, and blockchain-based identity management [16].

1.2 overview of classical cryptographic systems

Cryptography, the art and science of securing information, has evolved significantly from its classical roots to the sophisticated algorithms that underpin modern digital security [11]. Initially developed to protect military and diplomatic communications, early cryptographic methods, now known as classical cryptographic systems, employed ingenious yet straightforward techniques such as substitution and transposition to obscure messages from unauthorized readers. These foundational methods not only ensured secrecy in their time but also introduced core concepts that continue to shape the discipline today.

In the modern context, cryptography has expanded to two principal paradigms: symmetric and asymmetric cryptosystems [17]. Although both aim to ensure data confidentiality, integrity, and authenticity, they rely on fundamentally different mechanisms: symmetric systems use a shared secret key for both encryption and decryption. In contrast, asymmetric systems operate on a mathematically linked public-private key pair . Understanding the theoretical and practical distinctions of these models is crucial for analyzing contemporary security protocols and designing cryptographic solutions that address diverse application requirements in an increasingly interconnected digital landscape.

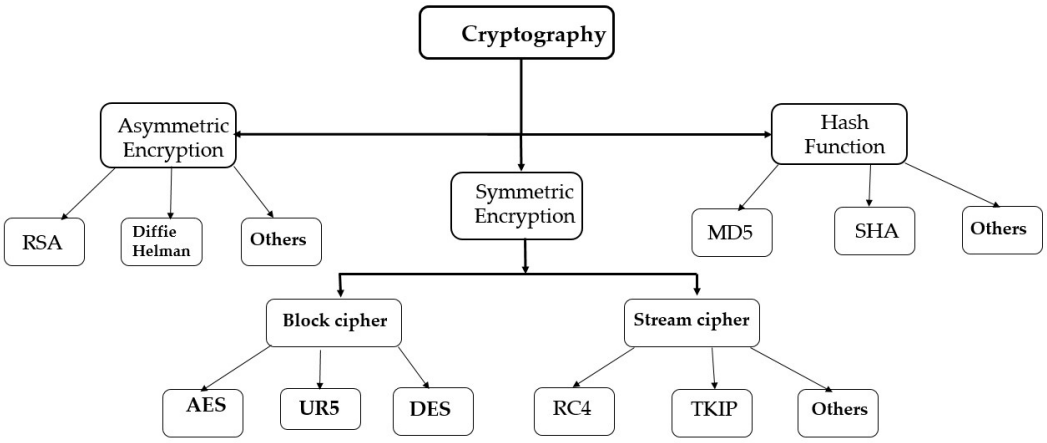


Figure 1.1: Basic Classification of Cryptography [12].

1.2.1 Asymmetric encryption

Asymmetric key cryptographic systems utilize two distinct keys: a public key, which is made available to anyone, and a private key, which remains confidential. The core principle behind this system is that the public key is used for encryption, while the private key is used for decryption. The two keys are mathematically related, meaning that data encrypted with the public key can only be decrypted by the corresponding private key [18]. This relationship is fundamental to the security of asymmetric cryptography, as it ensures that even if an attacker intercepts the public key, they can not decrypt the data without the private key. Asymmetric encryption offers a higher level of security compared to symmetric encryption.

Additionally, asymmetric encryption requires more computational power, leading to increased CPU utilization. Therefore, although asymmetric encryption is ideal for securely exchanging encryption keys or establishing trust between parties, it is often used in conjunction with symmetric encryption. In practice, asymmetric encryption is first used to exchange a symmetric key, which is then used for encrypting and decrypting the bulk of the data [19]. This hybrid approach leverages the security of asymmetric encryption for key exchange, while maintaining the efficiency of symmetric encryption for the data encryption process.

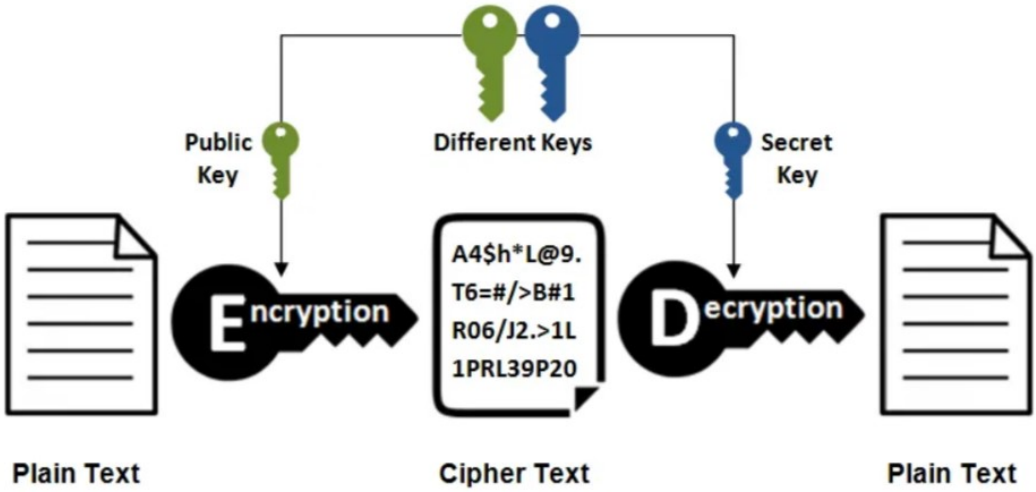


Figure 1.2: Asymmetric encryption scheme [19].

1.2.2 Symmetric encryption

Symmetric encryption is widely used for securing communications. Symmetric encryption is a cryptographic technique that uses the same secret key for both encryption and decryption of data. This means that both the sender and receiver must have access to the key, which must be securely exchanged to avoid unauthorised access[12]. The key is kept private between the two parties, and because it is shared, the method is often referred to as private key encryption. Symmetric encryption algorithms can be divided into two types:

- **Block Cryptosystems**: These algorithms encrypt data in fixed-size blocks. For example, the block might consist of 64 bits or 128 bits. In block cipher systems, the data is split into blocks, and each block is processed separately [20], meaning that even if one block of data is encrypted, the encryption process will remain consistent across other blocks.
- **Stream Cryptosystems**: Stream cyphers encrypt data in a Real-time bit stream. Each bit or byte of data is encrypted one at a time [21], making stream cyphers faster and better suited for encrypting real-time data, such as streaming video or audio.

Its main challenge lies in the secure sharing of the key between communicating parties to ensure that unauthorised entities cannot intercept or misuse it.

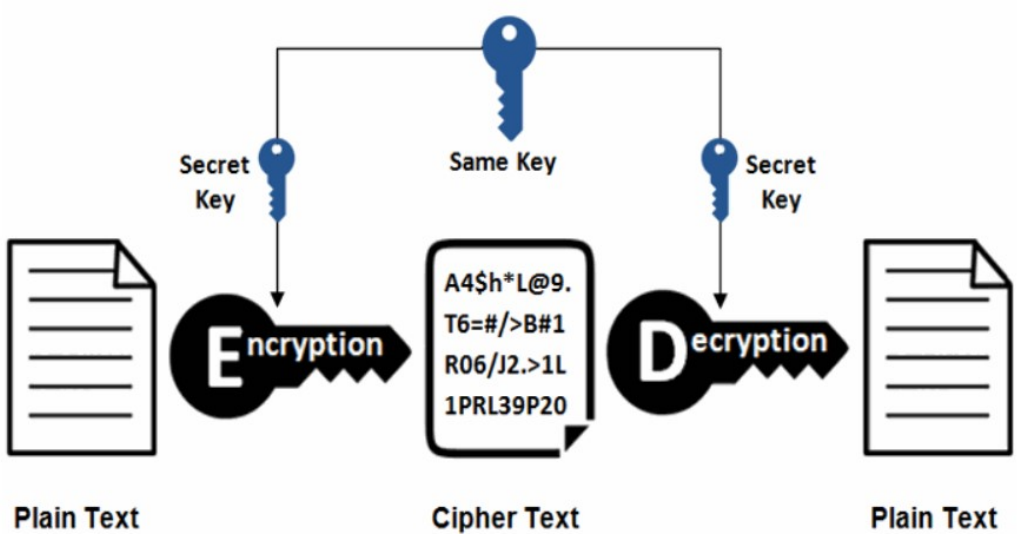


Figure 1.3: Symmetric encryption scheme [12].

1.2.3 hybrid encryption systems

A hybrid encryption system integrates both symmetric and asymmetric cryptographic techniques to capitalise on their respective advantages while mitigating their weaknesses. In such a system, the encryption process begins with the generation of a random symmetric key, often referred to as a session key. This key is used to encrypt the actual data using a symmetric algorithm, such as AES, which is computationally efficient and well-suited for handling large data volumes [22]. To ensure the secure transmission of the session key itself, it is encrypted using the recipient's public key via an asymmetric algorithm, such as RSA. Upon receiving the encrypted package, the recipient first uses their private key to decrypt the session key and then employs that symmetric key to decrypt the main data [23]. This combination allows hybrid systems to deliver both high-speed performance and strong security. Asymmetric encryption ensures a secure exchange of keys without prior sharing, while symmetric encryption offers the speed necessary for encrypting substantial datasets. This approach is widely adopted in modern communication protocols. A comparative summary of the characteristics of symmetric, asymmetric, and hybrid encryption systems is presented in Table 1.1.

Table 1.1: Extended Comparison of Symmetric, Asymmetric, and Hybrid Encryption

Feature	**Symmetric Encryption**	**Asymmetric Encryption**	**Hybrid Encryption**
Speed	Very fast, efficient for bulk data	Slower due to complex math operations	Fast for data, asymmetric part used only for key exchange
Security	Depends on secure key exchange	Strong security via public/private keys	Combines both for balanced security
Scalability	Poor (each pair needs a unique key)	Better suited for large systems	More scalable through asymmetric key distribution
Key Size	Short (128 or 256 bits)	Long (2048 bits or more)	Utilizes both types of keys
Complexity	Simple implementation	High computational complexity	Moderate, combines both algorithms
Use Cases	Encrypting files, disk storage	Digital signatures, certificates	Secure messaging, HTTPS, VPNs
Confidentiality & Integrity	Requires additional mechanisms (MAC)	Built-in through key pairs	Provides both effectively
Processing Overhead	Low resource usage	High CPU/memory consumption	Moderate, efficient for practical use

1.2.4 Hashing encryption

Cryptography serves as a cornerstone of secure data exchange in modern communication systems. Within this framework, **hash functions** play a critical role in preserving data integrity through irreversible mathematical operations. These algorithms efficiently convert variable-length input data into unique fixed-length outputs, enabling verification of unaltered content. Prominent examples include MD5 (128-bit digest), SHA-1, SHA-2, and SHA-3 [24], each offering distinct security properties.

While hashing effectively identifies accidental data corruption, it lacks robustness against intentional tampering by malicious actors, as demonstrated by vulnerabilities to man-in-the-middle attacks. Cryptographic systems often integrate keyed-hash message authentication codes (HMACs) to address this gap [25]. HMAC augments traditional hashing by requiring a shared secret key during hash generation, enabling both integrity validation and source authentication, a dual-layer safeguard against unauthorised modifications.

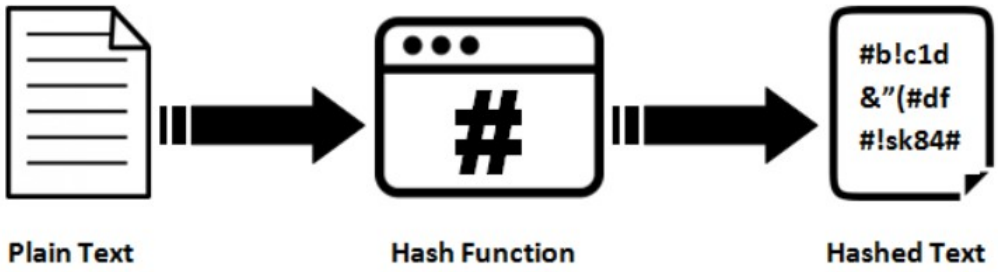


Figure 1.4: Cryptographic hash function [24].

1.3 Image Encryption Techniques

As the demand for secure visual communication grows, traditional cryptographic methods have proven insufficient to address the unique challenges posed by image data. Images differ from textual data in terms of size, redundancy, and pixel correlation, requiring specialized encryption techniques tailored to their structure. Image encryption techniques are designed to obscure the visual content by transforming it into an unintelligible form, ensuring that unauthorized users cannot access or interpret the information [13]. These techniques are crucial in applications such as medical imaging, military surveillance, cloud storage, and digital forensics, where image confidentiality and integrity are critical. This section explores the most common strategies used in image encryption, including pixel permutation, diffusion, and chaos-based systems, each offering distinct advantages in terms of security, efficiency, and adaptability [26].

1.3.1 Importance of Image Encryption

In the digital era, images constitute a substantial portion of transmitted and stored data across a wide range of domains, including healthcare, military surveillance, remote sensing, social media, and confidential communications. Unlike text data, images often contain rich, sensitive, and high-dimensional information that, if compromised, can lead to significant breaches of privacy and security. For instance, medical images, such as MRI or CT scans, carry personal health information (PHI) protected under strict regulations, like HIPAA, while satellite or drone-captured imagery may involve classified geopolitical data. Ensuring the confidentiality and integrity of such images is paramount, necessitating robust encryption techniques tailored to the unique characteristics of image data [27]. As these images are increasingly transmitted over open or untrusted networks, their protection becomes paramount. Conventional cryptographic algorithms, although effective for textual data, are often inadequate for images due to their larger size, high redundancy, and real-time processing demands [28]. Image encryption techniques are thus essential to ensure **confidentiality**, **integrity**, and **non-repudiation** of visual data during storage

and transmission. Moreover, as artificial intelligence and computer vision systems become more prevalent in automated decision-making, the risk of adversarial manipulation or data leakage further amplifies the need for robust image encryption protocols. Ensuring the security of images not only preserves privacy but also fosters trust in digital services and infrastructure that depend on visual data.

1.3.1.1 Confidentiality

Confidentiality refers to the assurance that visual data is accessible only to authorised parties and remains hidden from unauthorised users or adversaries. In the context of image encryption, confidentiality ensures that sensitive information embedded in an image, such as personal identities, health data, or classified intelligence, is protected from interception, surveillance, or theft during transmission and storage [29]. This is particularly vital in domains like telemedicine, where patient scans are shared over networks, or in military reconnaissance, where satellite imagery can reveal strategic assets. Image encryption achieves confidentiality by transforming the image into an unintelligible format using cryptographic algorithms, so that even if the data is intercepted, it remains unreadable without the proper decryption key. Advanced techniques such as chaos-based encryption, pixel shuffling, and bit-level scrambling are widely used to enhance the confidentiality of images by making statistical analysis and brute-force attacks infeasible [30].

1.3.1.2 Integrity

integrity in image encryption ensures that the image data remains unchanged during transmission or storage; that is, the receiver must be able to confirm that the encrypted image has not been tampered with, corrupted, or modified in any way. In practical terms, integrity safeguards both the authenticity of the content and the accuracy of the decryption output. Techniques such as cryptographic hash functions and digital signatures are commonly employed to detect any unauthorized alterations [31]. Recent advancements have introduced hybrid models that combine encryption with integrity verification mechanisms, enhancing the robustness of image security systems [32]. These methods are particularly vital in sensitive applications, such as medical imaging and military communications, where the accuracy and trustworthiness of visual data are paramount [29]. Any alteration, even a single bit, could render an encrypted image undecipherable or misleading, particularly in high-stakes applications such as forensic analysis, medical diagnostics, or the processing of legal evidence. Cryptographic hash functions and digital signatures are often integrated with image encryption schemes to verify integrity [33]. Furthermore, secure protocols may embed metadata or watermarking techniques to trace the origin and validate the legitimacy of image files. Preserving integrity is not only a technical necessity but also a crucial factor in ensuring trust and reliability in systems that heavily

rely on encrypted visual data.

1.3.1.3 Non-repudiation

Non-repudiation ensures that a sender cannot deny the authenticity of a transmitted image, and that the recipient can verify the origin of an image. This security principle is essential in legal, forensic, and governmental communications [34], where image evidence may be used to hold individuals or organizations accountable. In encrypted image systems, non-repudiation is typically enforced through digital signatures, which bind a unique cryptographic identity to the image data. When a user encrypts and signs an image using a private key, any recipient can verify its authenticity using the corresponding public key [35]. This mechanism prevents malicious users from claiming that an image was forged or altered post-distribution. Combined with audit trails and timestamping, non-repudiation strengthens accountability and traceability in image-sharing networks, making it a key pillar in secure visual data exchange protocols.

1.3.2 Existing Strategies in Image Encryption

To address the unique requirements of image encryption, researchers have developed a range of techniques explicitly tailored to image characteristics such as high data redundancy, pixel correlation, and large file sizes [36]. Unlike traditional encryption algorithms designed for textual data, image-specific strategies focus on disrupting the inherent patterns in visual data while maintaining computational efficiency [37]. Among the most widely adopted techniques are pixel permutation, diffusion, and encryption based on chaotic systems.

1.3.2.1 Pixel Permutation

Pixel permutation involves rearranging the positions of pixels within the image to obscure the original structure. This method reduces the correlation between adjacent pixels, a key statistical weakness in unencrypted images, without altering their values. The strength of permutation lies in its simplicity and speed; however, permutation alone is insufficient to provide strong security, especially against statistical or known-plaintext attacks. For this reason, permutation is often used as the first stage in more complex hybrid encryption frameworks [38]. The figure shows a 4×4 matrix before and after pixel permutation, demonstrating how the position of the elements is rearranged to obscure the original structure.

1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

13	10	11	2
14	16	5	9
15	3	1	6
7	8	4	12

Figure 1.5: 4×4 matrix before and after permutation.

1.3.2.2 Diffusion Techniques

Diffusion techniques aim to modify the actual pixel values by distributing small changes evenly across the image. A single-pixel modification in the plaintext image should ideally affect a vast area in the encrypted version, making it harder for attackers to infer original data [39]. In typical implementations, pixel values are modified using operations such as XOR, modular arithmetic, or substitution based on a chaotic key stream [40]. When combined with permutation, diffusion significantly increases the entropy and visual randomness of the encrypted image.

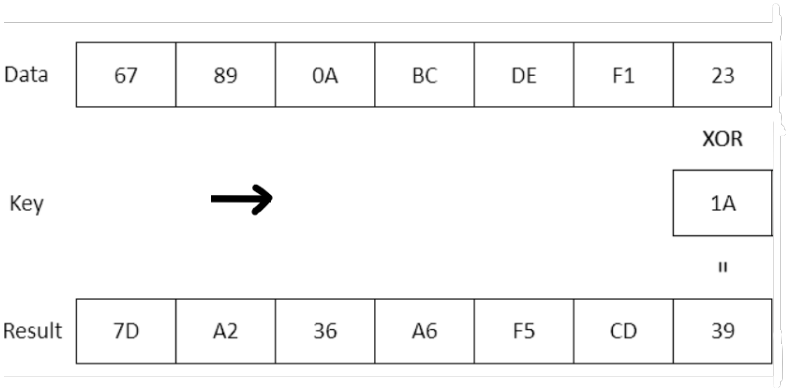


Figure 1.6: Simple XOR pixels diffusion

.

1.3.2.3 Hybrid Approaches

Modern image encryption methods often combine multiple strategies, permutation followed by diffusion controlled by a chaotic system, to achieve a secure, efficient, and application-specific solution [41]. These hybrid approaches strike a balance between speed and robustness, and can be adapted to meet application needs, such as real-time streaming or cloud-based storage. The growing need for lightweight encryption in resource-constrained environments, such as mobile or IOT devices, continues to drive innovation in this area.

1.3.2.4 Chaotic Systems

Chaotic systems provide a powerful foundation for image encryption due to their properties of sensitivity to initial conditions, pseudo-randomness, and ergodicity [42]. These systems generate sequences that appear random but are, in fact, deterministic and reproducible, provided a known key or parameter set is used. Commonly used chaotic maps include the Logistic Map, Henon Map, and Lorenz System [14]. Such systems are ideal for generating dynamic encryption keys or for controlling the permutation and diffusion stages of encryption. While detailed chaotic map mechanisms are discussed in the next chapter, it is essential to note that chaotic encryption schemes provide strong resistance to brute-force, statistical, and differential attacks, particularly when employed in hybrid configurations.

1.4 Chaos-Based Encryption

Chaotic systems are a class of deterministic dynamical systems that exhibit complex and random behavior. Despite being governed by simple mathematical equations, these systems are susceptible to initial conditions, highly nonlinear, and unpredictable in the long term [30]. These intrinsic properties make chaotic systems particularly well-suited for cryptographic applications, especially in the context of image encryption, where security, speed, and complexity are critical.

1.4.1 sensitivity to Initial Conditions

A defining feature of chaotic systems is their extreme sensitivity to initial conditions. Even a minuscule variation in the initial value of a system can lead to drastically different outcomes over time. This property, often referred to as the "butterfly effect, ensures that without exact knowledge of the initial parameters, it is computationally infeasible to predict or reconstruct the original data. In encryption, this translates into high key sensitivity, an essential attribute to resist brute-force and differential attacks [43].

1.4.2 Nonlinearity

Chaotic systems are governed by nonlinear mathematical functions, meaning their behavior cannot be represented as a simple combination of inputs. Nonlinearity is a key contributor to confusion in encryption, as it disrupts the linear relationship between the plaintext and ciphertext [44]. In image encryption, this results in better diffusion of pixel information, making statistical and known-plaintext attacks far more difficult.

1.4.3 Unpredictability and Ergodicity

Chaotic sequences are pseudo-random yet deterministic. It appears random but can be reproduced exactly with the correct key and parameters [45]. This unpredictability enhances encryption security by introducing randomness into the key stream used for permutation and diffusion processes. Additionally, many chaotic systems exhibit ergodicity, meaning their trajectories can cover the entire state space over time, which helps achieve a uniform pixel distribution in the encrypted image.

1.4.4 Benefits in Cryptographic Design

These properties collectively make chaos-based encryption systems highly robust and efficient [46]. They enable lightweight, real-time encryption suitable for high-throughput applications, such as satellite imaging, video surveillance, and mobile security. Furthermore, chaotic maps (Logistic Map, Henon Map, Lorenz System) can be easily implemented in both hardware and software environments with low computational cost [47].

In summary, the integration of chaotic systems into cryptographic design has significantly enhanced data security, particularly for images, due to their unpredictability, sensitivity to initial conditions, and low computational cost. However, while these methods effectively protect the content, they do not, on their own, ensure the identity of the user accessing the protected data.

In this regard, biometric approaches become essential, offering an authentication layer inherently tied to the individual. By combining robust cryptographic techniques with unique physiological or behavioral traits, modern security systems can provide dual assurance: data confidentiality and reliable identity verification. The following section provides an in-depth exploration of biometric security approaches, including their modalities, advantages, and challenges.

1.5 Biometric Security Approaches

Biometric security leverages unique physiological and behavioural characteristics to authenticate individuals, offering a robust alternative to traditional methods such as passwords and smart cards [48]. As digital threats become increasingly sophisticated, biometric systems offer enhanced protection through identity verification that is inherently tied to the individual, making impersonation more difficult.

1.5.1 Types of Biometric Modalities

Biometric authentication is categorised into two main types: physiological (based on body traits) and behavioral (based on actions).

1.5.1.1 Physiological Biometrics

- **Fingerprint Recognition:** Fingerprint recognition is a biometric technology that identifies individuals based on the unique ridge patterns found in their fingerprints [49]. Over time, it has transitioned from manual comparison methods to automated systems such as Automatic Fingerprint Identification Systems (AFIS), making it the most widely adopted biometric technique to date [50].

- **Facial Recognition:** The human face is a fundamental biometric trait that enables reliable individual differentiation within large populations. Due to its *ubiquity* and *inherent uniqueness*, facial recognition has become one of the most widely adopted and socially accepted biometric technologies [51]. The domain of facial recognition has attracted considerable research interest over the past four decades, positioning it as a central benchmark in the field of human identification and computer vision [52]. This sustained attention has led to significant advancements in algorithmic performance and real-world applicability. Facial recognition systems are now integral to numerous critical applications, including security surveillance, automated monitoring, border control, and the identification of missing persons or disaster victims.

- **Iris and Retina Scanning:** Iris recognition is a biometric authentication technique that leverages the unique and intricate patterns of the iris (colored ring surrounding the pupil) to identify individuals accurately. This method employs high-resolution imaging, often utilizing near-infrared illumination, to capture detailed iris patterns while minimizing reflections from the cornea. The captured images are then processed to extract distinctive features, which are converted into digital templates for comparison and identification purposes [53]. Unlike retinal scanning, which analyzes the blood vessel structure at the back of the eye, iris recognition is a non-invasive and more user-friendly method. The stability of iris features throughout a person's lifetime contributes to their high reliability and accuracy. Furthermore, iris recognition remains unaffected mainly by glasses or contact lenses, and among all biometric technologies, it has one of the lowest failure-to-enrol rates [54].

- **Vein Recognition:** Finger vein recognition is an emerging biometric modality that leverages the distinctive vascular patterns within the fingers for reliable personal identification. Unlike surface-level traits such as fingerprints, finger vein patterns are located beneath the skin, offering enhanced resistance to spoofing and environmental degradation [55]. Traditional recognition methods typically extract either minutiae-based features or binary texture descriptors such as Local Binary Patterns (LBP), Local Line Binary Patterns (LLBP), and Pattern-Based Binary Mapping (PBBM). While these approaches have shown utility, they present sev-

eral limitations [56]. Recent research suggests that anatomically inspired feature representations, which more accurately reflect the underlying vein structure, may offer a robust alternative to enhance the performance and reliability of finger vein recognition systems.

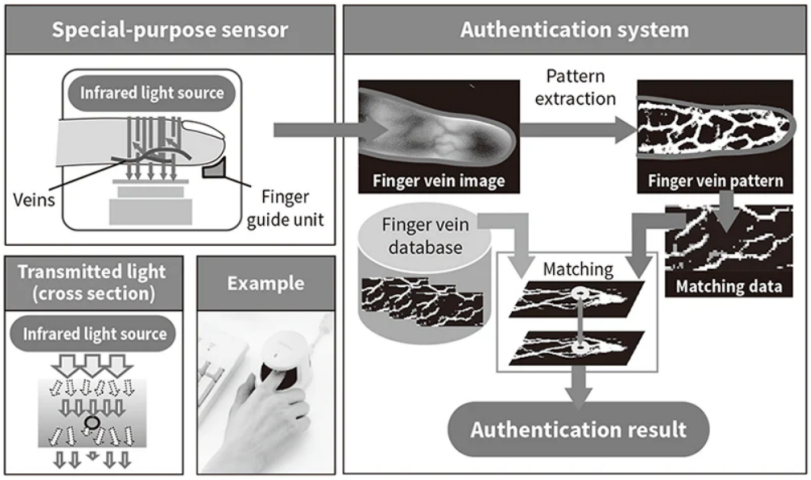


Figure 1.7: Vien Recognation System

.

1.5.1.2 Behavioral Biometrics

- **Voice Recognition:** Speech recognition is a core component of human–computer interaction, offering faster and more intuitive input than typing. Its widespread adoption is driven by applications such as virtual assistants, call centres, voice typing, and accessibility tools for users with physical limitations [57]. Despite advancements, current systems still lag behind human performance in speed and accuracy [58]. Speech signals are captured via microphones, converted into electrical signals, and processed using modern techniques to extract linguistic features. Audio is especially challenging to preprocess among various data types due to its variability and complexity.

- **Gait Recognition:** Gait recognition has emerged as a valuable biometric due to its ability to identify individuals remotely, even with low-resolution video and minimal equipment [59]. It functions without subject cooperation and remains effective when other traits, such as facial features or fingerprints, are obscured. Gait patterns are also challenging to replicate, enhancing security.
  With the rise of smartphones equipped with accelerometers and gyroscopes, gait data can now be captured passively. Combined with deep learning, this has led to more robust mobile gait recognition systems [60].

1.5.2 Advantages of Biometric Systems

- **Uniqueness:**Biometric systems rely on physiological and behavioral traits that are highly distinctive for each individual. Features such as fingerprints, iris patterns, facial structures, and vein maps are statistically unique, even among identical twins [61]. This uniqueness provides a strong basis for accurate identity verification, significantly reducing the chances of false acceptance or impersonation, which are common issues in traditional authentication methods.

- **Non-transferability:** Unlike passwords, smart cards, or access tokens, biometric traits are inherently bound to an individual and cannot be shared, borrowed, or forgotten. This intrinsic link between the user and their authentication credential enhances system integrity by eliminating the risks associated with stolen or misused credentials. As a result, non-transferability strengthens accountability and trust in access control systems.

- **Difficult to Forge:** Biometric traits such as fingerprints, iris patterns, and facial features are inherently difficult to replicate due to their complexity and uniqueness [62]. Unlike passwords or ID cards, they cannot be easily stolen or fabricated. Modern systems further enhance security through anti-spoofing methods, such as liveness detection and 3D sensing. Multimodal systems increase this resistance by requiring multiple traits for authentication [63].

- **Convenience:** Biometric systems simplify the authentication process by eliminating the need to remember complex passwords or carry physical devices. Authentication through fingerprint, facial recognition, or voice input is often faster and more intuitive, enhancing user experience and reducing operational delays [64]. This ease of use makes biometrics highly suitable for applications requiring frequent or rapid identity verification, such as mobile banking or airport check-ins.

- **Auditability:** Most biometric systems are designed to maintain detailed logs of authentication attempts, including timestamps and biometric match scores. These logs support forensic investigations and compliance with data protection regulations by providing traceable records of access events [15]. This level of auditability enhances transparency and promotes accountability in sensitive environments, such as healthcare or finance.

1.5.3 Security and Privacy Challenges

Despite offering significant advantages, biometric systems introduce specific security and privacy concerns that must be carefully addressed. These include:

- **Spoofing Attacks:** Biometric sensors can be deceived using artificial traits such as silicone fingerprints, 3D face masks, or recorded voice samples [62]. Without robust liveness detection, such systems are vulnerable to presentation attacks.
- **Template Theft:** Stored biometric templates are vulnerable to data breaches. Unlike passwords, compromised biometric data cannot be reissued, leading to long-term security risks [65]. Template protection techniques such as cancellable biometrics and biometric encryption are essential.
- **Sensor Noise and Environmental Variability:** The accuracy of biometric systems may degrade due to injuries, lighting changes, sensor quality, or environmental noise. These factors increase the chances of false acceptances or rejections [61].
- **Privacy Risks:** Biometric data is highly sensitive. Its unauthorized collection or misuse can lead to serious privacy violations and legal challenges. Applications like facial recognition in public surveillance highlight the ethical need for data protection, consent, and transparency [15].

1.5.4 Countermeasures and Liveness Detection

To mitigate the security and privacy vulnerabilities associated with biometric systems, various countermeasures have been developed to strengthen system robustness and trustworthiness. These include:

- **Liveness Detection:** This technique verifies that the biometric input originates from a live individual rather than an artificial replica. Methods include eye blink detection, blood flow analysis, skin texture, thermal imaging, and pulse detection [62]. These approaches are critical for resisting spoofing attacks such as fake fingerprints or 3D masks.
- **Multimodal Biometric Systems:** These systems integrate two or more biometric modalities, such as fingerprint and face recognition, to improve accuracy and security [63]. By requiring multiple independent traits, multimodal systems reduce the probability of false acceptance and improve resistance to spoofing and sensor failure.
- **Template Protection:** Biometric templates must be securely stored to prevent data breaches. Techniques such as biometric encryption, cancelable biometrics (which allow reissuable templates), and homomorphic encryption ensure that even if a template is compromised, the original biometric data remains unrecoverable [65].

1.5.5 Applications of Biometric Security

Biometric security systems use unique physical or behavioral traits for identity verification. They are widely applied in areas such as mobile authentication, banking, healthcare, and border control, offering enhanced security and convenience across both public and private sectors [66].

Table 1.2: Common Applications of Biometric Security

.

Domain	Use Case
Mobile Devices	Unlocking phones, app authentication
Healthcare	access to patient records, identity verification
Border Security	Automated passport control, traveller screening
Banking	ATM access, mobile login, voice-based services
Workplace	Time tracking, secure facility access
Voting Systems	Voter registration and identity verification
Law Enforcement	Suspect identification, surveillance systems
Smart Cities	Public access control, citizen ID systems
Education	Attendance tracking, exam proctoring
Retail	Payment authentication, loyalty access
Automotive	Driver verification, smart car start
Hospitality	Contactless check-in, room access
Military	Secure base entry, soldier ID checks

1.5.6 Future Trends

As biometric technologies continue to evolve, several emerging trends are shaping the future of secure identity verification systems. These developments aim to address current limitations related to accuracy, privacy, and scalability.

- **AI-driven Biometrics:** Deep learning and advanced artificial intelligence techniques are increasingly being used to improve recognition accuracy under challenging conditions such as poor lighting, occlusion, or noisy environments [66]. AI models can learn complex patterns in biometric data, enabling more robust detection and classification.

- **Behavioural Biometrics for Continuous Authentication:** Instead of relying on a single authentication event, behavioural biometrics monitor user behaviour continuously. Traits such as typing rhythm, mouse movement, gait, or device usage patterns enable seamless and passive authentication, improving both usability and security [16].

- **Edge Processing:** With increasing concerns over data privacy, there is a growing shift toward on-device biometric processing. Performing computations locally [67]

on smartphones or edge devices not only reduces latency and reliance on cloud infrastructure but also minimizes the risk of exposing biometric data.

- **Blockchain Integration:** Integrating blockchain technology with biometric systems introduces decentralised and tamper-resistant identity management solutions [68]. Blockchain can store biometric proof or transaction logs in a distributed ledger, ensuring transparency, auditability, and resistance to unauthorised modification.

1.6 Conclusion

In conclusion, this chapter has provided an overview of the context surrounding developments in information security, beginning with classical cryptographic systems, including symmetric, asymmetric, and hybrid encryption. These remain essential for secure communication and data protection. It then explored image encryption methods tailored to the unique structure of visual data, highlighting techniques like pixel permutation, diffusion, and chaos-based encryption, which offer high efficiency and robustness. Biometric security was also discussed as a modern alternative to passwords, utilizing traits like fingerprints, face, voice, and gait for authentication. Despite their advantages, biometrics face challenges such as spoofing and privacy risks, prompting the adoption of countermeasures, including liveness detection and template protection. Finally, the chapter outlines future trends, including AI-driven recognition, edge processing, and blockchain integration, which aim to make biometric systems smarter, more secure, and privacy-aware. These insights lay the groundwork for the research and innovation proposed in the following chapters.

Chapter 2

Chaotic Cryptographic and Biometric Security Systems

2.1 Introduction

In response to growing cybersecurity challenges, chaotic systems have gained significant attention in cryptography due to their inherent unpredictability and sensitivity to initial conditions. These properties make them highly suitable for tasks such as image encryption and secure key generation [69]. At the same time, biometric data, such as fingerprints and iris scans, have emerged as powerful tools for identity authentication, offering unique, non-replicable features. The integration of chaos theory and biometric-based key generation provides a hybrid framework that enhances both data security and access control [70]. Additionally, optical encryption techniques like Double Random Phase Encoding (DRPE) and the Fractional Fourier Transform (FrFT) further improve encryption robustness. This hybridisation ensures stronger resistance to statistical and differential attacks, making the system particularly suited for sensitive domains like medical imaging and secure digital identification[71]. This chapter presents essential chaotic map models alongside optical encryption methods such as Double Random Phase Encoding (DRPE) and the Fractional Fourier Transform (FrFT), highlighting how their integration with biometric-based key generation enhances security robustness against various attacks, thereby making the system highly effective for applications in medical image protection and secure digital identification.

2.2 Chaotic Maps in Cryptography

2.2.1 Introduction to chaos theory

Chaotic maps, rooted in chaos theory, have emerged as powerful tools in the design of modern cryptographic algorithms, particularly in fields such as image encryption

and key generation. Chaos theory describes the behavior of deterministic systems that are highly sensitive to initial conditions, a property known as the "butterfly effect", [72], leading to behavior that appears random and unpredictable. These characteristics, including ergodicity, topological mixing, and long-term unpredictability, make chaotic systems well-suited for cryptographic applications, where confusion, diffusion, and unpredictability are essential [43]. In particular, one-dimensional maps such as the logistic map, tent map, and Chebyshev map, as well as two-dimensional maps like the Henon and Baker maps, have been widely adopted to construct pseudorandom sequences and enhance data scrambling [73]. In image encryption, chaotic maps are used to generate dynamic keys and perform pixel-level permutation and substitution, thereby ensuring that even a slight change in the plaintext or key leads to a significantly different ciphertext. Additionally, the lightweight nature and high-speed implementation of chaotic systems make them attractive for securing real-time multimedia transmissions and IoT communications. However, despite their advantages, chaotic cryptographic schemes must be carefully designed and analyzed, as poor parameter selection or low-precision implementations can compromise security [74]. As research in this area matures, hybrid models combining chaos with DNA encoding, S-box substitution, or elliptic curve cryptography are gaining popularity for their enhanced security and complexity [75].

2.2.2 Relevance to Cryptography

Cryptography relies on principles of confusion, diffusion, and randomness to ensure the confidentiality, integrity, and authenticity of information. Traditional cryptographic algorithms such as AES and RSA employ algebraic structures and number theory to achieve these objectives. However, the rise of high-speed communication systems, real-time multimedia transmission, and the proliferation of IoT devices has prompted the exploration of lightweight and alternative cryptographic schemes [76].

Chaos-based cryptography offers a compelling alternative due to the inherent properties of chaotic systems. The unpredictability, ergodicity, and sensitivity to initial conditions in chaotic maps can be harnessed to generate key streams that are highly secure and difficult to reproduce [73]. These systems have gained considerable attention for their ability to provide strong security with lower computational cost, making them suitable for multimedia data protection, IoT, and embedded systems. For instance, foundational studies by Alvarez and Li [77], Kocarev and Lian [78] emphasise how chaotic dynamics meet core cryptographic requirements, such as diffusion and confusion, while surveys like Pisarchik and Flores-Carmona [79] highlight their computational efficiency for real-time applications. These properties make chaotic systems well-suited for designing symmetric encryption schemes, especially for images, videos, and sensor data, where traditional methods may struggle with speed and scalability [80]. Seminal work by Fridrich [81] on 2D

chaotic maps and recent advances by Wang and Chen [82] demonstrate their effectiveness in multimedia encryption, balancing robustness and low complexity.

Moreover, chaotic cryptographic systems often support real-time processing and can be embedded in resource-constrained environments. Hardware-efficient implementations, such as FPGA-based chaotic cyphers for IoT devices, and dynamic key-generation frameworks for edge computing, underscore their adaptability to cyber-physical systems [83]. Security analyses, confirm their resilience against differential and brute-force attacks, even in networked environments.

Moreover, chaotic cryptographic systems often support real-time processing and can be embedded in resource-constrained environments. As a result, chaos theory has become a foundational concept in the design of new cryptographic primitives, especially for lightweight encryption in cyber-physical systems and edge computing.

2.2.3 Classical Chaotic Maps Commonly Used

Various mathematical models of chaos, referred to as *chaotic maps*, are employed in cryptographic applications due to their sensitivity to initial conditions, ergodicity, and pseudo-random behavior. These maps differ in dimensionality (one-dimensional, two-dimensional, etc.), complexity, computational requirements, and their ability to generate cryptographically secure outputs. The most commonly used chaotic maps include the following:

- **Logistic Map**

  The logistic map is a simple yet powerful one-dimensional chaotic map described by the recursive equation:

  $$x_{n+1} = r x_n (1 - x_n), \tag{2.1}$$

  where $x_n \in (0, 1)$ and $r \in (3.57, 4)$ is the bifurcation parameter. It exhibits chaotic behavior when r approaches 4. Despite its simplicity, the logistic map produces highly unpredictable sequences and is widely used in lightweight encryption schemes, especially for image permutation and key stream generation. However, its effectiveness can degrade in digital implementations due to finite precision effects, leading to short cycles or convergence to fixed points if not properly scaled.

- **Quadratic map**

  The quadratic map is a simple one-dimensional nonlinear function that serves as a foundational model in the study of chaotic dynamics.The iterative recurrence relation defines it:

  $$x_{n+1} = r - x_n^2, \tag{2.2}$$

  where r is a control parameter, and $x_n \in \mathbb{R}$. This map exhibits a rich spectrum

of behaviours depending on the value of r, including fixed points, periodic orbits, bifurcations, and chaos.

As the parameter r increases, the system transitions from stable fixed points to chaotic regimes via period-doubling bifurcations, similar to the logistic map.For specific values of r, the map demonstrates sensitive dependence on initial conditions, a hallmark of chaotic systems

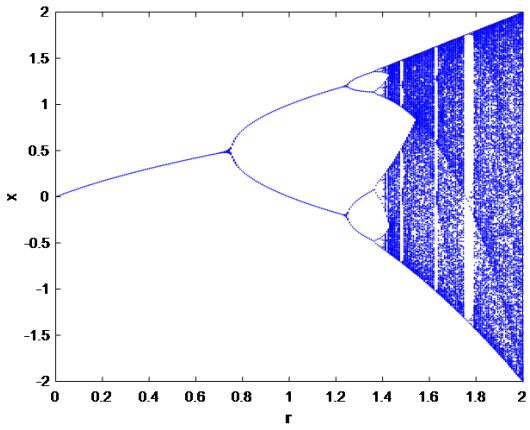


Figure 2.1: Quadratic map bifurcation diagram

.

In cryptographic applications, the quadratic map is valued for its simplicity and ability to generate pseudo-random sequences. It is especially useful in lightweight encryption schemes, chaotic key generators [84], and random bit stream production due to its low computational cost and complex dynamic behaviour.

- **Cubic map**

  The cubic map is another one-dimensional chaotic function that introduces an additional nonlinear term, allowing for even more complex dynamical behaviour than the quadratic map. It is commonly expressed as:

$$x_{n+1} = r \cdot x_n \cdot \left(1 - x_n^2\right) \tag{2.3}$$

  where r is real-valued parameter controlling the system's behavior.

  The cubic map exhibits both symmetric and asymmetric bifurcation structures, and depending on the parameter settings, it can transition between periodic and chaotic behaviour. Due to the cubic nonlinearity, it supports multi-stable states and exhibits stronger nonlinearity than the logistic or quadratic maps.

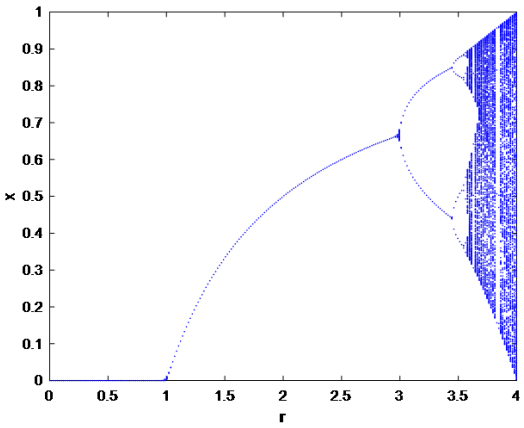


Figure 2.2: Cubic map bifurcation diagram

.

From a security perspective, the cubic map provides a greater degree of unpredictability and can be tuned more precisely, making it suitable for applications in image encryption, watermarking, and secure communication. Its increased sensitivity and adjustable complexity offer enhanced cryptographic strength, particularly when combined with other maps in hybrid systems.

- **Tent Map**

  The tent map is another one-dimensional map defined as:

$$x_{n+1} = \mu \min(x_n, 1 - x_n) \tag{2.4}$$

  where $\mu \in (0, 2]$ is the control parameter. The tent map is known for its uniform distribution of output values and strong mixing behavior. It generates key sequences with desirable statistical randomness, making it suitable for applications that require uniformity, such as image encryption and watermarking. The tent map is also computationally efficient and less prone to rounding errors, making it advantageous for hardware implementations [14].

- **Henon Map**

  The Henon map is a two-dimensional discrete-time dynamical system given by:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n, \\ y_{n+1} = bx_n, \end{cases} \tag{2.5}$$

  where $a = 1.4$ and $b = 0.3$ typically yield chaotic behavior. This map offers increased complexity over one-dimensional maps and provides better resistance to certain types of cryptanalytic attacks due to its higher dimensionality. In cryptographic

systems, the Henon map is used for pixel diffusion and generating multi-channel chaotic sequences. Its strong coupling between state variables increases entropy and enhances unpredictability in encryption outputs.

- **Lorenz System**

  The Lorenz system is a continuous-time, three-dimensional chaotic system originally developed to model atmospheric convection. It is defined by the differential equations:

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x), \\ \frac{dy}{dt} = x(\rho - z) - y, \\ \frac{dz}{dt} = xy - \beta z, \end{cases} \tag{2.6}$$

  where σ, ρ, β are system parameters. The Lorenz system is highly sensitive to initial conditions and exhibits complex chaotic attractors [47]. In cryptographic applications, its continuous nature can be discretized for digital implementations. It is particularly used in high-security contexts and hybrid schemes that combine multiple chaotic systems or integrate chaos with DNA encoding or neural networks. The Lorenz system supports parallelism and multi-level key generation, making it suitable for multimedia data encryption.

2.2.4 Applications in Image Encryption and Key Generation

The most prominent use of chaotic maps in cryptography lies in *image encryption*, where the high dimensionality and sensitivity of chaotic systems are leveraged to scramble pixel values and positions. Unlike text-based encryption, images possess spatial redundancy and large data volumes, which traditional algorithms are not optimized for. Chaos-based methods typically follow a two-stage process: permutation (confusion) and diffusion (modification of pixel values) [43].

Chaotic maps are also instrumental in *key generation*, producing pseudo-random sequences with strong unpredictability and large key spaces. The initialization values (seeds) of chaotic maps act as secret keys, and small deviations in these parameters result in completely different encryption outputs, which enhances resistance to brute-force attacks.

Additionally, hybrid systems often combine chaotic maps with DNA encoding, neural networks, or traditional cryptographic primitives to strengthen encryption, diversify key spaces, and adapt to different security requirements [72].

2.2.5 Advantages and Limitations

The use of chaotic maps in cryptographic systems offers several notable advantages:

- **High sensitivity to initial conditions**, which ensures resistance to brute-force and differential attacks.
- **Fast computation and parallelizability**, making them ideal for real-time applications and multimedia encryption.
- **Flexibility and adaptability**, allowing custom designs for specific use cases such as IoT, healthcare data, or embedded systems.

However, chaos-based cryptography is not without limitations:

- **Finite precision effects** in digital implementations can degrade the chaotic behavior, leading to predictability.
- **Lack of standardization** and formal security proofs, unlike AES or RSA, which have undergone extensive cryptanalysis.
- **Vulnerability to chosen plaintext attacks** if the chaotic system or key management process is poorly designed.

Therefore, while chaotic maps offer promising features for modern cryptographic applications, careful design, validation, and hybridization with traditional schemes are recommended to mitigate their weaknesses.

2.3 Introduction to DRPE and FrFT

2.3.1 Motivation and Background

Traditional cryptographic algorithms such as AES and RSA are primarily designed for textual or binary data. When applied to visual data like images, they often fail to exploit the inherent spatial redundancy and large data size, leading to inefficient performance and increased computational burden. Additionally, with the rising demand for secure image transmission in applications such as satellite imaging, medical diagnostics, and biometric systems, there is a need for specialized techniques that offer both high security and efficient processing.

Optical encryption techniques, particularly those based on transform domains, have gained prominence for their ability to handle large-scale visual data efficiently [85]. Among them, Double Random Phase Encoding (DRPE) and the Fractional Fourier Transform (FrFT) are widely studied for their potential to offer high-dimensional encryption and enhanced security.

2.3.2 Double Random Phase Encoding (DRPE)

Double Random Phase Encoding (DRPE) is a foundational optical encryption method introduced by Refregier and Javidi. It encrypts an image by modulating it with two statistically independent random phase masks one in the spatial domain and one in the frequency domain [86]. The process involves:

2.3.2.1 DRPE Encryption Process

The Double Random Phase Encoding (DRPE) technique encrypts an input image by introducing controlled randomness through phase modulation in both the spatial and frequency domains. The process involves the following key steps:

- **Modulating the input image with a spatial-domain random phase mask $R_1(x, y)$:**

  The original grayscale image $I(x, y)$, treated as a 2D intensity function, is first multiplied by a random phase mask $R_1(x, y) = \exp[i\phi_1(x, y)]$, where $\phi_1(x, y)$ is a matrix of uniformly distributed random phases between 0 and 2π. This modulation obscures the spatial features of the image and prepares it for transformation into the frequency domain:

  $$I'(x, y) = I(x, y) \cdot R_1(x, y)$$

- **Applying a forward Fourier Transform (FT):**
  A two-dimensional Fourier Transform is applied to the modulated image $I'(x, y)$ to move it into the frequency domain:

  $$F(u, v) = \mathcal{F}[I(x, y) \cdot R_1(x, y)]$$

- **Modulating the result with a frequency-domain random phase mask $R_2(u, v)$:**
  A second phase mask $R_2(u, v) = \exp[i\phi_2(u, v)]$ is applied:

  $$F'(u, v) = F(u, v) \cdot R_2(u, v)$$

- **Applying an inverse Fourier Transform (IFT):**
  The encrypted image is obtained by applying the inverse FT:

  $$E(x, y) = \mathcal{F}^{-1}[F'(u, v)]$$

Mathematically, this can be represented as:

$$E(x,y) = \mathcal{F}^{-1}\left\{\mathcal{F}\left[I(x,y)\cdot R_1(x,y)\right]\cdot R_2(u,v)\right\}$$

where $\mathcal{F}$ and $\mathcal{F}^{-1}$ denote the forward and inverse Fourier transforms, respectively.

The output $E(x,y)$ appears as a complex noise-like image and is unintelligible without knowledge of both phase masks, making DRPE a highly secure encryption technique. However, standard DRPE systems rely heavily on Fourier transforms, which may limit their flexibility in certain domains.

2.3.3 Fractional Fourier Transform (FrFT)

The Fractional Fourier Transform (FrFT) is a mathematical generalisation of the classical Fourier Transform (FT), extending the concept of signal representation from the time and frequency domains to intermediate domains. Unlike the standard FT, which provides a complete transition from time to frequency, the FrFT introduces a tunable parameter called the *fractional order* α, that allows partial transformation between these two domains.

Mathematically, the FrFT can be interpreted as a rotation in the time-frequency phase space by an angle $\theta = \alpha\frac{\pi}{2}$. When $\alpha = 0$, the FrFT becomes the identity operation. When $\alpha = 1$, the FrFT reduces to the conventional Fourier Transform. Similarly, $\alpha = 2$ corresponds to a time-reversed signal, and $\alpha = 4$ completes a full rotation back to the original signal, making the FrFT a periodic operator with period 4.

The one-dimensional FrFT of a signal $f(t)$ is defined by the integral:

$$F_\alpha(u) = \int_{-\infty}^{\infty} K_\alpha(u,t) f(t)\, dt$$

where $K_\alpha(u,t)$ is the FrFT kernel, given by:

$$K_\alpha(u,t) = A_\alpha \cdot \exp\left[i\pi(u^2+t^2)\cot\alpha - 2\pi iut\csc\alpha\right],$$

and

$$A_\alpha = \sqrt{1 - i\cot\alpha}.$$

This kernel allows continuous interpolation between the time and frequency domains by adjusting the value of α. The FrFT is linear, unitary, and preserves energy, making it a suitable and powerful tool in a variety of signal processing applications [87].

In practical terms, the FrFT offers several advantages over the classical FT. It enables intermediate-domain filtering, time-frequency localized analysis, and increased flexibility in transform-based algorithms. These characteristics make FrFT particularly valuable in

applications such as image watermarking, secure communication, radar signal processing, and optical encryption systems.

When applied in the context of encryption, especially in combination with techniques like Double Random Phase Encoding (DRPE-FrFT) adds an extra layer of security by embedding the fractional order α as an additional key parameter. The non-linear and order-sensitive nature of the FrFT significantly increases the complexity for unauthorized decryption attempts, thereby enhancing the robustness of the overall system.

2.3.4 Combination of DRPE and FrFT

The combination of DRPE and FrFT forms a powerful hybrid encryption technique. By replacing the standard Fourier transforms in the DRPE process with fractional Fourier transforms of variable orders, the system introduces an additional set of keys—the transform orders α_1 and α_2. The encryption process becomes:

$$E(x, y) = \mathcal{F}^{-\alpha_2} \left\{ \mathcal{F}^{\alpha_1} \left[I(x, y) \cdot R_1(x, y) \right] \cdot R_2(u, v) \right\}$$

This approach significantly enlarges the key space and increases the complexity of brute-force attacks, as the attacker must now guess the correct fractional orders in addition to the phase masks. Moreover, the use of FrFT enhances security against known-plaintext and chosen-plaintext attacks due to the non-linear and order-dependent behavior of the transform.

2.3.5 Applications and Advantages

The integration of Double Random Phase Encoding (DRPE) with the Fractional Fourier Transform (FrFT) has proven to be an effective and versatile technique for securing various forms of high-value data, particularly in the domains of image encryption and optical cryptography. Owing to its multi-dimensional key space and high resistance to attacks, the DRPE–FrFT combination has found applications across several fields requiring both real-time processing and robust confidentiality.

2.3.5.1 Applications

- **High-resolution image encryption**: In digital imaging and satellite surveillance, securing large image datasets against interception or unauthorized access is critical. DRPE–FrFT systems provide a scalable encryption framework that can process high-resolution grayscale or color images while preserving performance and security. Since both DRPE and FrFT can be implemented optically or digitally, they are especially suited to secure live data feeds in defense and remote sensing.

- **Medical image protection**: Protecting patient data is a legal and ethical imperative in healthcare systems. Encryption of medical images such as X-rays, MRI scans, and CT data using DRPE–FrFT prevents identity exposure, misdiagnosis, or data tampering. The layered encryption enabled by phase masks and fractional orders ensures that sensitive diagnostic data can be shared across hospital networks or cloud services without compromising security.
- **Military surveillance and secure communications**: Military-grade applications often demand rapid, secure transmission of aerial or reconnaissance imagery. DRPE–FrFT systems support robust encryption in battlefield environments and can be integrated into secure communication channels or satellite imaging workflows to guard against signal interception and reverse-engineering of encrypted data.
- **Multimedia content encryption**: Video streams, biometric datasets, and digital archives benefit from the adaptability of DRPE–FrFT, which enables frame-wise encryption, watermarking, and copyright protection. The system's transform-domain design allows for efficient embedding into compression and transmission pipelines, offering both confidentiality and content verification.
- **Optical computing**: In emerging optical systems, DRPE–FrFT is used for real-time encoding of holographic patterns. These encrypted holograms can be stored or transmitted in optical memory formats and later decrypted through synchronized optical setups using fractional transforms.

2.3.5.2 Advantages

- **High security**: The DRPE–FrFT scheme leverages multiple encryption keys, including two independent random phase masks and two fractional transform orders (α_1, α_2). This significantly expands the key space and makes brute-force or exhaustive search attacks computationally infeasible. Additionally, the nonlinearity of the FrFT introduces further resistance to linear cryptanalysis and chosen-plaintext attacks.
- **Efficiency and scalability**: Both DRPE and FrFT rely on mathematical transforms that are well-suited for fast computation using FFT-based algorithms. This makes the system compatible with real-time processing requirements and adaptable to parallel computation platforms such as GPUs or optical processors. Furthermore, DRPE–FrFT can be applied to datasets of varying sizes and formats without redesigning the core algorithm.
- **Robustness and error tolerance**: The encrypted data generated by DRPE–FrFT exhibits resilience against statistical analysis, differential attacks, and minor transmission noise. The deterministic yet complex nature of the system ensures that small

errors in transmission or channel distortion do not cause catastrophic decryption failure, which is vital in satellite, wireless, and optical network contexts.

- **Flexible integration**: Because the underlying algorithms are transform-based, DRPE–FrFT can be embedded within digital signal processing chains or optical systems [88]. This allows for hybrid encryption architectures that use digital encoding and optical decoding (or vice versa), supporting smart devices, IoT infrastructures, and cloud-based secure imaging systems.

In summary, the DRPE–FrFT approach addresses many of the limitations found in traditional image encryption schemes. It achieves a balance between computational efficiency and cryptographic strength, making it an attractive choice for a wide range of modern applications where visual information must be securely processed, stored, or transmitted.

2.4 Nonlinear Functions for image-processing

Nonlinear functions have emerged as essential tools in image processing due to their ability to model complex, real-world transformations that linear systems cannot adequately capture. Unlike linear operations, which preserve proportional relationships between input and output, nonlinear functions enable local adaptation, dynamic range compression, and chaotic transformations, making them indispensable in modern image encryption, enhancement, and analysis tasks. This chapter explores various nonlinear functions and their applications in secure and efficient image-processing systems.

2.4.1 Common Nonlinear Functions Used in Image Processing

A nonlinear function is one that does not satisfy the principle of superposition, meaning the output is not directly proportional to the input. Mathematically, these functions are defined by equations involving powers, exponentials, trigonometric functions, or piecewise rules. In image processing, nonlinear mappings are used to introduce nonuniform behavior in intensity transformations, spatial filtering, and encryption schemes. Common properties include sensitivity to initial conditions, boundedness, and differentiability, depending on the function. Several nonlinear functions have been adapted for image processing tasks:

2.4.1.1 Sigmoid Function

The sigmoid function, often denoted as $\sigma(x)$, is a widely used nonlinear activation function in image processing, machine learning, and signal transformation. It maps any real-valued input x to a value between 0 and 1, creating an "S"-shaped curve that smoothly

transitions from one asymptote to another. The mathematical definition of the sigmoid function is:

$$\sigma(x) = \frac{1}{1 + e^{-kx}} \tag{2.7}$$

where e is Euler's number (approximately 2.71828), $x \in \mathbb{R}$ is the input, and $k > 0$ is a parameter that controls the steepness of the curve. Larger values of k make the transition sharper, while smaller values produce a more gradual slope.

The sigmoid function outputs values in the range $(0, 1)$, making it particularly suitable for modeling probabilities, performing intensity normalization, and enhancing contrast in image processing. For large positive values of x, $\sigma(x)$ approaches 1, while for large negative values, it approaches 0. Near $x = 0$, the function behaves approximately linearly, providing smooth adjustments for pixel intensities close to the midrange.

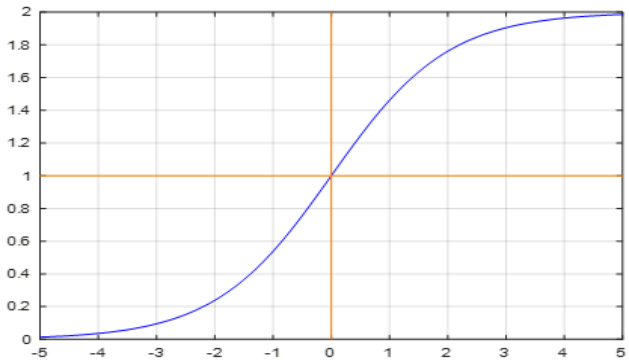


Figure 2.3: Sigmoid function

.

The bounded output and smooth gradient of the sigmoid function make it an ideal candidate for contrast stretching, image enhancement, and as an activation function in neural networks designed for image recognition or encryption tasks.

The inverse of the sigmoid function, known as the **logit function**, is essential in applications requiring the recovery of original input values from the sigmoid output, such as in decryption or signal reconstruction. The logit function is mathematically defined as:

$$\sigma^{-1}(y) = \ln\left(\frac{y}{1-y}\right), \quad y \in (0, 1) \tag{2.8}$$

where $\ln(\cdot)$ is the natural logarithm. The domain of σ^{-1} is $(0, 1)$, corresponding to the range of the sigmoid function [89] This inverse function allows for exact reconstruction of the input x given the output $\sigma(x)$, enabling reversible nonlinear transformations critical in image encryption and recovery processes.

2.4.1.2 Hyperbolic Tangent Function

The **hyperbolic tangent function**, denoted as $\tanh(x)$, is a fundamental nonlinear function widely used in image processing, neural networks, and signal transformation. It is defined as the ratio of the hyperbolic sine to the hyperbolic cosine of a given input value x:

$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{2.9}$$

In this equation, e represents Euler's number (approximately 2.71828), the base of the natural logarithm, and $x \in \mathbb{R}$ is the input variable, which can be any real number. The

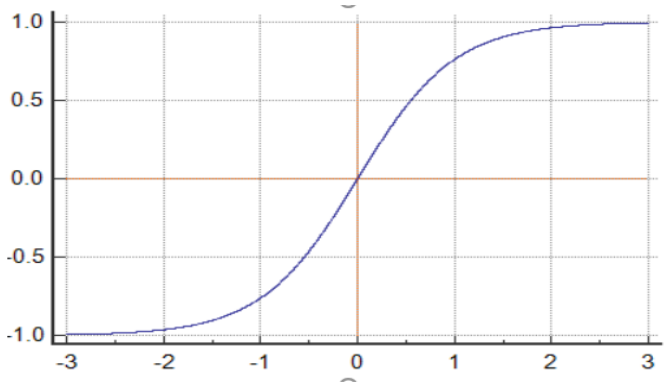


Figure 2.4: Tanh function

.

tanh function maps real numbers onto the interval $[-1, 1]$, producing an "S"-shaped curve known as a sigmoid-like activation. For large positive values of x, $\tanh(x)$ approaches 1, while for large negative values, it approaches -1. Near zero, the function behaves almost linearly, providing smooth transitions for small input values. This characteristic makes the hyperbolic tangent particularly useful in intensity normalization and contrast enhancement in images, as it compresses the dynamic range while preserving the relative order of pixel intensities.

The smooth and bounded nature of tanh helps reduce the impact of outliers and enhances feature visibility in underexposed or overexposed regions. Moreover, its differentiability makes it convenient for optimization algorithms in machine learning and adaptive filtering [90].

The inverse of the hyperbolic tangent function, called the **hyperbolic arctangent** and denoted as $\operatorname{atanh}(x)$ or $\tanh^{-1}(x)$, is crucial in applications such as image decryption and signal restoration, where one needs to recover the original values from the transformed data. It is defined by the formula:

$$\operatorname{atanh}(x) = \frac{1}{2} \ln\left(\frac{1+x}{1-x}\right), \quad x \in (-1, 1) \tag{2.10}$$

Here, $\ln(\cdot)$ denotes the natural logarithm. The domain of atanh is restricted to $(-1, 1)$, which corresponds to the range of the tanh function. This inverse function enables exact recovery of the input x from the output of the tanh function, making it vital in reversible image transformations and cryptographic schemes that rely on nonlinear mappings.

2.4.1.3 Piecewise Linear Chaotic Map (PWLCM)

The Piecewise Linear Chaotic Map (PWLCM) is a nonlinear function characterized by its simple piecewise linear structure and strong chaotic properties. It is often used in image encryption algorithms to generate pseudo-random sequences for pixel permutation and substitution. The *Piecewise Linear Chaotic Map (PWLCM)* is defined as:

$$x_{n+1} = \begin{cases} \frac{x_n}{p}, & 0 \leq x_n < p \\ \frac{1-x_n}{1-p}, & p \leq x_n \leq 1 \end{cases}$$

where $x_n \in [0, 1]$ and $p \in (0, 1)$ is the control parameter. The inverse of this function can be derived by solving for x_n in terms of x_{n+1} for both cases. For the first case, when $x_n \in [0, p]$, the inverse is $x_n = p \cdot x_{n+1}$. For the second case, when $x_n \in [p, 1]$, the inverse is $x_n = 1 - (1 - p) \cdot x_{n+1}$. Combining both cases, the inverse of the PWLCM is:

$$x_n = \begin{cases} p \cdot x_{n+1}, & 0 \leq x_{n+1} < p \\ 1 - (1 - p) \cdot x_{n+1}, & p \leq x_{n+1} \leq 1 \end{cases}$$

This inverse function allows for the reconstruction of the original values x_n from the transformed values x_{n+1}, making the PWLCM suitable for reversible encryption processes in cryptography [91].

Furthermore, the simplicity of PWLCM allows for straightforward analysis and integration with other chaotic maps or nonlinear functions, enhancing the overall robustness and complexity of cryptographic schemes.

2.4.2 Applications in Image Processing

Nonlinear functions find extensive use in a variety of image processing tasks due to their ability to model complex transformations and handle data adaptively. The following subsections highlight key application areas where nonlinear functions play a critical role.

2.4.2.1 Image Encryption

In image encryption, nonlinear chaotic maps such as the *logistic map* and *cubic map* are utilized to generate pseudo-random sequences that effectively scramble pixel positions and modify pixel values. These sequences exhibit high sensitivity to initial conditions

and control parameters, which ensures that small changes in the key or initial state produce drastically different encrypted outputs. This sensitivity and unpredictability form the foundation of cryptographic strength, making chaotic maps ideal for secure image encryption schemes. The nonlinear dynamics also help resist statistical and differential attacks by introducing complex confusion and diffusion properties in the encrypted image.

2.4.2.2 Contrast Enhancement

Nonlinear functions like the *sigmoid* and *hyperbolic tangent (tanh)* are widely used for contrast enhancement. These functions apply a nonlinear transformation to pixel intensities, allowing for selective amplification or compression of specific intensity ranges. For example, sigmoid functions can increase contrast in mid-tones while suppressing noise in very dark or bright regions, thereby improving the visibility of subtle details in underexposed or overexposed images. Such nonlinear mappings better mimic human visual perception, enhancing overall image quality without amplifying noise excessively.

2.4.2.3 Edge Detection and Segmentation

Nonlinear filtering techniques are crucial for edge detection and image segmentation tasks. Unlike linear filters, which tend to blur edges and important structural details, nonlinear filters preserve edges while effectively reducing noise. For example, median filters and anisotropic diffusion methods operate nonlinearly to smooth homogeneous regions while maintaining sharp transitions at object boundaries. This property is especially important in medical imaging and object recognition, where precise boundary delineation is essential for accurate diagnosis or classification.

2.4.2.4 Watermarking and Authentication

Nonlinear dynamical systems provide robust frameworks for digital watermarking and image authentication. By embedding watermark information using nonlinear chaotic sequences or transformations, the watermark becomes difficult to detect or remove without the correct key. The nonlinear embedding ensures that the watermark is imperceptible in normal viewing conditions yet can be reliably extracted during authentication. Additionally, nonlinear methods often allow reversible watermarking, enabling lossless recovery of the original image, which is critical in sensitive applications such as legal evidence or medical imagery.

2.4.2.5 Noise Suppression and Denoising

In noise suppression, nonlinear smoothing filters such as bilateral filters and median filters outperform classical linear techniques by maintaining image edges and textures while

reducing random noise. Bilateral filtering, for instance, combines spatial closeness and intensity similarity in a nonlinear weighting scheme, ensuring that only similar neighboring pixels influence the smoothing process. This selective smoothing helps retain important image features and avoids the oversmoothing artifacts common in linear filtering. Consequently, nonlinear denoising methods are widely adopted in photographic enhancement, video processing, and medical image restoration.

2.5 Biometric-Based Key Generation

Biometric-based key generation is an innovative approach to cryptographic key creation that leverages the unique physiological or behavioral characteristics of individuals, such as fingerprints, iris patterns, voice, or gait. Unlike traditional key generation methods relying on random number generators or user-chosen passwords, biometric-based systems extract cryptographic keys directly from biometric data, providing an intrinsic link between the user's identity and the security credentials.

2.5.1 Fundamentals

The core idea behind biometric-based key generation is to transform raw biometric measurements into a stable and reproducible cryptographic key. This process generally involves several stages:

- **Feature Extraction**: Relevant features are extracted from the biometric data using signal processing and pattern recognition techniques. These features must be distinctive, repeatable, and robust to noise or variations in biometric capture.
- **Quantization and Encoding**: The extracted features are quantized and encoded into a binary format suitable for cryptographic use. This step often employs error correction codes to handle variability and noise in biometric inputs.
- **Key Binding or Key Generation**: The encoded biometric data is then used either to directly generate a cryptographic key or to bind an externally generated key to the biometric template securely.

2.5.2 Methods

Several methods have been proposed for biometric key generation, including:

- **Fuzzy Commitment and Fuzzy Vault**: These schemes bind a secret key with biometric data using error-correcting codes, allowing key recovery only when the biometric input is sufficiently close to the enrolled template.

- **Helper Data Systems**: Helper data are publicly stored auxiliary information that assists in reconstructing the key from noisy biometric data without leaking sensitive information.
- **Cancelable Biometrics**: Biometric data are intentionally transformed with a revocable function before key generation, enhancing privacy and allowing template renewal in case of compromise.

2.5.3 Advantages

Biometric-based key generation offers several advantages over traditional approaches:

- **Enhanced Security**: Keys are inherently tied to the user's unique biometric traits, reducing the risk of key theft or guessing.
- **User Convenience**: Eliminates the need for users to remember complex passwords or carry physical tokens.
- **Non-Repudiation**: Biometric keys provide stronger assurance of user identity in authentication systems.

2.5.4 Challenges

Despite its potential, biometric-based key generation faces several challenges:

- **Variability in Biometric Data**: Natural variations due to sensor noise, environmental conditions, or physiological changes can cause inconsistency in biometric readings, complicating stable key generation.
- **Privacy Concerns**: Biometric data is sensitive and immutable; leakage can have long-term consequences, necessitating secure storage and template protection.
- **Computational Complexity**: The extraction, encoding, and error correction steps add computational overhead, which can affect system performance.

2.5.5 Applications

Biometric-based key generation is increasingly utilized across various sectors to provide strong, user-friendly authentication and secure cryptographic key management. In secure access control, it replaces traditional passwords and tokens by binding access rights to unique biometric traits, enhancing protection in corporate, government, and restricted environments. Mobile devices employ biometric keys for seamless unlocking and transaction authentication, safeguarding sensitive personal data. Financial institutions

use biometric-generated keys to prevent fraud and strengthen multi-factor authentication for banking services. Healthcare systems benefit by securing patient records and medical devices through biometric verification [70]. Government identity programs and border control integrate biometric key generation to improve citizen identification and digital service security. Emerging applications include securing IoT networks, cloud services, and blockchain-based identity frameworks, highlighting the versatility and growing importance of biometric key generation in modern security architectures.

2.6 Related Works Analysis

Various strategies have been explored in cryptographic systems to enhance security and efficiency, underscoring the significance of the proposed approach. In 2013, Liu et al. [92] introduced a novel image encryption technique that combined pixel scrambling with the fractional Fourier transform, strengthened by double random phase encoding for enhanced security. Their work highlighted the importance of advanced encryption mechanisms for safeguarding data during storage and transmission. Building on this foundation, Sathiyamurthi and Ramakrishnan 2017 developed new techniques for speech encryption by employing shift keying based on chaos theory [93]. This method utilized chaotic maps, including logistic, tent, quadratic, and Bernoulli maps, to shuffle speech samples, while the Chen map was incorporated to further enhance the chaotic dynamics. In 2019, Al-Dwairi et al. [94] proposed a robust and efficient encryption-decryption technique for digital colour images, which are widely used and frequently transmitted over the internet. Their evaluation demonstrated the superior performance of the proposed scheme compared to existing approaches, highlighting its efficiency and effectiveness.

Moreover, Jan Sher Khan et al. [95] developed a secure encryption algorithm specifically designed for medical data, utilizing chaotic maps in conjunction with the Discrete Wavelet Transform (DWT). This approach employed a DNA sequence and a plaintext image to derive the chaotic map's initial conditions using the SHA-512 algorithm. Simulation results validated the high security and reliability of the proposed method. On the other hand, Yunling et al. and Mokhnache et al. [96, 97] conducted cryptanalysis studies on an image block cipher designed with chaotic maps. Their findings revealed vulnerabilities, showing that attackers could generate substitute keys capable of decrypting other images encrypted with the valid key, thus exposing security weaknesses in such designs. In 2021, Subhajit and Sunil introduced an innovative audio encryption approach that combined Henon and Tent chaotic maps. The functions were integrated using an XOR operation to form the secret key, resulting in an efficient and secure encryption method [98].In 2023, Huang et al. [99] introduced an optical image cryptosystem that employed the FrFT in combination with the DRPE technique to generate encrypted images. Their system demonstrated strong key sensitivity, significantly enhancing security. By 2024,

D. Herbadji et al. [100] advanced chaotic systems by broadening the chaotic range and increasing randomness, resulting in improved efficiency compared to previous systems. Their algorithm specifically targeted audio processing, discarding silent and irrelevant segments prior to encryption, thereby optimizing resource utilization and reducing processing time.

Building on these advancements, our study integrates combined mapping techniques and the FrFT to develop an enhanced methodology for image encryption. While prior works have demonstrated significant progress in chaotic encryption systems, they often suffer from limitations such as restricted chaotic ranges, reduced randomness, and vulnerabilities to specific cryptographic attacks. For example, existing methods like those proposed by Benaissi et al. [101] and Herbadji et al. [100] offer strong security features but face challenges in scalability and computational efficiency when applied to large-scale image datasets or high-dimensional multimedia content.

In contrast, our proposed scheme leverages an enhanced composite chaotic map, which combines quadratic and cubic chaotic maps, to overcome these limitations by expanding the chaotic range and improving key sensitivity. By integrating optical DRPE and the FrFT, our system further strengthens encryption by utilizing both spatial and frequency domain transformations. These enhancements provide superior resistance to cryptanalytic attacks, better adaptability to diverse image types, and improved processing efficiency. Simulation results validate the effectiveness of the proposed method, demonstrating its robustness against cryptographic attacks and a higher degree of security compared to traditional approaches. Furthermore, our system addresses key challenges in prior studies, such as limited scalability and computational overhead, making it a more practical solution for modern image encryption needs. These advancements underscore the importance of the proposed work, offering a secure, efficient, and adaptable encryption framework suitable for contemporary multimedia security challenges. Several chaotic encryption techniques have been proposed, each with unique strengths and limitations. However, many existing approaches suffer from issues such as limited chaotic range, low key sensitivity, or vulnerability to statistical attacks.

2.7 Conclusion

This chapter provided a comprehensive review of modern visual cryptography approaches, highlighting the integration of chaotic systems, optical transforms, and biometric keys. The use of chaotic maps (logistic, quadratic, cubic, Henon, Lorenz, etc.) has proven to be a powerful tool for ensuring confusion and diffusion in encryption schemes due to their sensitivity to initial conditions and pseudo-random behavior. The adoption of opto-digital techniques such as Double Random Phase Encoding (DRPE) and the Fractional Fourier Transform (FrFT) has expanded the key space and introduced additional

computational complexity, thereby enhancing security against classical attacks such as chosen plaintext attacks. The DRPE–FrFT combination has shown to be particularly effective for encrypting medical, military, or satellite images, while remaining suitable for real-time and low-resource implementations. In addition, the study of nonlinear functions (sigmoid, hyperbolic tangent, PWLCM) illustrated their central role in contrast enhancement, edge detection, and watermark-based authentication, and adaptive image denoising. Through their dynamic behavior, these functions contribute significantly to the robustness and flexibility of image processing systems. Finally, biometric keys were introduced as a promising paradigm that links human identity with secure cryptographic key generation. Despite challenges such as biometric variability and privacy concerns, these systems provide an additional layer of security and non-repudiation in moderns architectures. Thus, this chapter lays the theoretical and technical groundwork for an advanced, secure, adaptable, and resilient encryption architecture, built upon the synergy between chaos, optics, and biometrics, all of which will be exploited in the following chapters for the design of a chaotic biometric image encryption system.

Contributions

Chapter 3

Chaotic Retinal Image Encryption Pre-processing Based on Biometric Key

3.1 Introduction

In the contemporary landscape of digital healthcare, medical imaging plays a pivotal role in diagnosis, treatment planning, and biometric verification. With the advent of telemedicine, electronic health records, and AI-powered diagnostics, there is an ever-increasing reliance on the storage and transmission of medical images across distributed networks [102]. Retinal images, in particular, offer a wealth of biometric information due to their highly detailed vascular structures and are frequently used in both medical and biometric identification systems. However, this critical data remains susceptible to unauthorized access, manipulation, and leakage, posing serious threats to patient privacy and healthcare integrity [103].

To address these challenges, robust encryption mechanisms are essential to ensure the confidentiality and integrity of medical image data [104]. Though widely employed, conventional cryptographic methods such as RSA, AES, and DES often fall short in real-time applications due to their computational complexity, large key sizes, and lack of adaptability to image structures [105]. Furthermore, these techniques typically do not exploit the image's inherent features or individuals' biometric traits, making them vulnerable in highly targeted or specialised attacks [106].

Chaos-based cryptographic systems have emerged as a promising solution in image security, particularly due to their high sensitivity to initial conditions, pseudorandom behavior, and ergodicity [107, 108]. These properties make chaotic systems particularly effective in image encryption, where spatial correlation and pixel redundancy are significant. Among chaotic functions, the logistic map stands out for its simplicity and efficiency, yet its conventional forms are becoming less resistant to modern cryptanalysis [104].

Recent developments in biometric cryptography aim to enhance traditional encryption systems by integrating unique human physiological traits, such as fingerprints, iris patterns, or retinal scans, into the cryptographic process. These traits are non-replicable, persistent over time, and offer an additional layer of identity-based protection [102]. Fusing biometric data with chaotic systems presents a synergistic approach, ensuring data-level encryption and identity-level security.

This chapter introduces a novel encryption framework explicitly designed for retinal images, employing a dual-biometric approach. The scheme integrates chaotic dynamic sequences generated through logistic maps with biometric features, the retinal image, and the fingerprint, as keys to a robust permutation-diffusion process. The key innovation lies in using the *hyperbolic tangent (tanh)* function as a nonlinear pre-processing step, enhancing the unpredictability of the encrypted output. The fingerprint is a secondary biometric key, tightly coupled with the retinal image to form a unique encryption signature for each subject.

The objectives of this study are as follows.

- To design a hybrid chaotic encryption algorithm tailored for retinal image protection using biometric keys;
- To evaluate the performance of the proposed method in terms of standard image encryption metrics such as correlation, Peak Signal-to-Noise Ratio (PSNR), and Mean Squared Error (MSE);
- To validate the robustness of the system through sensitivity and histogram analyses;
- To compare the proposed method against existing schemes and demonstrate its superiority in preserving data privacy and integrity.

Extensive simulations were conducted using MATLAB on the widely used DRIVE retinal image dataset, with the corresponding fingerprint inputs [109]. The results indicate that the proposed encryption framework provides enhanced security against statistical and differential attacks, while maintaining high image quality in the decryption phase.

The remainder of this chapter is organised as follows. Section 3.2 reviews the literature and foundational concepts in biometric encryption and chaotic systems. Section 3.3 details the mathematical preliminaries, including the hyperbolic tangent and logistic map functions. Section 3.4 describes the proposed encryption scheme and its implementation pipeline. Section 3.5 discusses the experimental setup and the evaluation metrics and presents and analyses the results, and finally, Section 3.7 concludes the chapter with insights and future directions.

3.2 Background and Related Work

Medical image security has become a critical field of research due to the sensitive nature of healthcare data and the growing use of digital imaging modalities. Retinal images, which capture the unique vascular patterns of the eye, serve both clinical and biometric purposes [108]. Ensuring the confidentiality and integrity of such images during storage and transmission is paramount to protecting patient privacy and complying with healthcare regulations.

Traditional encryption algorithms such as AES, RSA , and DES have been widely adopted in various domains. However, these methods often face challenges when applied directly to medical images. The large size of image data, coupled with inherent spatial redundancy and high correlation between neighbouring pixels, demands encryption schemes that can efficiently scramble image pixels while maintaining acceptable computational complexity.

Chaos theory has gained attention for addressing these challenges due to its inherent characteristics, including deterministic randomness, sensitivity to initial conditions, and complex dynamic behavior [110]. Chaotic maps, such as logistic, cubic, and quadratic maps, have been exploited to generate pseudorandom sequences that serve as encryption keys or perform pixel permutations and diffusion processes. These chaotic systems are particularly suitable for image encryption because their sensitivity ensures that even slight variations in initial parameters lead to drastically different encrypted outputs, thus enhancing security against brute-force and statistical attacks.

Despite their advantages, classical chaotic maps like the logistic map have demonstrated vulnerabilities under modern cryptanalysis, primarily due to predictable periodic windows and limited key space . Consequently, recent research has focused on improving chaotic encryption schemes by introducing novel nonlinear functions and hybrid chaotic systems to increase complexity and resistance to attacks [111].

Simultaneously, biometric cryptography has emerged as a promising paradigm that leverages unique physiological characteristics such as fingerprints, iris patterns, and retinal scans to enhance security. Unlike conventional passwords or keys, biometric traits are inherently tied to the individual, reducing the risk of unauthorized key sharing or loss. Several studies have proposed biometric-based encryption schemes that utilize fingerprint or iris features as cryptographic keys or to generate dynamic encryption parameters [**?**].

Combining biometric traits with chaotic encryption schemes creates a multi-layered defense mechanism. For example, using a retinal image as the data to be encrypted and a fingerprint as the encryption key binds the security process to two unique modalities of the same individual, significantly increasing the difficulty of unauthorized decryption [89]. This approach also mitigates the weaknesses of standalone chaotic systems by introducing additional entropy from biometric sources.

In retinal image encryption, the DRIVE database [109] is commonly used for benchmarking segmentation and encryption algorithms due to its standardized format and availability of annotated images. Several recent works have demonstrated the effectiveness of chaos-based encryption on retinal images, but most lack integration with multi-modal biometric keys or nonlinear pre-processing steps that enhance security [112].

This chapter builds upon this foundation by proposing a hybrid encryption scheme that combines chaotic logistic maps with a nonlinear hyperbolic tangent function and integrates a fingerprint biometric key. The scheme is designed to increase key space complexity, reduce correlation between encrypted and original images, and improve robustness against common cryptographic attacks.

3.3 Mathematical Preliminaries

This section presents the fundamental mathematical concepts and functions employed in the proposed encryption scheme. The two main components are the hyperbolic tangent function, which introduces nonlinearity, and the logistic map, which serves as the chaotic sequence generator.

3.3.1 Hyperbolic Tangent Function

The hyperbolic tangent function, denoted as $\tanh(x)$, is defined as the ratio of the hyperbolic sine to the hyperbolic cosine functions:

$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}, \tag{3.1}$$

e is the base of the natural logarithm (approximately 2.71828), and $x \in \mathbb{R}$ is the input variable.

The tanh function maps the real line to the interval $[-1, 1]$ and exhibits an S-shaped curve. This nonlinearity is beneficial in encryption as it helps diffuse the image pixel values across a bounded range, enhancing the unpredictability of the transformation.

The inverse of the hyperbolic tangent function, known as the hyperbolic arctangent or $\operatorname{atanh}(x)$, is used during the decryption phase to reverse the nonlinear transformation:

$$\operatorname{atanh}(x) = \frac{1}{2} \ln\left(\frac{1+x}{1-x}\right), \quad x \in (-1, 1), \tag{3.2}$$

where $\ln(\cdot)$ is the natural logarithm. This inverse function enables the recovery of the original image values after the nonlinear processing stage.

3.3.2 Chaotic Logistic Map

The logistic map is a simple yet widely studied nonlinear difference equation that exhibits chaotic behavior for certain parameter ranges. It is defined as:

$$x_{i+1} = r\, x_i(1 - x_i), \tag{3.3}$$

where $x_i \in (0, 1)$ is the state at iteration i, and r is the control parameter typically chosen in the interval $[3.98, 4]$ to ensure chaotic dynamics.

The logistic map generates a random sequence and is highly sensitive to initial conditions (x_0) and the control parameter (r). This sensitivity and unpredictability make it well-suited for generating pseudorandom sequences used as encryption keys or scrambling image pixels.

3.3.3 Properties Relevant to Encryption

The key properties of the hyperbolic tangent function and logistic map exploited in the encryption scheme are:

- **sensitivity to initial conditions:** Small variations in the input or parameters yield significantly different outputs, thwarting unauthorized decryption attempts.
- **Nonlinearity:** The tanh function introduces a nonlinear mapping of pixel intensities, which helps disperse statistical properties.
- **Bounded outputs:** Both $\tanh(x)$ and the logistic map outputs are confined within known ranges, facilitating normalization and stability in encryption and decryption.
- **Ergodicity and mixing:** The logistic map's chaotic behavior thoroughly mixes pixel positions and values during permutation and diffusion steps.

Together, these mathematical tools form the backbone of the chaotic encryption framework, ensuring robustness against cryptanalytic attacks and maintaining high data confidentiality levels.

3.4 Proposed Encryption Scheme

This section details the proposed chaotic retinal image encryption scheme that integrates biometric keys derived from fingerprints and retinal images. The scheme is structured around a permutation-diffusion framework enhanced by nonlinear preprocessing using the hyperbolic tangent function. The overall architecture is illustrated in Figure 3.1.

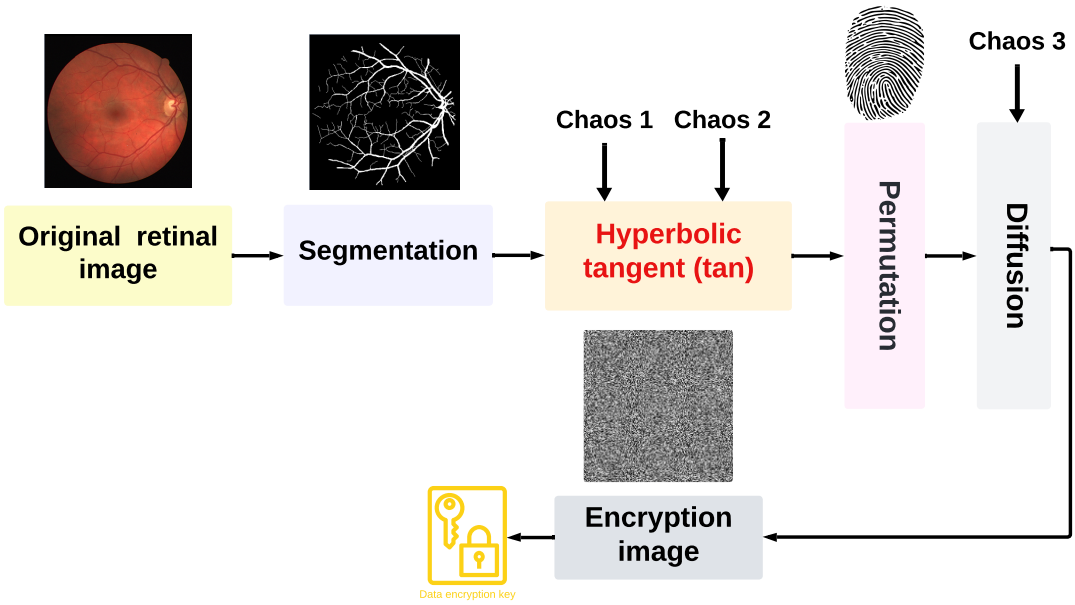


Figure 3.1: The proposed chaotic retinal image encryption scheme.

3.4.1 Overview

The encryption process begins with the segmentation and preprocessing of retinal images, which are then converted into vector forms. Simultaneously, the corresponding fingerprint image, the biometric key, is similarly processed into a vector. Three sequences are generated using logistic chaotic maps with carefully selected parameters to drive permutation and diffusion steps. Nonlinear transformation using the hyperbolic tangent function is applied to enhance security. Finally, a combination of permutation and XOR-based diffusion encrypts the image. The steps of the proposed method can be summarized as:

1. Segment and preprocess the retinal image and corresponding fingerprint.
2. Convert images into vectors V and V'.
3. Generate chaotic sequences v, u, C_2 using logistic maps.
4. Compute summation vector S and apply nonlinear transformation $S' = \tanh(S)$.
5. Generate permutation vector IX and permute S' to obtain X.
6. Perform XOR-based diffusion with C_2 to produce encrypted vector y.

Step 1: Image and Fingerprint Vectorization

Given an original retinal image I of dimensions $m \times n$, and its corresponding fingerprint image I', both images are preprocessed and segmented to remove noise and enhance features. Subsequently, each image is transformed into a one-dimensional vector:

$$V = \text{vec}(I) \in \mathbb{R}^{1\times(m\times n)}, \quad V' = \text{vec}(I') \in \mathbb{R}^{1\times(m\times n)},$$

where $\text{vec}(\cdot)$ denotes the vectorization operation.

Step 2: Generation of Chaotic Vectors

Using logistic maps with initial parameters (x_0, r_0) and (x_1, r_1), two chaotic vectors v and u of length $m \times n$ are generated:

$$v = \{v_k\}, \quad u = \{u_k\}, \quad k = 1, 2, \ldots, m \times n,$$

Where each element is computed iteratively via:

$$v_{k+1} = r_0\, v_k(1 - v_k), \quad u_{k+1} = r_1\, u_k(1 - u_k),$$

with initial conditions $v_1 = x_0$ and $u_1 = x_1$.

A third chaotic vector C_2 is also generated using a third logistic map with parameters (x_2, r_2).

Step 3: Summation and Nonlinear Transformation

The vectors V, V', v, u, and two constant vectors C_0, C_1 (initialized constants or keys) are combined into a summation vector S:

$$S = V + V' + v + u + C_0 + C_1,$$

After summation, the nonlinear hyperbolic tangent function is applied element-wise to produce S':

$$S' = \tanh(S).$$

This nonlinear mapping increases the diffusion of pixel values, improving encryption strength.

Step 4: Permutation

A permutation vector IX is constructed by sorting S' in ascending order. Using IX, the vector S' is rearranged to form a permuted vector X:

$$X = S'_{IX}.$$

This step scrambles the pixel positions, reducing spatial correlation and further obfuscating the image structure.

Step 5: Diffusion via XOR Operation

The final encrypted vector y is obtained through a diffusion process combining the third chaotic vector C_2 and the permuted vector X using XOR operations:

$$y_k = \begin{cases} C_{2_k} \oplus S_{1_k}, & k = 2 \\ C_{2_k} \oplus S_{1_k} \oplus y_{1_{k-1}}, k = 1, 2, \ldots m \times n \end{cases} \tag{3.4}$$

where $\oplus$ denotes the bitwise XOR operator.

This diffusion step ensures that each element of the encrypted vector depends on all previous elements, significantly increasing the complexity and sensitivity to key changes.

This process results in a securely encrypted retinal image tightly bound to the biometric fingerprint key, making unauthorized decryption computationally infeasible. Decryption involves applying the inverse operations in reverse order, including the use of the inverse hyperbolic tangent function atanh$(\cdot)$ to recover the original image from the encrypted vector, assuming possession of the correct biometric key and chaotic parameters.

3.5 Implementation of the Proposed Scheme

This section describes the practical aspects of implementing the proposed chaotic retinal image encryption scheme. It includes details about the software environment, datasets, pre-processing steps, and parameter settings used during the experimentation.

3.5.1 Software Environment

The encryption algorithm was implemented and tested using MATLAB R2016b, which was chosen for its extensive image processing and mathematical computing capabilities. Simulations were conducted on a personal computer equipped with an Intel Core i7 processor, 16 GB of RAM, and running Windows 10. The choice of MATLAB facilitated rapid prototyping and reproducibility of results.

3.5.2 Dataset

The widely used DRIVE (Digital Retinal Images for Vessel Extraction) database [109] served as this study's source of retinal images. The database comprises 20 color retinal images of size 768×584 pixels with a 45-degree field of view, captured using a Canon CR5 non-mydriatic camera. The photos include diverse cases with varying levels of diabetic retinopathy and were accompanied by ground truth vessel annotations.

Corresponding fingerprint images were collected or synthetically generated as biometric keys. Fingerprint pre-processing involved alignment and resizing to match the retinal image vector dimensions, ensuring compatibility for combined encryption.

3.5.3 Parameter Selection

The chaotic logistic maps utilised three sets of initial conditions and control parameters:

$$(x_0, r_0) = (0.35, 3.9955), \quad (x_1, r_1) = (0.45, 3.9955), \quad (x_2, r_2) = (0.25, 3.9955).$$

These parameters were carefully chosen to operate within the chaotic regime of the logistic map, maximising the unpredictability of generated sequences. The constants C_0 and C_1 used in the summation step were initialised to fixed random vectors for consistent encryption behaviour.

All simulations were run multiple times to assess stability and repeatability. The execution time for encrypting and decrypting images of size 768×584 was measured, revealing processing times suitable for offline or near real-time applications.

3.6 Results and Discussion

This section presents the outcomes of the proposed encryption scheme, with extensive analysis based on multiple performance metrics and security evaluations. All experiments were conducted using MATLAB 2016 on a personal laptop, with retinal images from the DRIVE database and corresponding fingerprint inputs.

3.6.1 Performance Metrics

Table 3.1 summarizes the key metrics, including correlation coefficient (CORR), peak signal-to-noise ratio (PSNR), and mean squared error (MSE), computed over 20 retinal images. They are defined as follows:

$$\text{corr}_{I_0 I_r} = \frac{\text{cov}\,(I_0, I_r)}{\sqrt{D_{l_0}} \times \sqrt{D_{l_r}}} \tag{3.5}$$

$$E\left(I_0\right) = 1/(m \times n) \times \sum_{i=1}^{N} I_{0_i} \tag{3.6}$$

$$E\left(I_0\right) = 1/(m \times n) \times \sum_{i=1}^{m \times n} \left(I_{0_i} - E\left(I_0\right)\right)^2 \tag{3.7}$$

$$\begin{aligned} &\operatorname{cov}\left(I_0, I_r\right) \\ &= \frac{1}{(m \times n) \times \sum_{i=1}^{m \times n} \left(I_{0_i} - E\left(I_0\right) \times \left(I_{r_i} - E\left(I_r\right)\right)\right)} \end{aligned} \tag{3.8}$$

$$PSNR = 10 \log_{10}\left(d^2/MSE\right) \tag{3.9}$$

$$MSE = (1/m \times n) \times \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(I_0(i,j) - I_r(i,j)\right)^2 \tag{3.10}$$

With a signal dynamic range of d=255 (representing values within 8 bits) and considering I_0 and I_r of dimensions m × n.
The proposed method shows a marked improvement in structural decorrelation between encrypted and original images, evidenced by a lower average CORR of 0.0018 compared to 0.0036 in the technique of [113].

PSNR values remain nearly identical for both methods, with a slight advantage to the proposed approach (-43.3680 dB vs. -43.3772 dB), indicating minimal loss in image quality upon decryption. Similarly, MSE values show marginal improvement, suggesting reduced distortion.

These results confirm the proposed scheme's capability to effectively obscure original image content while preserving decrypted image fidelity, which is crucial for medical applications.

Table 3.1: Performance metrics results.

Methods	Method used on [113]			**Proposal Method**		
Images	CORR	PSNR	MSE	CORR	PSNR	MSE
Image01	0.0055	-43.3772	2.1803e+04	0.0006	-43.3619	2.1725e+04
Image02	-0.0057	-43.3607	2.1727e+04	0.0073	-43.3551	2.1700e+04
Image03	-0.0054	-43.3424	2.1623e+04	-0.0016	-43.3720	2.1771e+04
Image04	0.0066	-43.3692	2.1784e+04	-0.0029	-43.3550	2.1712e+04
Image05	0.0051	-43.3678	2.1766e+04	0.0050	-43.3540	2.1697e+04
Image06	-0.0014	-43.3569	2.1705e+04	-0.0014	-43.3734	2.1787e+04
Image07	-0.0053	-43.3677	2.1761e+04	-0.00018	-43.3568	2.1707e+04
Image08	0.0042	-43.3972	2.1915e+04	0.0023	-43.3754	2.1805e+04
Image09	-0.0032	-43.3662	2.1752e+04	0.0031	-43.3623	2.1732e+04
Image10	-0.0059	-43.3553	2.1694e+04	0.0063	-43.3805	2.1821e+04
Image11	0.00016	-43.3460	2.1639e+04	-0.00035	-43.3553	2.1685e+04
Image12	-0.0041	-43.3615	2.1727e+04	0.0024	-43.3742	2.1790e+04
Image13	0.000378	-43.3695	2.1767e+04	0.0024	-43.3383	2.1611e+04
Image14	0.0014	-43.3575	2.1715e+04	0.0056	-43.3607	2.1732e+04
Image15	-0.0031	-43.3419	2.1632e+04	0.0021	-43.3806	2.1826e+04
Image16	-0.0020	-43.3334	2.1601e+04	0.0024	-43.3814	2.1841e+04
Image17	0.0009	-43.3730	2.1787e+04	0.0028	-43.3600	2.1723e+04
Image18	-0.0073	-43.3609	2.1726e+04	-0.0043	-43.3857	2.1850e+04
Image19	0.0006	-43.3753	2.1798e+04	-0.0042	-43.3563	2.1703e+04
Image20	-0.00475	-43.3674	2.1753e+04	-0.0028	-43.3648	2.1741e+04
Average	0.0036	-43.3772	2.1774e+04	**0.0018**	**-43.3680**	**2.1770e+04**

3.6.2 Histogram Analysis

Figure 3.2 shows histograms of the original retinal images alongside their encrypted versions. The original images have distinct histogram patterns reflecting the natural structures like vessels and tissues, which attackers could exploit. However, the encrypted images have nearly uniform histograms, resembling white noise, indicating that pixel intensities are well randomized.

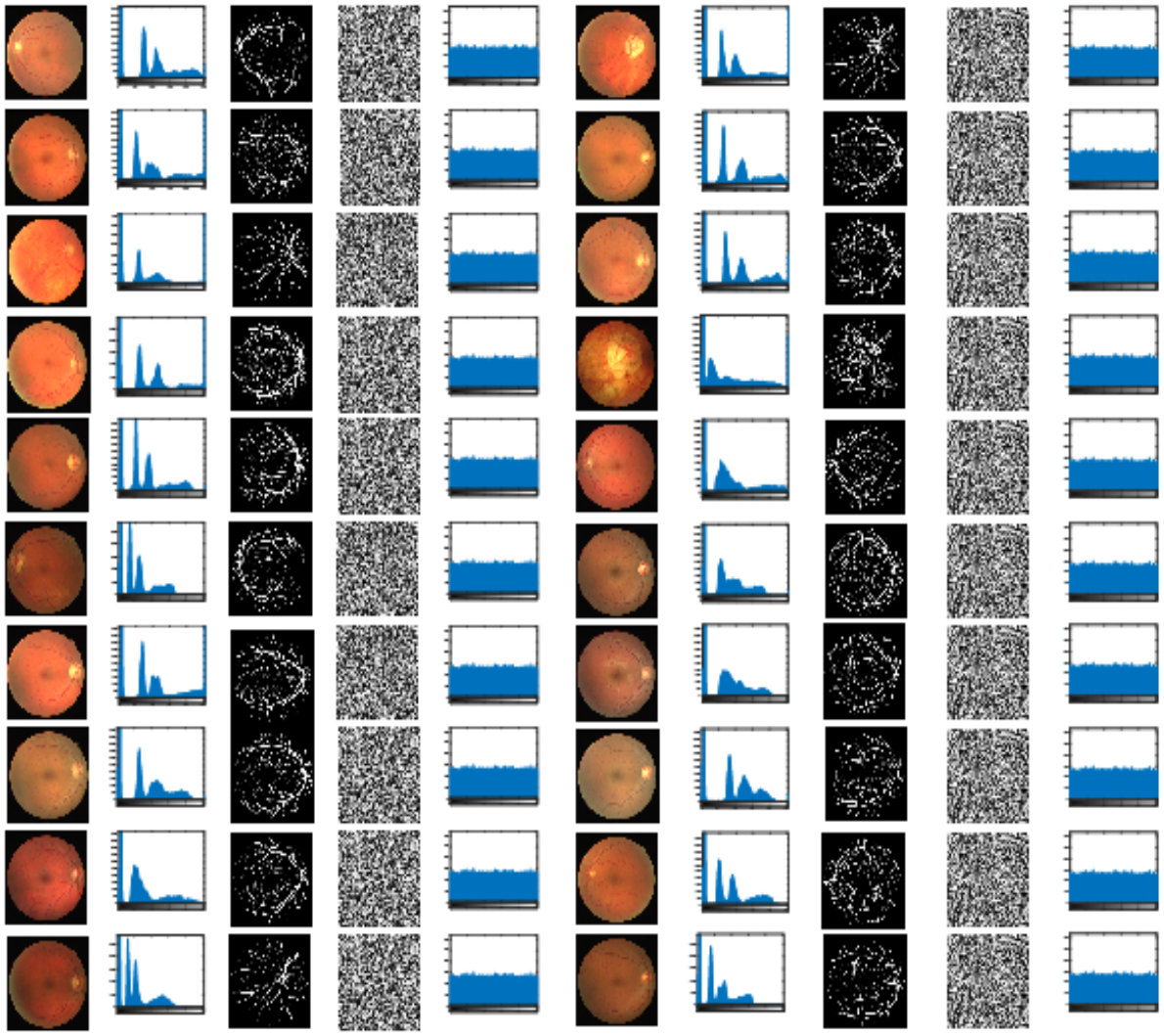


Figure 3.2: Results of the encryption process.

This uniform distribution means that the encryption disrupts all statistical patterns, making it practically impossible to gain any meaningful information through histogram analysis. In other words, attackers can't use simple statistical clues to break the encryption, highlighting the proposed scheme's strength and effectiveness.

3.6.3 Sensitivity Analysis

An essential feature of any secure encryption scheme is its sensitivity to the encryption key. In our method, the key consists of the chaotic logistic map parameters $(x_0, r_0, x_1, r_1, x_2, r_2)$ combined with the biometric fingerprint f_0. Even a minute change in any component of this key should lead to a drastically different encrypted image, making unauthorized decryption practically impossible.

To verify this, we performed a sensitivity analysis by introducing tiny perturbations on the order of 10^{-15} to 10^{-16} to individual chaotic map parameters while keeping all others constant. The results showed that such tiny changes caused the encrypted output

to differ entirely from that produced with the original key.

This high sensitivity ensures the robustness of the encryption process against brute-force or approximate key attacks. Furthermore, if the wrong fingerprint is used during decryption, the output image becomes unintelligible noise, reinforcing the importance of biometric binding for security.

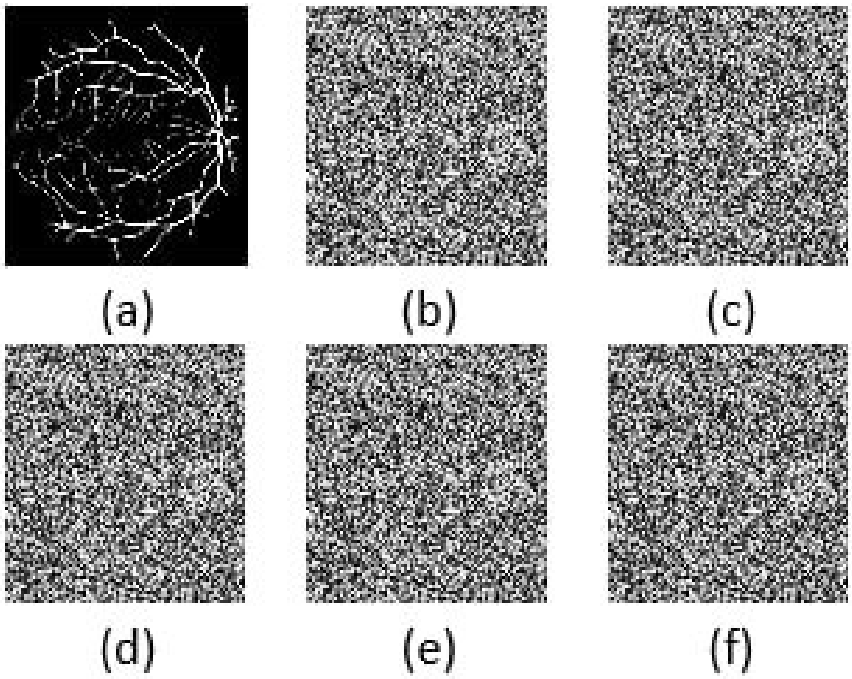


Figure 3.3: Sensitivity analysis: (a) segmented test image $(b)(x')_0 = x_0 + (10))^(- 16)(c)(r')_0 = r_0 + (10)^(- 15)(d)(x')_1 = x_1 + (10)^(- 16)(e)(r')_1 = r_1 + (10)^(- 15)(f)(x')_2 = x_2 + (10)^(- 16)$.

Figure 3.3 illustrates examples of encrypted images generated with slight variations in key parameters, demonstrating the scheme's extreme key sensitivity.

3.6.4 Key Space Analysis

A sufficiently large key space safeguards an encryption scheme against brute-force attacks. The key space size reflects the number of possible keys an attacker must try to break the encryption by exhaustive search.

In our scheme, the key includes six chaotic map parameters $(x_0, r_0, x_1, r_1, x_2, r_2)$ and a biometric fingerprint f_0. Based on the sensitivity analysis, the parameters x_i and r_i have precisions on the order of 10^{-16} and 10^{-15}, respectively. The fingerprint adds complexity with a precision equivalent to 2^{28} possibilities.

Combining these yields a key space estimated as:

$$(10^{15} \times 10^{15} \times 10^{15} \times 10^{16} \times 10^{16} \times 10^{16}) \times 2^{28} \approx 2^{287}.$$

This expansive key space significantly exceeds the commonly accepted minimum threshold of 2^{100} for secure encryption, making brute-force attacks computationally infeasible with current technology.

Therefore, the proposed encryption scheme offers a high level of security due to its large and complex key space, which is strengthened further by biometric integration.

3.6.5 Attacks with Wrong Fingerprint

The biometric nature of the encryption key is crucial for the system's security. Each retinal image is paired uniquely with its owner's fingerprint, which forms part of the encryption key. To assess the importance of this biometric binding, we performed decryption tests using incorrect fingerprints.

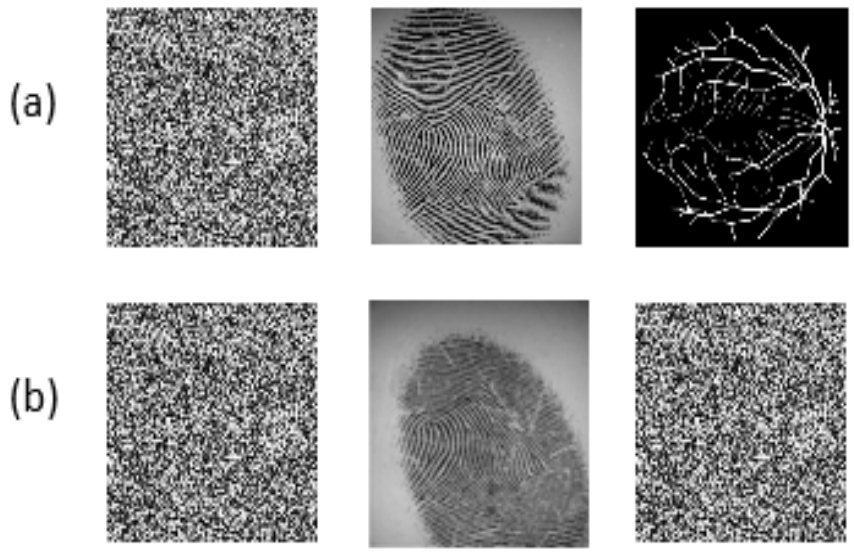


Figure 3.4: Sensitivity analysis:(a) segmented test image $(b)(x')_0 = x_0 + (10))^(- 16)(c)(r')_0 = r_0 + (10)^(- 15)(d)(x')_1 = x_1 + (10)^(- 16)(e)(r')_1 = r_1 + (10)^(- 15)(f)(x')_2 = x_2 + (10)^(- 16)$.

Figure 3.4 shows the results of decrypting an encrypted retinal image with (a) the correct fingerprint and (b) an incorrect fingerprint. Using the correct fingerprint yields a clear, recognizable image. However, decryption with the wrong fingerprint produces a chaotic, unintelligible output.

This experiment highlights the critical role of the fingerprint in the encryption key, confirming that unauthorized users lacking the exact biometric cannot recover the original

image. This biometric dependency adds a strong layer of security beyond traditional key-based encryption.

3.7 Conclusion

This chapter presented a novel chaotic encryption scheme for retinal images that leverages biometric keys derived from fingerprint data. By integrating nonlinear pre-processing via the hyperbolic tangent function with chaotic logistic maps, the proposed method achieves a robust permutation-diffusion encryption framework.

Extensive experiments using the DRIVE retinal image database demonstrated the scheme's effectiveness in securely encrypting images while preserving high-quality decrypted outputs. Performance metrics such as correlation coefficient, PSNR, and MSE confirmed the superior decorrelation and low distortion compared to existing methods.

Security analyses, including histogram uniformity, key sensitivity, key space evaluation, and biometric binding, reinforced the system's robustness against common cryptographic and brute-force attacks. The biometric fingerprint acts as a critical key component, preventing unauthorized decryption even if other parameters are compromised.

Overall, the proposed approach provides a strong and practical solution for safeguarding sensitive retinal images in telemedicine and biometric applications. Future work could explore real-time implementation, integration with other biometric modalities, and optimization for resource-constrained devices.

Chapter 4

New Composite Chaotic Map for Image Encryption in Cybersecurity

4.1 Introduction

Recently, The rapid advancement of digital technologies has revolutionized the way information is stored, transmitted, and processed. Among various data formats, digital images hold a prominent place due to their widespread applications in communication systems, medical diagnostics, military surveillance, and multimedia entertainment [114]. However, the increasing reliance on image data across distributed networks and cloud platforms raises critical concerns about data security and privacy. Images transmitted over insecure channels are vulnerable to unauthorised access, interception, and tampering, which can lead to severe consequences ranging from privacy violations to the compromise of sensitive information [115].

Traditional encryption algorithms, such as the AES and the RSA algorithm, have been widely adopted to secure digital data. Despite their proven effectiveness in encrypting text and binary data, these conventional methods are often not optimal for image data [116]. The inherent characteristics of images—such as large data size, high pixel correlation, and redundancy—require specialised encryption schemes that can efficiently and securely handle visual information without excessive computational overhead [117].

Chaos theory has emerged as a promising foundation for image encryption schemes owing to its distinctive properties, including high sensitivity to initial conditions, deterministic randomness, and ergodicity [118]. Chaotic systems produce pseudo-random sequences that are highly unpredictable, making them suitable for generating encryption keys and scrambling image pixels. Early chaotic maps, including the logistic, quadratic, and cubic maps, have been successfully employed to design image encryption algorithms [89, 119]. However, these classical chaotic maps often have limitations such as narrow chaotic intervals, predictability in specific parameter ranges, and relatively small key spaces [104]. These weaknesses reduce their resistance against modern cryptanalytic at-

tacks and limit their practical security [106].

To address these challenges, this chapter proposes an Improved Composite Chaotic Map (ICCM) that integrates the quadratic and cubic chaotic maps to leverage both advantages while mitigating their shortcomings [120]. The ICCM exhibits a wider chaotic range and enhanced complexity, providing stronger security guarantees. To further augment the encryption process, the ICCM is combined with the Fractional Fourier Transform (FrFT) and Double Random Phase Encoding (DRPE) techniques, which introduce additional layers of confusion and diffusion, thereby strengthening the cryptosystem [121].

The proposed encryption framework is designed to provide a secure, efficient, and robust method for image encryption applicable to cybersecurity domains. It offers ample key space, high sensitivity to initial conditions, and resistance to various attack models, including statistical and differential cryptanalysis. Comprehensive experiments are conducted to validate the performance and security of the scheme using standard image datasets. Metrics such as the correlation coefficient, peak signal-to-noise ratio, mean squared error, pixel change rate, and unified average changing intensity are utilized to quantify encryption quality and robustness [122].

This chapter is organised as follows: Section 4.2 reviews fundamental concepts in chaotic systems and related encryption approaches. Section 4.3 introduces the mathematical foundations of the ICCM, including its dynamical properties. Section 4.4 details the proposed image encryption algorithm that integrates ICCM with FrFT and DRPE. Section 4.5 presents experimental results and security analyses. Finally, Section 4.6 concludes the chapter and outlines future research directions.

4.2 Background and Related Works

Image encryption based on chaotic systems has become a vibrant research area due to the excellent cryptographic properties of chaos, such as sensitivity to initial conditions, unpredictability, and complex dynamic behavior [103, 107]. Early chaotic maps, such as the logistic, quadratic, and cubic maps, have been widely used for image encryption [119]. These maps provide deterministic pseudo-random sequences that can be used for pixel permutation and diffusion, key operations in image encryption algorithms.

However, classical chaotic maps have inherent drawbacks. The logistic map, for example, exhibits chaotic behavior only in limited parameter ranges, with periodic windows where chaos is lost, making it vulnerable to cryptanalysis [104]. Similarly, while more complex, quadratic and cubic maps suffer from small key spaces and predictable regions under certain conditions [108]. These limitations motivate the design of composite or hybrid chaotic maps that combine multiple chaotic functions to enhance chaotic properties and expand the key space.

Recent studies have introduced composite chaotic maps that blend multiple simple

maps to generate sequences with improved randomness and complexity. For instance, a composite of quadratic and cubic maps was proposed to address weaknesses in individual maps by increasing the Lyapunov exponent and chaotic interval [120]. These enhanced chaotic maps have shown promise in producing more secure and robust encryption schemes.

In parallel, transform-domain encryption methods such as those based on the Fractional Fourier Transform (FrFT) and Double Random Phase Encoding (DRPE) have gained attention. FrFT generalizes the classical Fourier transform by adding a fractional order parameter, increasing the key space and providing greater encryption flexibility [121]. DRPE applies random phase masks in both the input and Fourier domains, introducing significant confusion and diffusion to encrypted images [123].

Combining chaotic maps with transform-domain techniques yields hybrid encryption frameworks that benefit from the strengths of both approaches. The chaotic sequences control key parameters or mask generation, while the transform provides a robust domain for scrambling and diffusion. This combination enhances security against attacks, including statistical, differential, and brute-force [112].

Despite these advances, existing schemes often fail to fully leverage the potential of composite chaotic maps in the transform domain. They do not comprehensively analyze the dynamical properties, such as Lyapunov exponents and entropy measures, which are crucial for understanding security strengths. This chapter aims to fill this gap by proposing an Improved Composite Chaotic Map (ICCM) integrated with FrFT-DRPE encryption, accompanied by an extensive theoretical and experimental evaluation. However, many existing approaches suffer from limited chaotic range, low key sensitivity, or vulnerability to statistical attacks. Table 4.1 provides a comparative analysis of prior works, highlighting their limitations and the improvements introduced by the proposed ICCM-based scheme.

Table 4.1: Comparison of existing schemes with the proposed ICCM.

Reference	**Approach**	**Limitations**	**Proposed ICCM Improvements**
Ref. [92]	Pixel scrambling + FrFT-DRPE	Limited chaotic range, fixed parameters	Expanded chaotic range, dynamic parameterization
Ref. [42]	MPD-FrFT with a piecewise linear chaotic map (PLCM)	Low key sensitivity	Enhanced key sensitivity (10^{-15} precision)
Ref. [124]	Hybrid chaotic framework	Vulnerable to statistical attacks	Uniform histogram, NIST-validated randomness
Ref. [43]	Simple chaotic dynamics	Narrow chaotic regions, predictability	Full-range chaos, hybrid complexity
Ref. [100]	Logistic map for audio encryption	Not optimized for images	Tailored for images, integrated with FrFT-DRPE

4.2.1 Our Contributions

This chapter presents a series of novel contributions in chaos-based image encryption, combining theoretical advancements in dynamical systems with practical enhancements to encryption frameworks. The key contributions can be summarized as follows:

1. **Development of a Full-Range Chaotic System Independent of Control Parameter Constraints.** One of the significant limitations of classical chaotic systems, such as the logistic, quadratic, and cubic maps, is that they only exhibit chaotic behavior within narrowly confined ranges of their control parameters. For instance, chaotic behavior in the logistic map is typically observed for $r \in [3.98, 4.0]$, while quadratic and cubic maps have even more limited chaotic intervals, such as $r \in [1.8, 2.0]$ [104, 119]. These constraints reduce the flexibility and security of encryption systems relying on such maps. The proposed Improved Composite Chaotic Map (ICCM) addresses this issue by achieving chaotic dynamics across the entire parameter space. This full-range chaotic behavior ensures greater flexibility in key generation, enhances the unpredictability of the encryption keys, and allows the system to maintain chaotic behavior under a much wider variety of operating conditions, making it more resilient and adaptable in practical applications.

2. **Introduction of a Parameterised Composite Chaotic System with Enhanced Dynamical Complexity.** Inspired by the structural design of classical chaotic maps, the proposed ICCM introduces two tunable control parameters, denoted r_{01} and r_{02}, each defined over the positive real domain, $[0, \infty[$. Unlike fixed-parameter maps, this parametrisation grants the system more configurability and complexity. The two-parameter control enables greater modulation of the system's behaviour, resulting in richer bifurcation structures, higher Lyapunov exponents, and more uniform entropy across the dynamic range. These improvements are essential in cryptographic applications, where sequence unpredictability and sensitivity to initial conditions directly translate to better security. Simulation results confirm that the ICCM produces pseudo-random sequences with strong statistical properties, making it a powerful core for key generation and control of cryptographic operations.

3. **Design of a Novel Image Encryption Framework Based on ICCM and Transform-Domain Processing.** Building on the chaotic capabilities of ICCM, a complete image encryption scheme is developed, combining spatial-domain techniques (such as pixel reorganization and permutation-diffusion) with transform-domain encryption (via the Fractional Fourier Transform and Double Random Phase Encoding). This hybrid approach ensures strong diffusion and confusion properties, two pillars of cryptographic security. The system dynamically generates keys

and scrambling patterns using ICCM-generated sequences, resulting in highly secure ciphertexts that resist cryptanalytic attacks, including known-plaintext and chosen-ciphertext attacks. The encryption algorithm is computationally efficient, maintaining low processing overhead, which is especially beneficial for real-time or embedded applications in IoT and telemedicine.

4. **Demonstration of Exceptional Key sensitivity and High Security Robustness.** The proposed system shows an exceptionally high sensitivity to all cryptographic keys, including initial conditions and ICCM control parameters. Minor deviations in any key component result in entirely different decrypted outputs, ensuring that unauthorized users cannot reconstruct even partial image content. Key deviation experiments, differential attack analysis, and histogram evaluations validate this sensitivity. Furthermore, the system demonstrates robustness to brute-force attacks through a vast key space, which far exceeds standard cryptographic security benchmarks. These results affirm the proposed framework's ability to provide high confidentiality, integrity, and resistance to statistical and differential cryptanalysis.

4.3 Mathematical Foundations

A thorough understanding of the mathematical structures underlying chaotic systems is essential for designing and analyzing secure image encryption schemes. This section lays the theoretical groundwork for the proposed framework by first revisiting classical chaotic maps, namely, the quadratic and cubic maps, which serve as the conceptual and mathematical basis for the newly proposed Improved Composite Chaotic Map (ICCM). These foundational maps have long been employed in cryptographic applications due to their nonlinear dynamics and sensitivity to initial conditions. Yet, their parameter constraints and chaotic range limitations motivate the development of more robust alternatives.

The section introduces the ICCM, a hybrid chaotic system that integrates and extends the behaviors of quadratic and cubic maps to produce richer chaotic dynamics. The construction of ICCM is accompanied by a detailed explanation of its mathematical formulation, control parameters, and switching logic. The map's behavior is evaluated through a series of established chaos diagnostics, including bifurcation diagrams, Lyapunov exponents, and entropy measures. These collectively demonstrate the system's ability to generate unpredictable and highly sensitive chaotic sequences.

Furthermore, sensitivity analysis examines the system's dependence on initial conditions and parameters, a crucial property for ensuring cryptographic strength. These analyses validate the suitability of ICCM as a secure key generator and highlight its advantages over conventional single-map systems.

The comprehensive exploration of these mathematical tools forms the backbone of the encryption process described in subsequent sections. By establishing the chaotic robustness and enhanced complexity of ICCM, this section ensures a deep theoretical foundation upon which the proposed image encryption algorithm is constructed.

4.3.1 Classical Chaotic Maps

This subsection discusses the mathematical formulations and dynamical behaviors of two widely studied chaotic maps: the quadratic and cubic maps, which serve as a foundation for more advanced systems, such as the Improved Composite Chaotic Map (ICCM) [43]. These maps are known for exhibiting rich nonlinear dynamics and a relatively wide range of chaotic behavior, making them valuable tools in secure communications and image encryption.

The bifurcation diagrams of these maps reveal complex patterns and transitions from stable to chaotic regimes as control parameters vary. These chaotic regions, often visualized as dense, shadowed bands in the bifurcation space, underscore the system's sensitivity to initial conditions, a hallmark feature of chaotic systems and a critical requirement for robust encryption mechanisms [43].

Such sensitivity implies that infinitesimal changes in initial values lead to diverging outcomes over successive iterations, thereby generating pseudo-random sequences that are practically impossible to predict without exact initial conditions. This characteristic is instrumental in constructing secure cryptographic systems, where unpredictability and non-reproducibility form the backbone of confidentiality.

The mathematical definitions of the quadratic and cubic maps are given below, as detailed in [43]:

$$x_{n+1} = U(x_0, r_{01}) = r_{01} - x_n^2, \tag{4.1}$$

$$x_{n+1} = U(x_0, r_{02}) = r_{02} \cdot x_n \cdot (1 - x_n^2), \tag{4.2}$$

where r_{01} and r_{02} are the control parameters, x_0 is the initial value, and n is the iteration index.

Figure 4.1 illustrates both maps' bifurcation diagrams and Lyapunov exponent plots. These visual tools demonstrate the presence of strong chaotic zones and validate their utility in designing secure key generators.

4.3.2 The Improved Composite Chaotic Map (ICCM)

In digital communication and multimedia security, image encryption plays a pivotal role in safeguarding the confidentiality and integrity of visual data. However, due to its large

volume, high redundancy, and correlation among adjacent pixels, conventional cryptographic methods such as AES and RSA often struggle when directly applied to image data. Chaotic cryptography, by contrast, offers an attractive alternative due to its intrinsic properties—such as high sensitivity to initial conditions, pseudo-random behavior, and ergodicity—which are well-suited for encryption tasks [125].

To overcome the limitations of single-function chaotic maps and enhance the cryptographic strength of image encryption schemes, this work introduces a novel Improved Composite Chaotic Map (ICCM). This system is derived from combining modified quadratic and cubic chaotic functions [126]. The integration is carefully designed to leverage the individual strengths of both maps, producing a system with broader chaotic intervals, higher entropy, and increased key sensitivity.

The ICCM distinguishes itself from classical maps by incorporating two independent control parameters, r_{01} and r_{02}, both of which contribute to the system's chaotic behavior across a wide range. This parameterization enables finer control over the dynamic response and significantly expands the feasible key space—an essential factor in resisting brute-force attacks.

The mathematical formulation of the ICCM is given by:

$$x_{n+1} = \left[r_{02} \cdot (r_{01} - e^{x_n^2}) \cdot \left(1 - (r_{01} - e^{x_n^2})^2\right) \right] \bmod 1, \tag{4.3}$$

where $x_0 \in (0, 1)$ is the initial value, r_{01} and r_{02} are the control parameters of the ICCM, and mod1 ensures that the output remains within the interval $[0, 1]$. The exponential term $e^{x_n^2}$ introduces a nonlinearity that greatly enhances unpredictability and prevents the generation of repeatable patterns.

Experimental evaluations of ICCM reveal superior chaotic behavior compared to its constituent maps, as evidenced by higher Lyapunov exponents, denser bifurcation structures, and stronger statistical randomness. These properties are crucial in generating high-quality pseudo-random sequences, which form the core of the proposed image encryption framework.

4.3.3 Evaluation of ICCM Chaotic Behavior

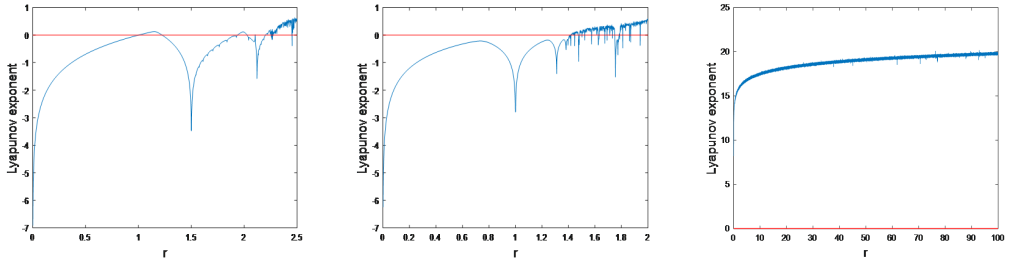
Before integrating the Improved Composite Chaotic Map (ICCM) into an encryption framework, it is essential to evaluate its dynamical behavior quantitatively. The strength and unpredictability of the chaotic sequence generated by ICCM are measured using three standard tests: the Lyapunov exponent, the bifurcation diagram, and Kolmogorov entropy. These metrics comprehensively understand the system's sensitivity, complexity, and entropy—key properties for secure cryptographic applications.

4.3.3.1 Lyapunov Exponent

Lyapunov Exponents are fundamental in verifying the chaotic behaviour of dynamical systems. A system is considered chaotic if it exhibits at least one positive Lyapunov Exponent (LE). This exponent quantifies the average rate of divergence or convergence of nearby trajectories in the system and is formally defined as follows [43]:

$$LE = \lim_{m\to\infty} \frac{1}{m} \sum_{n=1}^{m-1} \ln \left| f'\left(x_n\right) \right| \tag{4.4}$$

Here, f' represents the derivative of the underlying chaotic map, and x_n denotes the system's state at iteration n. For a chaotic map of dimension m, there are m Lyapunov Exponents.



(a) (b) (c)

Figure 4.1: Lyapunov exponent diagrams for (a) Cubic, (b) Quadratic, (c) ICCM maps.

In the case of a one-dimensional map, the presence of one positive Lyapunov exponent (LE) confirms the chaotic nature of the system.

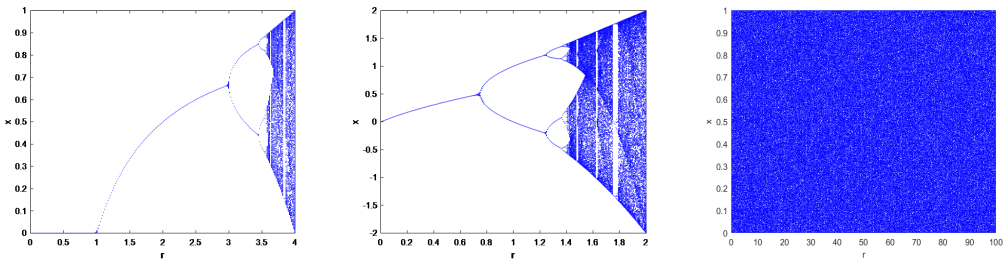
Table 4.2: Lyapunov exponent values of different chaotic maps.

Chaotic Map	LE Values
Ref. [127]	3.5317
Zigzag map [128]	≈4.9020
Logistic 1D map [128]	≈5.2247
Tent map [128]	5.2145
Xingyuan [129]	≈7
Ref. [130]	6.2402
Ref. [131]	14.250
Ref. [100]	≈19
ICCM	≈21.42

4.3.3.2 Bifurcation Diagram

The bifurcation diagram provides a visual representation of how the ICCM output evolves as the control parameter is varied. This diagram helps identify the system's stable, periodic, and chaotic regions. Chaotic or encryption should demonstrate a wide chaotic range with few periodic windows.

As shown in Figure 4.2, the ICCM shows a rich bifurcation structure with high-density chaotic regions, especially when the parameters are tuned within operational limits. Compared to classical maps, the ICCM exhibits an extended chaotic domain, ensuring robust unpredictability during key generation.



(*a*) (*b*) (*c*)

Figure 4.2: Bifurcation diagrams for (a) Cubic, (b) Quadratic, (c) ICCM maps.

4.3.3.3 Kolmogorov Entropy (KE)

Kolmogorov entropy, also referred to as metric entropy, is a fundamental measure of the unpredictability and complexity of a dynamical system. It quantifies the rate at which a system generates new information or loses predictability over time. Mathematically, it is defined as:

$$H_{KE} = \sum_{\lambda_n > 0} \lambda_n, \tag{4.5}$$

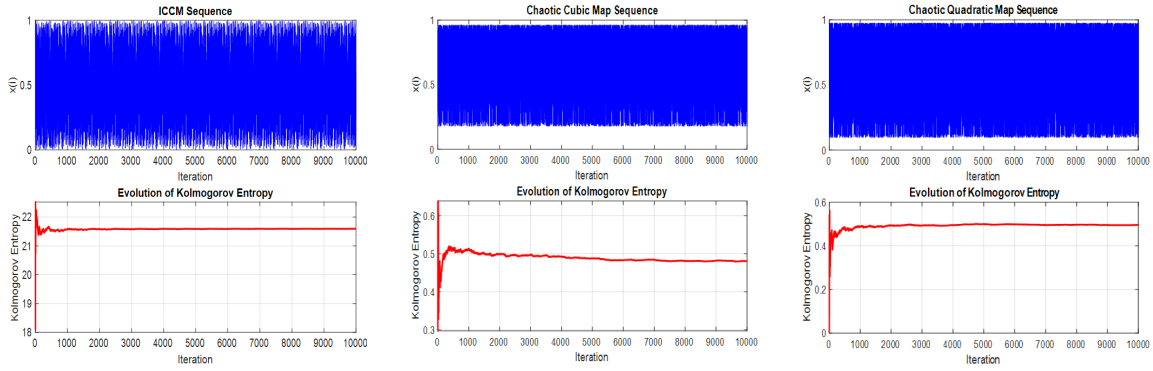
Where λ_n represents the Lyapunov exponents (LEs), which quantify the average exponential rates of divergence or convergence of nearby trajectories in the system's phase space. This relationship, known as Pesin's identity, establishes a direct link between Kolmogorov entropy and the chaotic nature of a system. Specifically, KE aggregates the contributions of the largest expanding directions (positive λ_n), reflecting the degree of randomness and sensitivity to initial conditions.

A higher Kolmogorov entropy value signifies increased unpredictability, meaning that even slight variations in the initial state lead to trajectories that diverge exponentially. This property makes KE an essential metric for evaluating the strength of chaos in cryptographic applications and encryption algorithms.

In our study, the Kolmogorov entropy analysis was conducted to assess the chaotic behavior of the proposed ICCM approach compared to classical chaotic maps, including the

quadratic and cubic maps. The computed KE values confirm the superior chaotic properties of ICCM, with a significantly higher entropy value of $KE = 21.5923$, demonstrating enhanced complexity and randomness.

Figure 4.3 presents the Kolmogorov entropy visualizations for different chaotic maps, illustrating the increased entropy and complexity of ICCM in comparison to conventional chaotic functions. It is demonstrated that the ICCM exhibits a significantly higher entropy, indicating stronger chaotic behavior and enhanced security for cryptographic applications.



(a) ICCM (b) Cubic Map (c) Quadratic Map

Figure 4.3: Kolmogorov Entropy comparison: (a) ICCM, (b) Cubic map, and (c) Quadratic map.

These properties collectively validate the ICCM as a robust pseudo-random sequence generator suitable for cryptographic systems, paving the way for its integration into the proposed encryption framework.

4.3.4 Initial Value Sensitivity Test

A fundamental characteristic of chaotic systems is their extreme sensitivity to initial conditions. This property implies that two trajectories originating from initial values that differ by an infinitesimally small amount will diverge exponentially over time, producing completely distinct outcomes. This phenomenon, often referred to as the "butterfly effect," is essential for ensuring unpredictability and security in chaos-based cryptographic applications.

To empirically demonstrate this sensitivity in the proposed Improved Composite Chaotic Map (ICCM), a numerical experiment was conducted. Two sequences were generated from initial values that differ by a minute perturbation of 10^{-16}, specifically $x_0 = 0.6$ and $x_0 = 0.6 + 10^{-16}$. The remaining control parameters of the ICCM, including r_{01} and r_{02}, were held constant during each simulation run to isolate the effect of initial condition variation.

Figure 4.4 depicts the evolution of the two trajectories over successive iterations for three representative values of the control parameter r_{01}: 10, 50, and 100. Initially, both trajectories exhibit nearly identical behavior, reflecting the negligible difference in their starting points. However, as iterations progress, the trajectories diverge rapidly and ultimately become statistically uncorrelated. This divergence occurs regardless of the proximity of the initial conditions, confirming the high sensitivity and chaotic nature of the ICCM.

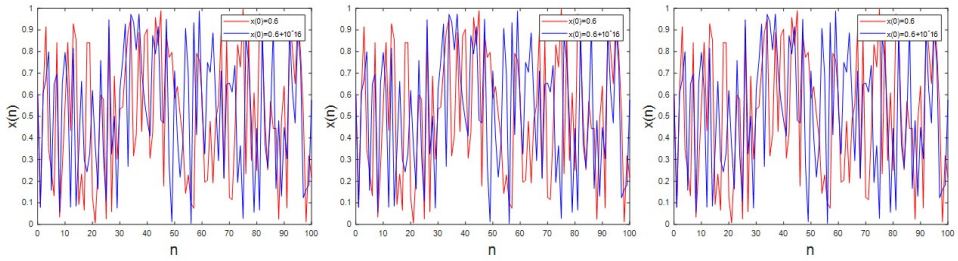


Figure 4.4: Initial value test: (a)$r_{01} = 10$ (b) $r_{01} = 50$ (c) $r_{01} = 100$.

The three subfigures (a), (b), and (c) correspond to different dynamical regimes controlled by r_{01}. As the parameter increases, the rate and complexity of divergence vary, illustrating the flexibility of ICCM in generating diverse chaotic behaviors. This capability is particularly beneficial in cryptographic contexts, where adjustable chaotic dynamics allow for customizable security levels and key space expansion.

This initial value sensitivity ensures that the ICCM produces pseudo-random sequences that are computationally infeasible to predict or reproduce without precise knowledge of the initial conditions. Consequently, any attempt to approximate or guess the initial key parameters results in entirely different encrypted outputs, significantly enhancing the robustness and confidentiality of the encryption system.

4.3.5 Randomness tests

In 2001, the National Institute of Standards and Technology (NIST) introduced a comprehensive set of statistical tests, commonly referred to as the NIST test suite, designed to assess the randomness of binary sequences. These tests are crucial for evaluating the suitability of sequences produced by cryptographic systems. For a sequence to pass the randomness evaluation, each test must yield a P-value greater than 0.01.

In this research, we applied the NIST test suite to the encrypted image to verify its random characteristics. The results of these tests are summarized in the presented table, where the symbol "◯" indicates a passing result. These findings validate the robustness of the ICCM in producing highly random and secure sequences.

Table 4.3: NIST test analysis results.

Test	**P-value**	**Result**
Frequency	6.576×10^{-2}	◯
Block frequency	94.889×10^{-2}	◯
Runs	27.682×10^{-2}	◯
Longest runs of ones	88.224×10^{-2}	◯
Binary matrix rank	41.238×10^{-2}	◯
DFT	1.289×10^{-2}	◯
Non-overlapping template	55.259×10^{-2}	◯
Overlapping template	83.489×10^{-2}	◯
Maurer's universal statistical test	6.893×10^{-2}	◯
Linear complexity	40.315×10^{-2}	◯
Serial	43.305×10^{-2}	◯
Approximate entropy	53.194×10^{-2}	◯
Cumulative sums	6.807×10^{-2}	◯
Random excursions	37.074×10^{-2}	◯
Random excursions variant	97.891×10^{-2}	◯

4.3.6 Double Random Phase Encoding (DRPE) Method

Double Random Phase Encoding (DRPE) is a prominent optical encryption technique introduced in the early 1990s that has since become a cornerstone in secure image processing and cryptography. DRPE achieves image encryption by applying two independent random phase masks in both the spatial and frequency domains, effectively scrambling the original image information into an unrecognizable, noise-like ciphertext.

The process begins by multiplying the input image with a spatial domain random phase mask. This multiplication modulates the amplitude and phase of the image pixels, introducing initial confusion. The modulated image then undergoes a Fourier transform, which translates the image from the spatial domain to the frequency domain. In the frequency domain, a second random phase mask is applied, further diffusing the image information. The result is an encrypted image that appears as a complex interference pattern, susceptible to both random phase masks.

Mathematically, let $f(x, y)$ be the original image function, and $\phi_1(x, y)$ and $\phi_2(u, v)$ be two independent random phase masks uniformly distributed over $[0, 2\pi)$. The encrypted image $E(u, v)$ can be expressed as:

$$E(u, v) = \mathcal{F}\left\{f(x, y)e^{j\phi_1(x,y)}\right\} \cdot e^{j\phi_2(u,v)},$$

where $\mathcal{F}$ denotes the Fourier transform operation, and $j = \sqrt{-1}$ is the imaginary unit.

The decryption process is the inverse operation, requiring exact knowledge of both random phase masks and the correct sequence of inverse transformations. Without these keys, any attempt to retrieve the original image results in noise, thus securing the image against unauthorized access.

The strength of DRPE lies in its high sensitivity to the phase masks; even slight alterations in the masks render decryption impossible. This property, combined with the infinite key space of continuous phase masks, provides a robust defense against brute-force and statistical attacks.

However, classical DRPE schemes based purely on Fourier transforms face limitations such as vulnerability to specific known-plaintext attacks and relatively fixed key space. To address these concerns, DRPE has been enhanced by integrating fractional transforms, such as the Fractional Fourier Transform (FrFT), which generalizes the Fourier domain and increases the dimensionality of the transform parameters, significantly enlarging the key space and improving security.

Understanding the DRPE method and its mathematical foundation is essential for appreciating its integration with the FrFT in the proposed hybrid encryption framework, which we discuss in the subsequent subsection.

4.3.6.1 Fractional Fourier Transform (FrFT)

The Fractional Fourier Transform (FrFT) is a powerful generalization of the classical Fourier Transform, extending the concept of signal transformation to fractional orders. Whereas the classical Fourier transform represents a rotation by 90 degrees in the time-frequency plane, the FrFT corresponds to a rotation by an arbitrary angle, denoted by the fractional order α.

Mathematically, for a two-dimensional input function $f(x, y)$, the FrFT of order α is defined by the integral transform:

$$\begin{aligned} F_\alpha(X,Y) &= \wp^\alpha[f(x,y)](X,Y) \\ &= M_\alpha \iint f(x,y) \exp\left\{ \frac{i\pi\left(x^2+y^2+X^2+Y^2\right)\cos\phi_\alpha - 2(xX+yY)}{\sin\phi_\alpha} \right\} \mathrm{d}x\mathrm{d}y, \end{aligned} \tag{4.6}$$

where the parameter $\phi_\alpha = \alpha\pi/2$ defines the fractional rotation angle, $\alpha \in \mathbb{R} \setminus \{0\}$ is the fractional order, and the normalization constant M_α is given by

$$M_\alpha = \frac{\exp\left(-i\pi\frac{\mathrm{sgn}(\sin\phi_\alpha)}{4}\right)}{\sqrt{|\sin\phi_\alpha|}}. \tag{4.7}$$

The FrFT reduces to the conventional Fourier Transform when $\alpha = 1$ and to the identity operator when $\alpha = 0$.

In image encryption, the FrFT's ability to operate in fractional domains enhances security by introducing additional secret keys (the fractional orders). When combined with DRPE, the FrFT modulates the phase and amplitude of the image in intermediate domains, increasing resistance to attacks that exploit fixed-domain vulnerabilities.

In our proposed encryption algorithm, $f(x, y)$ corresponds to the pre-processed image after pixel scrambling and diffusion. Applying the FrFT within the DRPE framework nonlinearly transforms the encrypted image, thereby strengthening its confusion and diffusion properties and mitigating linear attack strategies [132].

Figure 4.5 illustrates the mathematical implementation of the FrFT-DRPE system, highlighting how the fractional transform and random phase masks interleave to produce a secure encrypted image.

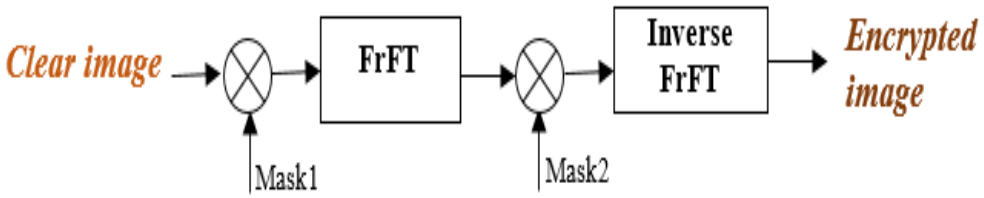


Figure 4.5: Mathematical implementation of the FrFT-DRPE encryption system.

4.3.6.2 Optical DRPE System Implementation

To further enhance the security and efficiency of the proposed encryption framework, the Double Random Phase Encoding (DRPE) technique is implemented in the optical domain. Optical encryption leverages the inherent parallelism and high data throughput of optical systems, enabling rapid and secure processing of large-scale image data. The schematic of the optical DRPE implementation is depicted in Figure 4.6.

In this setup, two Spatial Light Modulators (SLMs), denoted as MSL1 and MSL2, serve as dynamic phase masks during both the encryption and decryption stages. MSL1 modulates the incoming optical wavefront with a complex-valued phase distribution corresponding to the first random phase mask, while MSL2 applies a second phase modulation in the Fourier domain or fractional Fourier domain, depending on the system design.

The encoded optical signal is then captured using a Charge-Coupled Device (CCD) camera, which digitizes the complex amplitude and phase information for subsequent processing and analysis. This digital capture is crucial for interfacing the optical setup with digital computation platforms, allowing for hybrid optical-digital cryptographic architectures.

By exploiting the parallel processing capabilities of optical systems, this approach achieves high-speed encryption and decryption, significantly outperforming purely digital implementations in terms of throughput and latency. Moreover, the physical nature of the optical keys (phase masks displayed on SLMs) adds a tangible layer of security; these keys are inherently difficult to replicate or intercept, thereby strengthening resistance against conventional hacking and tampering attempts.

The integration of the DRPE technique in the optical domain complements the chaos-based key generation provided by the Improved Composite Chaotic Map (ICCM). The synergistic combination ensures that encrypted images exhibit intense confusion and diffusion characteristics while benefiting from the speed and security advantages of optical processing.

Overall, this optical DRPE system implementation embodies a practical and robust solution for real-time, high-security image encryption, making it well-suited for applications in secure communications, biometric authentication, and confidential data storage.

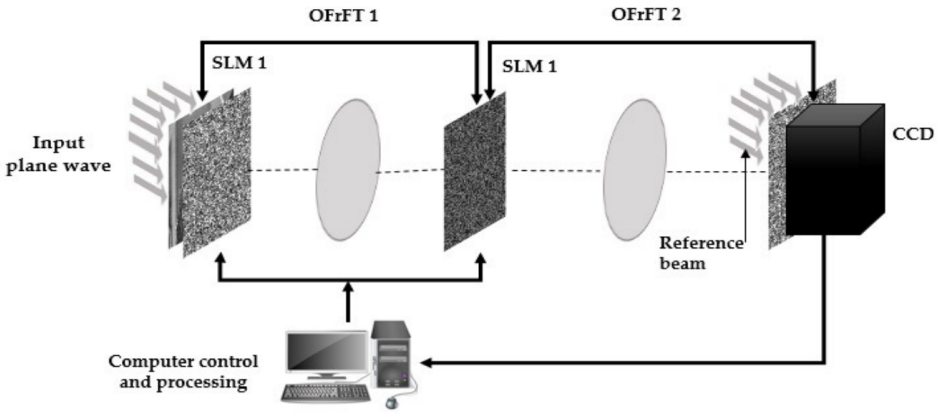


Figure 4.6: Optical FrFT-DRPE system

4.4 Proposed Algorithm

This section presents the proposed image encryption algorithm, which integrates the ICCM scheme with the FrFT-DRPE technique. This algorithm aims to enhance encryption security by leveraging the superior chaotic properties of ICCM and the multi-domain transformation capabilities of FrFT-DRPE. The section begins with a detailed formulation of the encryption process, outlining the sequence of operations, including chaotic sequence generation, pixel permutation, diffusion, and phase encoding. The decryption process is then described, ensuring the accurate retrieval of the original image under the correct key parameters. Additionally, the computational efficiency and security features of the proposed scheme are analyzed, highlighting its robustness against cryptanalytic attacks. This section provides a comprehensive understanding of the proposed method (Figure 6), establishing its advantages over conventional encryption techniques.

4.4.1 Encryption and decryption scheme

In this proposed algorithm, several important steps of image encryption and decryption are involved. We start with scrambling the input image via the permutation-diffusion architecture to prepare it for the second phase, which is the FrFT-DRPE technique of our ICCM, where each chaotic key is characterized by its initial value and double control parameters.
The detailed steps of the algorithm are outlined as follows:

- Consider an input image M of size (m, n) as the starting point for the scheme.
- Resize the image into a one-dimensional vector of length $(1, m \times n)$, referred to as M_1.
- Generate two chaotic vectors, $C_0(x_0, r_{01}, r_{02})$ and $C_1(x_1, r_{11}, r_{12})$, using the ICCM chaotic map. Here, $C_i(x_i, r_{i1}, r_{i2})$ represents the chaotic map's control parameters, with a length of $(1, m \times n)$ for $i = 0, 1$.
- Similarly, generate two additional chaotic vectors, $C_2(x_2, r_{21}, r_{22})$ and $C_3(x_3, r_{31}, r_{32})$, also based on the ICCM chaotic map, where $C_i(x_i, r_{i1}, r_{i2})$ are the control parameters, with a length of $(1, m \times n)$ for $i = 2, 3$.
- Perform the permutation of the M_1 vector according to the order specified by the C_0 vector. This rearranges the pixels in M_1 to generate the scrambled vector, denoted as M_s1 .
- Apply an XOR operation between the M_{s1} and C_1 vectors using the following formula:

$$y_k = \begin{cases} M_{\text{s1}} \oplus C_{11}, & k = 1 \\ M_{\text{s1}} \oplus C_{11} \oplus y_{1_{k-1}}, & k = 1, 2, \ldots m \times n \end{cases} \tag{4.8}$$

where $C_{11} = round(C_1 \times 256)$ and y_k is the obtained result.

- Reshape the vector y_k into an encrypted image matrix of size (m, n). This matrix is then encrypted using the FrFT-DRPE technique with the parameters α and β, resulting in a ciphered image denoted as Y_f. The encryption process follows the scheme illustrated in Fig. 5, where $mask1$ and $mask2$ are generated chaotically using the ICCM chaotic maps $C_2(x_2, r_{21}, r_{22})$ and $C_3(x_3, r_{31}, r_{32})$, respectively.

These encryption steps ensure the security and integrity of the encrypted image during transmission or storage, protecting it against potential unauthorized access or tampering.

Algorithm 1 Encryption algorithm

Require: Input image `img_cry`, secret keys `r0`, `r1`, `r2`, `r3`
Ensure: Encrypted image `out_img`

1: Initialize `x(1) =x0`.
2: **for** $i = 1$ to $m \times n - 1$ **do**
3: $x(i+1) = mod(r1 \times r0 - r1 \times r0^3 + (3 \times r1 \times r0^2 - r1) \times exp(2 \times x1(i)) - 3 \times r \times r0 \times exp(4 \times x1(i)) + r1 \times exp(6 \times x1(i)), 1)$.
4: **end for**
5: $w \Leftarrow x_i$.
6: $masq1 = exp(2j \times \pi \times w)$.
7: `matrix` $\leftarrow$ `img_cry`$\times$`masq1` .
8: **for** $i = 1$ to number of rows/columns in `matrix` **do** state Apply the Discrete Fractional Fourier Transform (DFRFT) on each row of `matrix` with angle `angles1(1)` and store in `temp(i,:)`.
9: **end for**
10: Initialize `y(1) =y0`.
11: **for** $jj = 1$ to $m \times n - 1$ **do**
12: Compute $y(jj+1) = mod(r3 - r2^2 \times exp(2 \times y(jj)) - r2^2 \times exp(6 \times y(jj)) + 2 \times r2^2 \times exp(4 \times y(jj)), 1)$.
13: **end for**
14: $w1 \Leftarrow y_i$.
15: $masq2 = exp(2j \times \pi \times w1)$.
16: `matrix1` $\Leftarrow$ `oout`$\times$`masq2` .
17: **for** $i = 1$ to number of rows/columns in `matrix1` **do**
18: Apply the inverse DFRFT on each row of `matrix1` with angle `-angles1(1)` and store in `temp(i,:)`.
19: **end for**
20: `out_img` $\leftarrow$ $double(oout1)$.

4.4.2 Decryption phase

The detailed steps of the decryption phase for the improved scheme are outlined in the pseudo-code provided below.

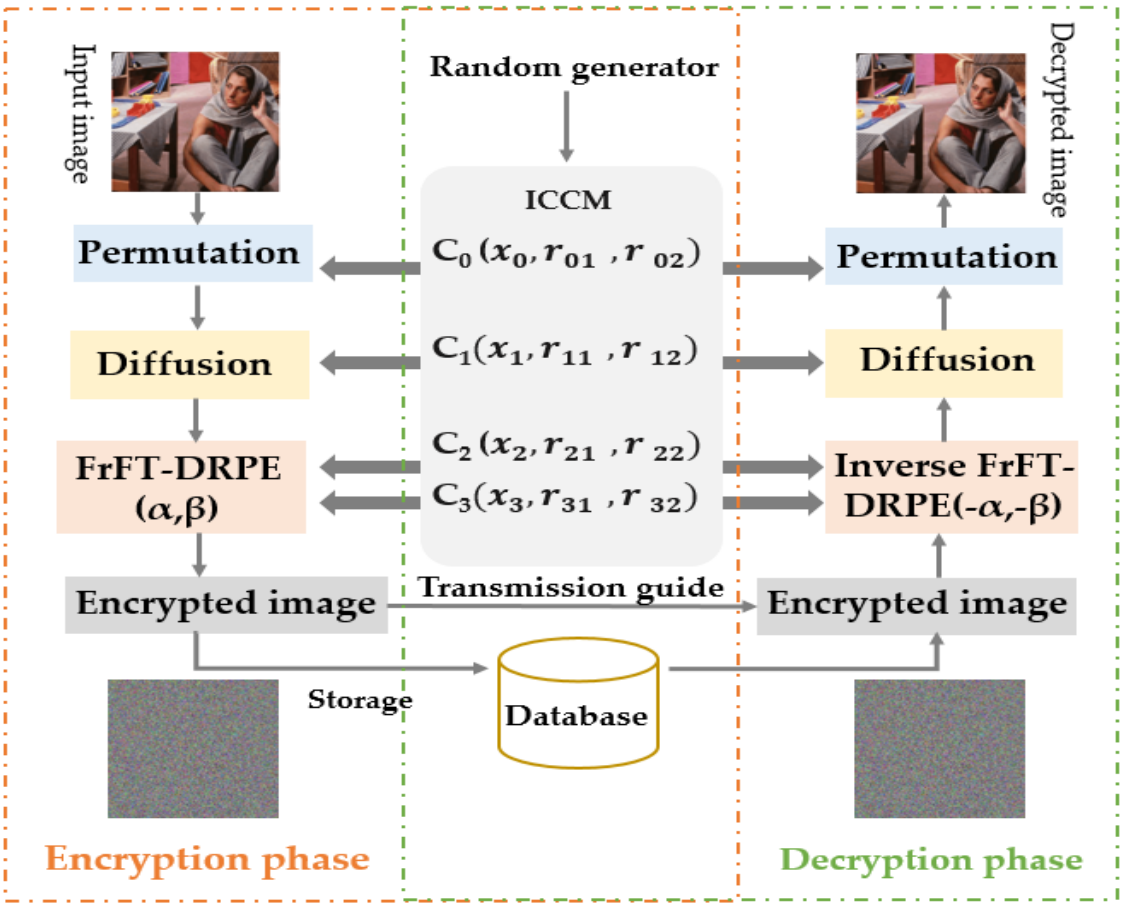


Figure 4.7: Proposed encryption and decryption scheme.

Algorithm 2 Decryption algorithm

Require: Input image $oout1$, $masq2$, $masq1$, $angles1$, secret keys $r1$, $r5$, $r6$, $r2$
Ensure: Decrypted image dec_img

Load input image matrix $oout1$ and masks $masq1$, $masq2$
Initialize fraction with $fraction(1,1)$ and $fraction(1,2)$
Set angles: $angles1 = [fraction(1,1), fraction(1,2)]$
for $k = 1$ to number of rows in $matrix$ **do**
    Apply FRFT: $temp(k,:) \leftarrow disfrft(matrix(k,:), +angles1(1))$
end for
for $k = 1$ to number of columns in $matrix$ **do**
    Apply FRFT: $oout(:,k) \leftarrow disfrft(temp(:,k), +angles1(2))$
end for
Normalize $matrix1 \leftarrow oout/masq2$
for $k = 1$ to number of rows in $matrix1$ **do**
    Apply inverse FRFT: $temp1(k,:) \leftarrow disfrft(matrix1(k,:), -angles1(1))$
end for
for $k = 1$ to number of columns in $matrix1$ **do**
    Apply inverse FRFT: $oout2(:,k) \leftarrow disfrft(temp1(:,k), -angles1(2))$
end for
Compute $matrix2 \leftarrow abs(oout2/masq1)$
Generate chaotic sequence yy and XOR with ss to get SS
Generate chaotic sequence Z and permute SS to form $SS1$
Reshape $SS1$ into matrix and convert to $uint8$ as dec_img

So, to recover the original image from the processed ciphered image, the following steps are performed:

- Apply the inverse FrFT-DRPE technique to the ciphered image.
- Perform the inverse of the classical encryption architecture, including diffusion and permutation, using the correct keys and control parameters.

4.5 Simulation results: analysis and discussions

This section presents the results obtained from implementing the proposed algorithm. The simulations were conducted on a personal computer running Windows 11 (64-bit) with MATLAB R2018b. The hardware setup included a RYZEN processor and 16 GB of random access memory (RAM). To evaluate the performance and robustness of the proposed encryption and decryption scheme, various images of length $256\times256, 512\times512$, and 1024×1024 were employed, sourced from the USC-SIPI and Kodak databases.

The efficacy of the proposed system was assessed through a series of rigorous tests, each designed to validate specific aspects of the algorithm. These tests include sensitivity analysis, statistical evaluations, keyspace and key sensitivity analysis, and comparative performance analysis with existing methods. The following subsections provide a detailed account of the simulation results and their implications.

4.5.1 Performance metrics

The evaluation of the proposed approach is conducted using several performance metrics, including the correlation coefficient (Corr), Peak Signal-to-Noise Ratio (PSNR), and Mean Square Error (MSE). These metrics are mathematically defined as follows:

$$\mathrm{corr}_{I_0 I_r} = \frac{\mathrm{cov}\left(I_0, I_r\right)}{\sqrt{D_{l_0}} \times \sqrt{D_{l_r}}} \tag{4.9}$$

$$E\left(I_0\right) = 1/(m \times n) \times \sum_{i=1}^{N} I_{0_i} \tag{4.10}$$

$$D_{I_0} = \frac{1}{m \times n} \sum_{i=1}^{m \times n} \left(I_{0i} - E(I_0)\right)^2 \tag{4.11}$$

$$\mathrm{cov}(I_0, I_r) = \frac{1}{m \times n} \sum_{i=1}^{m \times n} \left(I_{0i} - E(I_0)\right)\left(I_{ri} - E(I_r)\right) \tag{4.12}$$

$$PSNR = 10\log_{10}\left(d^2/MSE\right) \tag{4.13}$$

$$MSE = (1/m \times n) \times \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(I_0(i,j) - I_r(i,j)\right)^2 \tag{4.14}$$

where: $m \times n$ is the total number of pixels in the image.
d is the maximum possible pixel value (e.g, 255 for 8-bit images), $I_o(i,j)$ and $I_r(i,j)$ are pixel values at position (i,j) in the original and encrypted images. .
D_{I_o} and D_{I_r}, $\text{cov}(I_o, I_r)$ are the Variances and the Covariance between the original and encrypted images, respectively.
The correlation measures the statistical dependence between the original and encrypted images. Notably, for secure encryption, the correlation coefficients between I_0 and I_r in our case should be close to zero. Given that the encryption keys are generated randomly, the correlation values vary with each execution of the algorithm. To ensure robustness, we calculated the average correlation coefficient over 20 iterations for each image.
A greater disparity between the original and encrypted images indicates a more efficient encryption process. This is quantitatively assessed using PSNR and MSE. In the context of image encryption, a lower PSNR value signifies higher encryption strength, as it reflects significant deviation and image scrambling. The results of these evaluations are summarized in Table 4.4.

Thus, the effectiveness of the ICCM is demonstrated by a high MSE value exceeding (10^4), combined with a low PSNR value (< 10). These metrics indicate significant deviation and image scrambling, validating the robustness of the encryption scheme. Additionally, the closer the correlation coefficient is to zero, the more reliable and secure the system becomes. When compared to existing works, the proposed scheme exhibits superior performance in resisting various cryptographic attacks. Table 4.5 presents a comparative analysis of correlation coefficients across different directional components,

Table 4.4: Performance metrics Corr, MSE, and PSNR of test images and corresponding encrypted ones.

Test Image	**Encrypted Image**		
	Corr (ideal value = 0)	**MSE** ($> 10^4$)	**PSNR** (< 10)
Building	-0.00031	17508.25	5.6984
Cameraman	-0.00193	22860.84	5.6118
Barbara	0.00012	15548.98	6.2025
X31-f18	-0.00050	27996.27	3.6598
Baboon	0.00286	18525.275	7.1529
Peppers	0.00166	14995.54	6.6709
Couple	-0.00014	21509.68	5.9534
Clock	0.00094	37675.91	2.3702

highlighting the enhanced robustness of our scheme.

Table 4.5: Correlation coefficient of our algorithm compared with existing ones.

Scheme	**Input image**	**Correlation coefficients**		
		Horizontal	**Vertical**	**Diagonal**
	Ideal value	≈0	≈0	≈0
Ours	Baboon	0.0011	-0.0011	-0.0072
	Barbara	-0.0001	-0.0053	-0.0002
	Cameraman	0.0001	0.0004	-0.0007
	Pepper	0.0061	-0.0002	0.0012
Ref. [101]	Barbara	0.0022	-0.0024	-0.0004
	Baboon	-0.0036	-0.0014	-0.0065
	Cameraman	0.0036	-0.0058	-0.0001
	Pepper	0.0004	0.0013	-0.0007
Ref. [124]	Barbara	0.0136	0.0084	0.0146
	Peppers	0.0115	0.0109	-0.0101
Ref. [133]	Baboon	-0.0138	-0.0267	-0.0187
	Peppers	0.0190	-0.0029	0.0072

4.5.2 Histogram analysis

The image histogram represents the pixel intensity distribution and encapsulates the critical information processed. In this subsection, we evaluate the effectiveness of the proposed encryption algorithm by analyzing the histograms of both original and encrypted images. The results demonstrate that each original image exhibits a unique and distinctive histogram corresponding to its pixel intensity distribution. In contrast, the encrypted images produced by the algorithm display uniform histograms resembling a Gaussian spectrum, as illustrated in 4.8. This uniformity indicates that no discernible information about the original image can be inferred from the encrypted image. This behavior affirms the robustness and security of the proposed encryption scheme, as it effectively obfuscates the underlying data, preventing potential attackers from extracting meaningful insights.

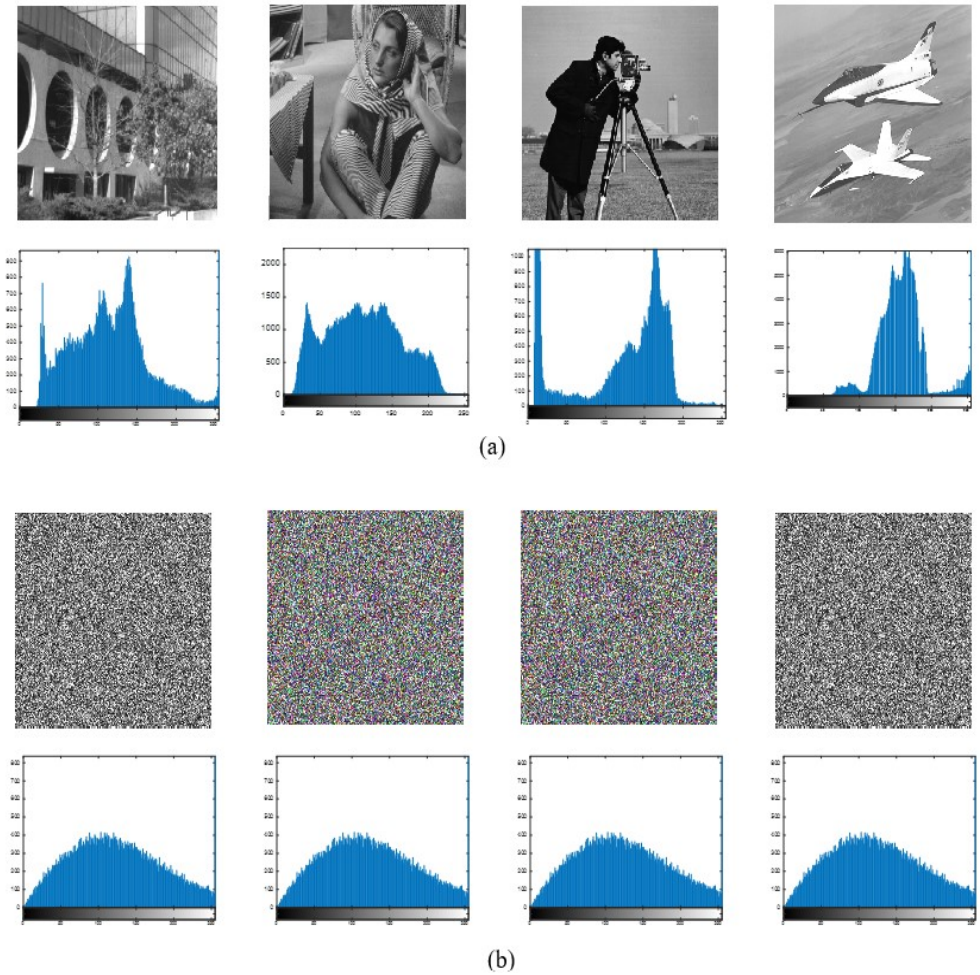


Figure 4.8: Histogram analysis:(a) original test images of size ($256 * 256$ Building and cameraman, $512 * 512$ Barbara and $x31_f18$) and their corresponding histograms, and (b) encrypted test images and their corresponding histograms.

4.5.3 loss data tests

In the process of transferring and exchanging information, it is common for some data to become damaged or distorted, resulting in missing portions of the transmitted content. This subsection examines the performance of the proposed encryption scheme under scenarios where parts of the ciphered image are lost during transmission between the sender and the recipient. Specifically, we simulate data loss rates of 12.5%, 25%, and 50% of the encrypted image.

The results of the decryption process demonstrate that the original image remains clearly distinguishable, even after losing more than half of the encrypted information. This highlights the robustness of the proposed algorithm and its resilience against one of the most challenging issues in data security and transmission. Figure 4.9 illustrates the results of this experiment, showing the decrypted images corresponding to encrypted images with 12.5%, 25%, and 50% data loss, respectively.

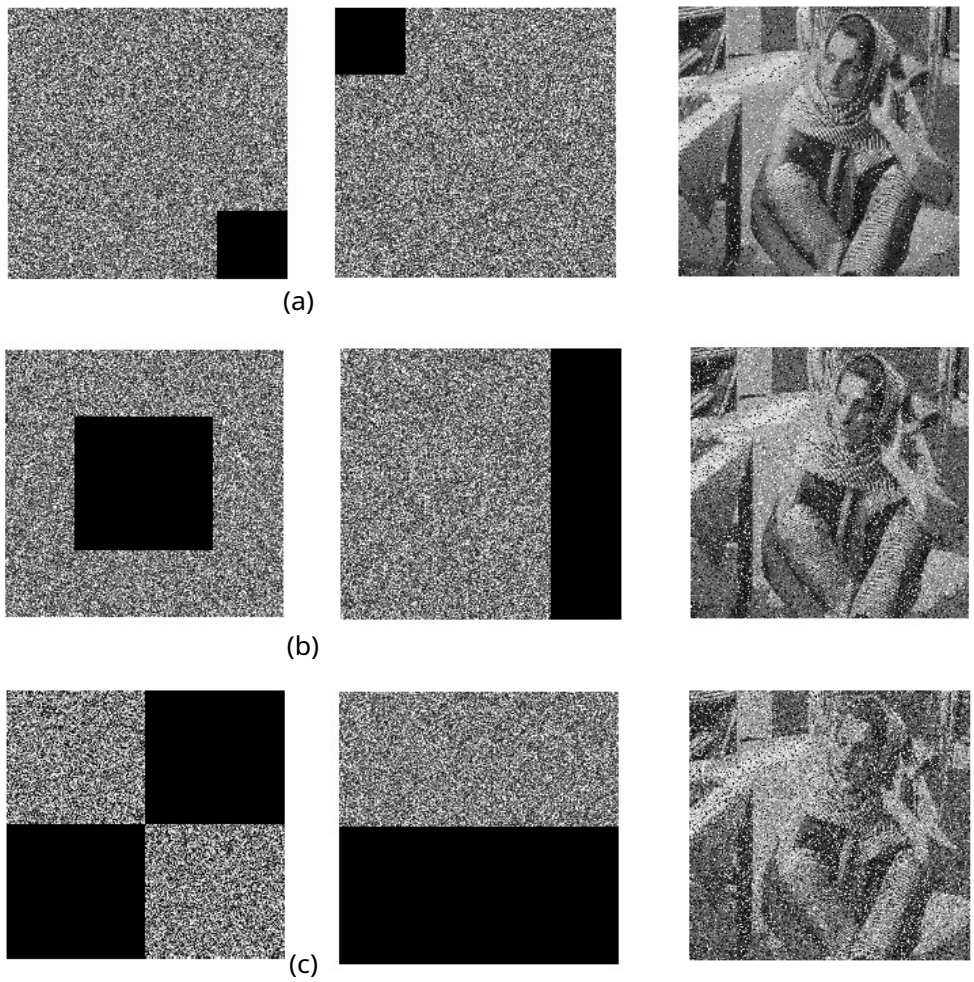


Figure 4.9: Loss data tests for the encrypted *Barbara* image and the respective decrypted images resulted in: (a) 12.5%, (b) 25%, and (c) 50%.

4.5.4 Sensitivity and keyspace analysis

In this subsection, we analyze the sensitivity and keyspace of the proposed encryption scheme. The encryption key is constructed using the parameters of the newly developed chaotic map in combination with those of the FrFT. These parameters are denoted as:

$$k(x_0, r_{01}, r_{02}, x_1, r_{11}, r_{12}, x_2, r_{21}, r_{22}, x_3, r_{31}, r_{32}).$$

Similarly, during the decryption process, it is assumed that the decryption key follows the same structure, represented as:

$$k'(x'_0, r'_{01}, r'_{02}, x'_1, r'_{11}, r'_{12}, x'_2, r'_{21}, r'_{22}, x'_3, r'_{31}, r'_{32}).$$

For sensitivity analysis, a slight variation is introduced in one parameter of the encryption key while keeping the other parameters unchanged. This process is repeated for each parameter to evaluate the impact of small deviations. The analysis reveals that the threshold for the appearance of the original image is approximately 10^{-15} for variations

in r_i and 10^{-16} for variations in x_i and $r_{i1,2}$. The precision levels for these thresholds are 10^{14} and 10^{15}, respectively. The results, as illustrated in Figure 4.10, confirm the high sensitivity of the proposed scheme to its encryption keys. This characteristic reinforces its robustness, ensuring that even minor deviations in the key parameters render decryption infeasible, thus enhancing the security of the encryption process.

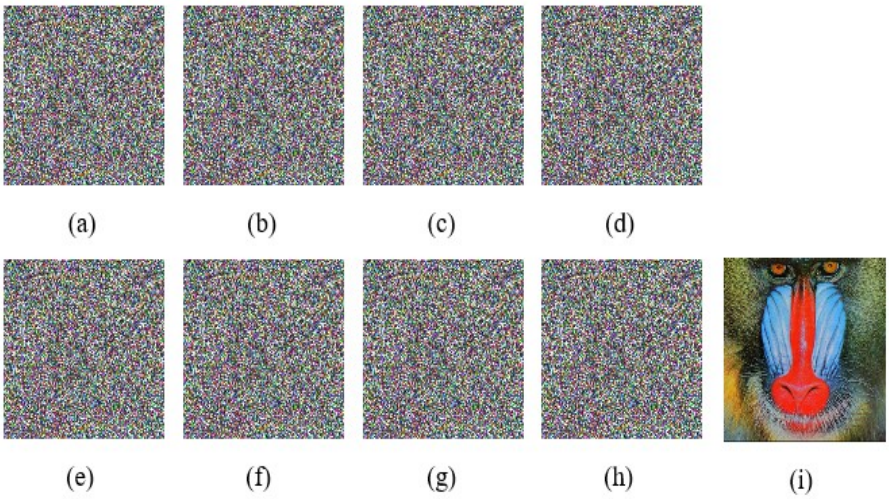


Figure 4.10: Sensitivity test results: $(a)x_0 = x_0 + 10^{-16}$, $(b)r_{01} = r_{01} + 10^{-15}$, $(c)r_{02} = r_{01} + 10^{-15}$, $(d)x_1 = x_1 + 10^{-16}$, $(e)r_{11} = r_{11} + 10^{-15}$, $(f)r_{12} = r_{12} + 10^{-15}$, $(g)\alpha = \alpha + 10^{-16}$, $(h)\beta = \beta + 10^{-16}$, (i) decryption Baboon $512 * 512$ image with the correct keys$(k = k')$.

4.5.4.1 Keyspace Analysis

In this part, we introduce a small error, $k = 0.01$, fluctuating between -0.2 and $+0.2$, into the parametric orders of the FrFT, defined as $\alpha^* = \alpha + k$ and $\beta^* = \beta + k$, to evaluate the sensitivity of the fractional encryption key in the proposed scheme.

The corresponding MSE is calculated to quantify the impact of these variations. The results, presented in

Figure 4.11, clearly demonstrate the sensitivity of the proposed scheme to changes in the fractional key parameters.

This analysis confirms the superiority of the proposed method over the reference method [88] and the DRPE method based on FrFT [134], as the proposed scheme exhibits higher robustness and better error tolerance. The accuracy of the ICCM parameters $(x_i, r_{i1,2})$ at precision levels of 10^{15} and 10^{16}, respectively, has been verified and validated through sensitivity tests and keyspace analysis, as outlined in the preceding section. The total keyspace of the proposed scheme is calculated using Equation (13), where the contributions of α and β are negligible. The resulting keyspace far exceeds the encryption security requirement of 2^{100}, providing a robust safeguard against brute-force attacks.

Additionally, we compared the key space size of the proposed method with that of existing encryption schemes, as summarised in Table 4.6. The results demonstrate that

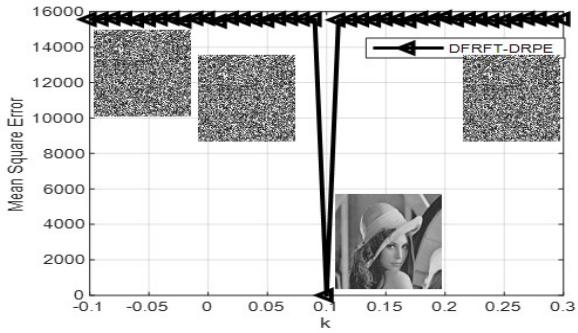


Figure 4.11: The MSE curve depending on the values of parameter k

the proposed scheme offers a significantly larger keyspace, reinforcing its superior security performance.

$$\text{Keyspace size} = 10^{15\times 8} \times 10^{16\times 4} \quad = 10^{184} \approx 2^{674} \tag{4.15}$$

Table 4.6: Keyspace sizes compared to existing schemes.

Scheme	**Proposed**	[100]	[135]	[136]	[137]	[138]	[139]
KeySpace	2^{674}	2^{600}	2^{477}	2^{320}	2^{284}	2^{279}	2^{262}

4.5.5 Effeciency Metrics

In this subsection, we present the obtained results, comparing them with various existing works, using the Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), Differential Attack analysis, and Encryption time test.

4.5.5.1 NPCR and UACI test

To further evaluate the robustness of the proposed encryption scheme, the NPCR and UACI tests were employed to analyze the system's sensitivity to minor changes in the original image. These metrics are crucial for evaluating the encryption scheme's ability to generate significantly different encrypted images even when the input image undergoes the slightest modification. The results, as demonstrated in Table 4.7, reveal that the proposed scheme achieves an impressive NPCR average of 99.6164% and a UACI of 33.4524%. Such high values indicate that the encryption system exhibits excellent plain image sensitivity, ensuring that even the smallest alterations in the input image lead to substantial changes in the encrypted output.

Moreover, the stability of these results across multiple test images of different types (grayscale and color) and sizes (256×256, 512×512, 1024×1024) underscores the reliability and consistency of the proposed scheme, making it a robust solution for secure image encryption in real-world applications.

Table 4.7: NPCR and UACI test results on plain image sensitivity.

input image	**Ref. [140]**		**Proposed Scheme**	
	NPCR (%)	**UACI (%)**	**NPCR (%)**	**UACI (%)**
5.1.10.tiff	99.6162	33.4645	99.6181	33.4601
5.1.13.tiff	99.6119	33.4597	99.6241	33.4541
5.2.08.tiff	99.6080	33.4589	99.6123	33.4398
5.3.01.tiff	99.6107	33.4595	99.6121	33.4487
7.1.02.tiff	99.6140	33.4635	99.6115	33.4610
7.1.05.tiff	99.6083	33.4643	99.6191	33.45678
boat.512.tiff	99.6098	33.4825	99.6160	33.4731
elaine.512.tiff	99.6098	33.4521	99.6171	33.4322
gray21.512.tiff	99.6122	33.4713	99.6141	33.4689
ruler.512.tiff	99.6115	33.4453	99.6198	33.4291
Average	99.6113	33.4598	**99.6164**	**33.4524**

4.5.5.2 Differential Attacks analysis

Differential attacks are a fundamental method for assessing the security robustness of encryption schemes, particularly in image cryptosystems [141]. These attacks evaluate how minor modifications in the plaintext affect the corresponding ciphertext, which is crucial for determining the sensitivity and resistance of an encryption algorithm to differential cryptanalysis. In this study, we conducted a differential attack analysis by modifying a single bit in the plaintext image and observing the resulting differences in the encrypted outputs. Specifically, we altered the Least Significant Bit (LSB) and the Most Significant Bit (MSB) of the input image and analyzed their impact on the generated ciphertext. A well-designed encryption scheme should exhibit high sensitivity to these small changes, meaning that even a single-bit modification in the plaintext should propagate extensively throughout the encrypted image. This property ensures that the encryption system is resistant to differential attacks, as any minor alteration in the input image results in a significantly different encrypted output. To validate the security of our proposed ICCM approach, we conducted a bitwise differential analysis where:

- An original image was encrypted using ICCM.
- A modified version of the image was generated by flipping a single bit (LSB or MSB).
- Both the original and modified images were re-encrypted.
- The differences between the two encrypted images were visualized to measure the diffusion effect.

Figure 4.12 presents the results of the differential attack analysis, where it can be observed that even a single-bit change in the plaintext leads to a drastic and unpredictable transformation in the ciphertext, confirming the high sensitivity of ICCM to input variations. The obtained results substantiate the robustness of the proposed encryption approach in resisting differential attacks.

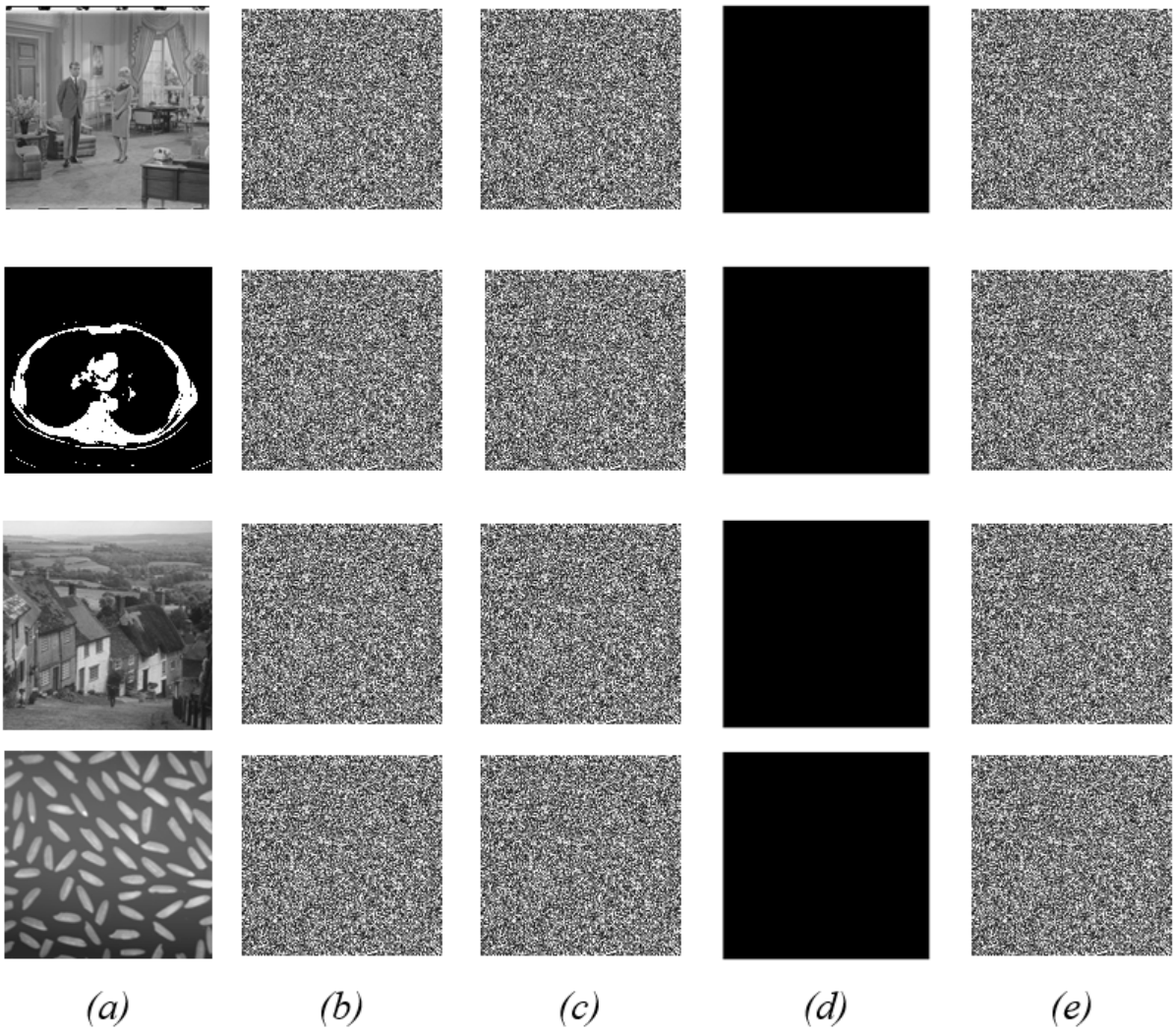


Figure 4.12: Results of differential attack analysis. (a) Original images. (b) Encrypted images. (c) Encrypted modified images (LSB change). (d) Difference between the original and modified encrypted images. (e) Difference between the corresponding encrypted outputs.

4.5.5.3 Encryption time test

In modern digital imaging systems where large-scale data transmission and high-speed processing are paramount, encryption efficiency emerges as a critical performance metric for practical deployment, algorithms demonstrating suboptimal computational speed risk becoming impractical for real-world implementation despite theoretical security merits. To rigorously evaluate our proposed scheme's operational viability, we implemented a

comprehensive experimental evaluation framework comparing ICCM against contemporary encryption methods. As detailed in Table 4.8, the encryption time analysis across standardized image resolutions ($256\times256, 512\times512$, and 1024×1024 pixels) compared with existing works in the same field. the empirical results conclusively demonstrate ICCM's competitive temporal performance across standardized image dimensions while maintaining robust security characteristics.

Table 4.8: Encryption time (Second).

Algorithm	**256 × 256**	**512 × 512**	**1024 × 1024**
Ref.[142]	0.2197	0.9417	3.8712
Ref.[143]	0.4497	1.8927	7.6805
Ref. [142]	0.1223	0.5684	2.6734
Ref.[144]	0.0622	0.2767	1.1461
Ref.[145]	0.1253	0.4932	2.1363
Ref. [146]	0.0240	0.0977	0.3993
ICCM	0.0263	0.0842	0.3165

4.6 Conclusion

This paper proposed a novel image encryption scheme based on an ICCM integrated with the FrFT-DRPE technique. By leveraging the strengths of quadratic and cubic chaotic maps, the proposed approach enhances key sensitivity, expands the chaotic range, and significantly improves resistance against cryptographic attacks. The effectiveness of the encryption scheme was validated through extensive security and performance analyses, including correlation coefficient tests, MSE, PSNR, histogram analysis, and keyspace evaluation. The results demonstrated that the ICCM-based encryption scheme provides superior security compared to existing methods, exhibiting strong robustness against brute-force, statistical, and differential attacks. Furthermore, histogram analysis confirmed that the encrypted images have uniform distributions, preventing information leakage, while sensitivity and keyspace analysis underscored the high precision and unpredictability of the encryption keys.

Despite its strong performance, the proposed method presents certain limitations. While it effectively enhances security, optimizing computational efficiency remains an area of interest, particularly for real-time applications such as video encryption and IoT devices. Additionally, scalability must be further explored to ensure that the encryption framework can handle high-resolution images and large multimedia datasets without compromising processing speed. Future research could focus on integrating ICCM with advanced cryptographic techniques, such as quantum cryptography or deep learning-based encryption, to enhance adaptability and security. Moreover, as artificial intelligence-driven attacks continue to evolve, analyzing the resilience of the proposed scheme against AI-based cryptanalysis and developing effective countermeasures will be essential.

In conclusion, the proposed ICCM-based encryption scheme contributes significantly to the advancement of chaotic cryptography, offering a robust and efficient solution for secure image transmission and storage. By addressing existing challenges and exploring new research directions, this work paves the way for further improvements in modern encryption techniques, with potential applications in secure communications, medical imaging, military data protection, and digital forensics.

Chapter 5

Conclusion and Future Outlook

General Conclusion

This doctoral thesis presented a comprehensive investigation into the development and implementation of advanced chaotic algorithms for information security and biometric-based identification. Motivated by the increasing need for robust, adaptive, and scalable encryption systems in a highly interconnected digital world, the research focused on enhancing existing cryptographic frameworks using chaos theory, biometric signals, and optical transformations.

A significant contribution of this work is the formulation of the Improved Composite Chaotic Map (ICCM), which synthesizes quadratic and cubic nonlinearities into a single configurable model. The ICCM significantly broadens the chaotic domain and enhances sensitivity to initial conditions, as validated through rigorous mathematical tools including bifurcation diagrams and Lyapunov exponent analysis. Its incorporation into encryption schemes introduces a stronger, more unpredictable key space while ensuring resistance against classical, statistical, and differential attacks.

Another key innovation lies in the integration of ICCM with optical encryption techniques, such as the Double Random Phase Encoding (DRPE) and the Fractional Fourier Transform (FrFT). This hybrid opto-digital model achieves multi-domain scrambling, thereby reinforcing confidentiality through transformation diversity. Empirical results demonstrated that the proposed scheme performs exceptionally well in terms of Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), correlation coefficients, and entropy, outperforming many existing algorithms in both robustness and efficiency.

The thesis also introduced a novel biometric-dependent encryption framework, specifically targeting the protection of retinal images. This scheme dynamically generates encryption keys from original biometric patterns, ensuring identity binding and personalisation in the encryption process. Extensive simulations using benchmark datasets such as DRIVE and STARE, as well as standard evaluation metrics including NIST random-

ness tests, confirmed the system's effectiveness in maintaining both security and image integrity.

In addition to cryptographic theory, this work addressed practical considerations in medical image security and biometric data protection. By proposing a system that simultaneously ensures privacy, data integrity, and resistance to tampering, this thesis contributes toward the growing field of privacy-preserving computing and secure identity verification.

Looking ahead, several promising avenues exist for extending this research. One direction includes implementing the proposed models in real-time embedded systems or edge devices, where lightweight encryption with high throughput is critical. Another future development could involve coupling chaotic encryption with machine learning for adaptive intrusion detection or biometric spoofing prevention. Moreover, exploring quantum-resilient variants of chaos-based systems would be a valuable contribution in preparing for the post-quantum cryptographic landscape.

In conclusion, this work offers a significant step forward in the intersection of chaotic dynamics, optical security, and biometric encryption. It provides a robust, adaptable, and efficient framework for secure identification and data protection in domains where privacy, trust, and speed are of paramount importance. The findings presented in this thesis lay a strong foundation for further interdisciplinary research in secure systems engineering, biometric computing, and applied nonlinear dynamics.

Bibliography

[1] Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, 1996.

[2] Stallings, W. *Cryptography and Network Security: Principles and Practice*. Pearson, 8th edition, 2021.

[3] Pecora, L.M. and Carroll, T.L. Synchronization in chaotic systems. *Physical Review Letters*, 64(8):821–824, 1990.

[4] Pareek, N.K., Patidar, V., and Sud, K.K. Image encryption using chaotic logistic map. *Image and Vision Computing*, 24(9):926–934, 2006. doi: 10.1016/j.imavis.2006.02.021.

[5] El-Latif, A.A.A.A. and Hwang, J.N. A hybrid chaotic system and advanced encryption standard for image encryption. *Optics & Lasers in Engineering*, 51(6):665–673, 2013.

[6] Wang, X., Zhang, Y., and Zheng, X. A novel chaotic image encryption algorithm based on bit-level permutation and dynamic diffusion. *Optics and Lasers in Engineering*, 73:53–61, 2015.

[7] Nanda, D.K., Sahu, S., and Panda, G. Chaotic and biometric-based image protection for secure medical data storage. *Signal Processing*, 134:150–161, 2017.

[8] Zhang, Y., Wu, Y., and Lu, W. Optical image encryption using drpe and chaos in the fractional fourier domain. *Optics Communications*, 285(6):870–876, 2012.

[9] Rukhin, A. and et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report Special Publication 800-22, National Institute of Standards and Technology (NIST), 2001.

[10] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376, 2015.

[11] Stallings, W. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2017.

[12] Alenezi, M.N., Alabdulrazzaq, H., and Mohammad, N.Q. Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, 12(2):256–272, 2020.

[13] Mohamed, M.A., Fouad, M.M., and Aly, M.H. A survey on image encryption techniques: From chaos to neural networks. *Multimedia Tools and Applications*, 80: 16921–16956, 2021.

[14] Farooq, U., Zafar, M., and Anwar, S. Chaotic image encryption techniques: Recent advances and challenges. *Journal of Information Security and Applications*, 58: 102750, 2021.

[15] Rodriguez, J., Torres, J., and Palafox, L. Privacy in biometric systems: Models and architectures. *Computers & Security*, 86:335–349, 2019.

[16] Baker, S., Liu, Y., and Lee, S. Behavioral biometrics for continuous authentication: a survey. *IEEE Access*, 11:40291–40315, 2023.

[17] Kshetri, N., Rahman, M.M., Rana, M.M., Osama, O.F., and Hutson, J. algotric: Symmetric and asymmetric encryption algorithms for cryptography – a comparative analysis in ai era. *arXiv preprint arXiv:2412.15237*, 2024.

[18] Abood, O.G. and Guirguis, S.K. A survey on cryptography algorithms. *International Journal of Scientific and Research Publications*, 8(7):495–516, 2018.

[19] Riman, C. and Abi-Char, P.E. Comparative analysis of block cipher-based encryption algorithms: a survey. *Information Security and Computer Fraud*, 3(1):1–7, 2015.

[20] Xiang, T., Liao, X., Tang, G., Chen, Y., and Wong, K.w. A novel block cryptosystem based on iterating a chaotic map. *Physics Letters A*, 349(1-4):109–115, 2006.

[21] Canteaut, A., Carpov, S., Fontaine, C., Lepoint, T., Naya-Plasencia, M., Paillier, P., and Sirdey, R. Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression. *Journal of Cryptology*, 31(3):885–916, 2018.

[22] Wang, Y. and Li, X. Efficient aes-based encryption algorithms for big data applications. *Journal of Cryptography and Information Security*, 38(2):202–215, 2023. doi: 10.1016/j.jcis.2023.03.002.

[23] Narayan, V., Joshi, A., and Patel, R. A lightweight hybrid cryptosystem for secure medical image transmission in e-healthcare applications. *Journal of Ambient Intelligence and Humanized Computing*, 2024. In press.

[24] Menezes, A.J., van Oorschot, P.C., and Vanstone, S.A. *Handbook of Applied Cryptography*. CRC Press, 2nd edition, 2023.

[25] Zhou, J. and Wei, Z. Secure data integrity verification and authentication using hmac and sha algorithms in cloud computing. *Journal of Cryptographic Engineering*, 8(2):123–139, 2023.

[26] Shakhmetova, G., Barlybayev, A., Saukhanova, Z., Sharipbay, A., Raykul, S., and Khassenov, A. Enhancing visual data security: A novel fsm-based image encryption and decryption methodology. *Applied Sciences*, 14(11):4341, 2024.

[27] Kolivand, H., Hamood, S.F., Asadianfam, S., and Rahim, M.S. Image encryption techniques: A comprehensive review. *Multimedia Tools and Applications*, 83:12345–12367, 2024.

[28] Zhang, Y., Wang, X., and Zhang, Z. Limitations of conventional encryption algorithms for image data. *IEEE Transactions on Image Processing*, 32(1):76–88, 2021.

[29] SaberiKamarposhti, M., Ghorbani, A., and Yadollahi, M. A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. *Chaos, Solitons & Fractals*, 178:114361, 2024.

[30] Zhang, B. and Liu, L. Chaos-based image encryption: Review, application, and challenges. *Mathematics*, 11(11):2585, 2023.

[31] Rashid, F.B., Rankothge, W., Sadeghi, S., Mohammadian, H., and Ghorbani, A. Privacy-preserving for images in satellite communications: A comprehensive review of chaos-based encryption. *arXiv preprint arXiv:2410.21177*, 2024.

[32] Wang, X., Zhao, L., and Feng, H. A survey on chaotic maps and their applications in image encryption. *Mathematics*, 11(3):587, 2023.

[33] Miao, Y., Chen, H., and Lu, Z. Challenges in image decryption with minimal information leakage. *Journal of Visual Communication and Image Representation*, 70:102808, 2020.

[34] Hussein, K.W., Sani, N.F.M., Mahmod, R., and Abdullah, M.T. A novel authentication scheme to increase security for non-repudiation of users. 2013.

[35] Chen, L., Moody, D., Regenscheid, A., and Robinson, A. Digital signature standard (dss). Technical Report FIPS 186-5, National Institute of Standards and Technology, 2023.

[36] Boussif, M., Guerchi, D., and Khelifi, F. A comprehensive review on chaotic image encryption techniques. *Multimedia Tools and Applications*, 79:12157–12199, 2020.

[37] Elhoseny, M., Yuan, X., and Hassanien, A.E. Secure medical data transmission model for iot-based healthcare systems. *IEEE Access*, 6:20596–20608, 2018.

[38] Zhang, X., Liu, S., and Lu, J. Image encryption based on dna encoding and permutation-diffusion architecture. *Signal Processing*, 158:134–146, 2019.

[39] Enayatifar, R., Abdullah, A.H., Isnin, I.F., Altameem, A., and Lee, M. Image encryption using a synchronous permutation-diffusion technique. *Optics and Lasers in Engineering*, 90:146–154, 2017.

[40] Wang, X., Qin, C., and Zhang, L. A survey on image encryption methods based on chaos. *Entropy*, 22(10):1100, 2020.

[41] Bakar, A. and Ramasamy, R. Hybrid image encryption algorithms: A review of recent trends. *Journal of Applied Cryptography*, 12(4):56–72, 2021.

[42] Azoug, S.E. and Bouguezel, S. A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional fourier transform. *Optics Communications*, 359:85–94, 2016.

[43] Mokhnache, S., Daachi, M.E.H., Bekkouche, T., and Diffellah, N. A combined chaotic system for speech encryption. *Engineering, Technology & Applied Science Research*, 12(3):8578–8583, 2022. doi: 10.48084/etasr.4912.

[44] Rasband, S.N. *Chaotic dynamics of nonlinear systems*. Courier Dover Publications, 2015.

[45] Tutueva, A.V., Nepomuceno, E.G., Karimov, A.I., Andreev, V.S., and Butusov, D.N. Adaptive chaotic maps and their application to pseudo-random numbers generation. *Chaos, Solitons & Fractals*, 133:109615, 2020.

[46] Grosse-Erdmann, K.G. and Manguillot, A.P. *Linear chaos*. Springer Science & Business Media, 2011.

[47] Chen, Y., Xie, S., and Zhang, J. A hybrid domain image encryption algorithm based on improved henon map. *Entropy*, 24(2):287, 2022.

[48] Unar, J., Seng, W.C., and Abbasi, A. A review of biometric technology along with trends and prospects. *Pattern recognition*, 47(8):2673–2688, 2014.

[49] Nath, D., Ray, S., and Ghosh, S.K. Fingerprint recognition system: design & analysis. In *conference international conference on scientific paradigm shift in information technology & management, SPSITM*, 2011.

[50] Descope. 5 popular biometric authentication methods, 2023.

[51] Kumar, R. and Singh, A. Global adoption of facial recognition technology with special reference to india. *Medico-Legal Journal*, 91(4):1–5, 2023. doi: 10.1177/00258024241227717.

[52] Zhao, W., Chellappa, R., Phillips, P.J., and Rosenfeld, A. Past, present, and future of face recognition: A review. *Electronics*, 9(8):1188, 2020. doi: 10.3390/electronics9081188.

[53] Baker, S.E., Hentz, A., Bowyer, K.W., and Flynn, P.J. Degradation of iris recognition performance due to non-cosmetic prescription contact lenses. *Computer Vision and Image Understanding*, 114(9):1030–1044, 2010.

[54] Jain, A.K., Flynn, P., and Ross, A.A. *Handbook of Biometrics*. Springer, 2008.

[55] Wu, W., Elliott, S.J., Lin, S., Sun, S., and Tang, Y. Review of palm vein recognition. *IET Biometrics*, 9(1):1–10, 2020.

[56] Yang, L., Yang, G., Yin, Y., and Xi, X. Finger vein recognition with anatomy structure analysis. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(8):1892–1905, 2017.

[57] Rao, K. and Sinha, R. Speech recognition: From fundamentals to recent advances. *Journal of the Acoustical Society of India*, 48(1):25–35, 2021.

[58] Almakky, M.Y. et al. A review on automatic speech recognition architectures and challenges. *International Journal of Advanced Computer Science and Applications*, 11(9):605–611, 2020.

[59] Nixon, M.S. and Carter, J.N. A survey on gait recognition. *ACM Computing Surveys*, 51(5):1–35, 2018.

[60] Zou, Q., Wang, Y., Wang, Q., Zhao, Y., and Li, Q. Deep learning-based gait recognition using smartphones in the wild. *IEEE Transactions on Information Forensics and Security*, 15:3197–3212, 2020.

[61] Jain, A.K., Ross, A., and Prabhakar, S. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4–20, 2004.

[62] Galbally, J., Marcel, S., and Fierrez, J. Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, 2:1530–1552, 2014.

[63] Nandakumar, K. Multibiometric systems: Fusion strategies and template security. *Handbook of Biometric Anti-Spoofing*, pages 31–49, 2015.

[64] Zhang, Y., Wang, X., and Li, Q. Biometric authentication for mobile devices. *IEEE Communications Surveys & Tutorials*, 21(3):2347–2376, 2019.

[65] Ratha, N.K., Connell, J.H., and Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[66] Modi, K. and Devaraj, L. Advancements in biometric technology with artificial intelligence. *arXiv preprint arXiv:2212.13187*, 2022.

[67] Yang, L., Chen, X., and Wang, H. Edge ai for real-time biometric authentication: Opportunities and challenges. *IEEE Internet of Things Journal*, 10(3):1922–1935, 2023.

[68] Gai, K., Qiu, M., and Zhao, H. Blockchain meets biometrics: A secure and decentralized approach to identity verification. *Future Generation Computer Systems*, 100:701–709, 2019.

[69] Kouadra, I. Classical chaotic maps commonly used. In *Thesis: Chaotic Cryptographic and Biometric Security Systems*, pages 24–28, 2025.

[70] Kouadra, I. Biometric-based key generation – applications. In *Thesis: Chaotic Cryptographic and Biometric Security Systems*, pages 39–41, 2025.

[71] Kouadra, I. Double random phase encoding (drpe) and fractional fourier transform (frft). In *Thesis: Chaotic Cryptographic and Biometric Security Systems*, pages 30–33, 2025.

[72] Li, C., Wang, Z., and Zhang, J. Secure and efficient data transmission for smart grid using chaotic maps and dna coding. *IEEE Access*, 6:32011–32025, 2018.

[73] Rao, K.V. and Saxena, A. Chaos-based cryptography: A comprehensive survey. *Computers & Security*, 95:101858, 2020.

[74] Alshammari, B., Alsabaan, M., and Alotaibi, N. Challenges and vulnerabilities in chaos-based encryption algorithms: A review. *IEEE Access*, 9:112214–112234, 2021.

[75] Ponnusamy, C. and Deepalakshmi, P. Hcac-ehr: hybrid cryptographic access control for secure ehr retrieval in healthcare cloud. *Journal of Ambient Intelligence and Humanized Computing*, 13:12345–12360, 2022.

[76] Zhang, W., Liu, M., and Chen, L. A review of homomorphic encryption for privacy-preserving biometrics. *Sensors*, 23(7):3566, 2022.

[77] Alvarez, G. and Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(08):2129–2151, 2006. doi: 10.1142/S0218127406015970.

[78] Kocarev, L. and Lian, S., editors. *Chaos-Based Cryptography: Theory, Algorithms and Applications*. Springer, 2011. ISBN 978-3-642-20541-5. doi: 10.1007/978-3-642-20542-2.

[79] Pisarchik, A.N. and Flores-Carmona, N.H. Chaos in cybersecurity: A survey. *IEEE Access*, 7:29231–29258, 2019. doi: 10.1109/ACCESS.2019.2901968.

[80] Çavuşoğlu, et al. A novel chaos-based encryption algorithm over tcp/ip protocol. *Nonlinear Dynamics*, 89:1425–1438, 2017. doi: 10.1007/s11071-017-3523-0.

[81] Fridrich, J. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, 08(06):1259–1284, 1998. doi: 10.1142/S021812749800098X.

[82] Wang, X. and Chen, G. A lightweight chaos-based image encryption scheme for resource-constrained devices. *IEEE Transactions on Circuits and Systems for Video Technology*, 30(12):4584–4596, 2020. doi: 10.1109/TCSVT.2019.2963299.

[83] Rech, P.C. et al. Fpga implementation of a chaotic encryption system for real-time secure communication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 29(7):1403–1414, 2021. doi: 10.1109/TVLSI.2021.3077255.

[84] Chen, L. and Zhao, D. Lightweight audio encryption using quadratic chaos for wearables. *IEEE Sensors Journal*, 20(15):8790–8801, 2020. doi: 10.1109/JSEN.2020.2985588.

[85] Jiang, X., Xiao, Y., Xie, Y., Liu, B., Ye, Y., Song, T., Chai, J., and Liu, Y. Exploiting optical chaos for double images encryption with compressive sensing and double random phase encoding. *Optics Communications*, 484:126683, 2021.

[86] Zhou, K., Fan, J., Fan, H., and Li, M. Secure image encryption scheme using double random-phase encoding and compressed sensing. *Optics & Laser Technology*, 121:105769, 2020.

[87] Luo, Y., Zhang, L., and Ruan, H. An acquisition algorithm based on frft for weak gnss signals in a dynamic environment. *IEEE Communications Letters*, 22(6):1212–1215, 2018.

[88] Bekkouche, T. and Bouguezel, S. A recursive non-linear pre-encryption for opto-digital double random phase encoding. *Optik*, 158:940–950, 2018. doi: 10.1016/j.ijleo.2017.12.142.

[89] Kouadra, I. and Ziet, L. Nonlinear biometric pre-processing applied to image encryption scheme. 1:465–474, 2023.

[90] Oulmi, N., Bekkouche, T., Bouloufa, A., and Bey, H. An efficient nonlinear post-processing applied to image encryption. *Przegląd Elektrotechniczny*, 2023(10), 2023.

[91] Luo, Y., Zhou, R., Liu, J., Cao, Y., and Ding, X. A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. *Nonlinear Dynamics*, 93(3):1165–1181, 2018.

[92] Liu, Z., Li, S., Liu, W., Wang, Y., and Liu, S. Image encryption algorithm by using fractional fourier transform and pixel scrambling operation based on double random phase encoding. *Optics and Lasers in Engineering*, 51(1):8–14, 2013. ISSN 0143-8166. doi: 10.1016/j.optlaseng.2012.08.004.

[93] Sathiyamurthi, P. and Ramakrishnan, S. Speech encryption using chaotic shift keying for secured speech communication. *EURASIP Journal on Audio, Speech, and Music Processing*, 2017:1–11, 2017. doi: 10.1186/s13636-017-0118-0.

[94] Al-Dwairi, M.O., Hendi, A., and AlQadi, Z. An efficient and highly secure technique to encrypt-decrypt color images. *Engineering, Technology & Applied Science Research*, 9(3):4165–4168, 2019. doi: 10.48084/etasr.2525.

[95] Khan, J.S., Ahmad, J., Ahmed, S.S., Siddiqa, H.A., Abbasi, S.F., and Kayhan, S.K. Dna key based visual chaotic image encryption. *Journal of Intelligent & Fuzzy Systems*, 37(2):2549–2561, 2019.

[96] Ma, Y., Li, C., and Ou, B. Cryptanalysis of an image block encryption algorithm based on chaotic maps. *Journal of Information Security and Applications*, 54:102566, 2020.

[97] Mokhnache, A. and Ziet, L. Cryptanalysis of a pixel permutation based image encryption technique using chaotic map. *Traitement du Signal*, 37(1):95–100, 2020.

[98] Adhikari, S. and Karforma, S. A novel audio encryption method using henon–tent chaotic pseudo random number sequence. *International Journal of Information Technology*, 13(4):1463–1471, 2021. doi: 10.1007/s41870-021-00714-x.

[99] Huang, Y., Liu, Y., Lu, H., and Fu, H. A lightweight color image encryption algorithm based on fractional-order memristor chaotic system and dynamic dna coding. *Mathematics and Computers in Simulation*, 203:394–408, 2023. doi: 10.1016/j.matcom.2022.10.010.

[100] Herbadji, D., Herbadji, A., Kahia, H., Belmeguenai, A., Derouiche, N., et al. An enhanced logistic chaotic map based tweakable speech encryption algorithm. *Integration*, 97:102192, 2024. doi: 10.1016/j.vlsi.2024.102192.

[101] Benaissi, S., Chikouche, N., and Hamza, R. A novel image encryption algorithm based on hybrid chaotic maps using a key image. *Optik*, 272:170316, 2023. doi: 10.1016/j.ijleo.2022.170316.

[102] Jeevitha, S. and Prabha, N.A. Novel medical image encryption using dwt block-based scrambling and edge maps. *Journal of Ambient Intelligence and Humanized Computing*, 12:3373–3388, 2021.

[103] Shankar, K., Elhoseny, M., Chelvi, E.D., Lakshmanaprabu, S., and Wu, W. An efficient optimal key based chaos function for medical image security. *IEEE Access*, 6:77145–77154, 2018.

[104] Bao, Z., Xue, R., Hu, J., and Liu, Y. Color image encryption based on lite dense-resnet and bit-xor diffusion. *Multimedia Tools and Applications*, 2023.

[105] Farah, M.B., Guesmi, R., Kachouri, A., and Samet, M. A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation. *Optics & Laser Technology*, 121:105777, 2020.

[106] Romero-Arellano, A., Moya-Albor, E., Brieva, J., Cruz-Aceves, I., Avina-Cervantes, J.G., Hernandez-Gonzalez, M.A., and Lopez-Montero, L.M. Image encryption and decryption system through a hybrid approach using the jigsaw transform and langton's ant applied to retinal fundus images. *Axioms*, 10(3):215, 2021.

[107] Herbadji, D., Derouiche, N., Belmeguenai, A., Bekkouche, T., Labiad, A., Lashab, M., and Herbadji, A. A new image encryption scheme using an enhanced logistic map. pages 1–6, 2018.

[108] Belilita, F., Bekkouche, T., and Amardjia, N. An improved chaotic system-based 1d logistic map applied to gray scale images encryption. *Przeglad Elektrotechniczny*, 98(5), 2022.

[109] Staal, J., Abramoff, M.D., Niemeijer, M., Viergever, M.A., and Ginneken, B.V. Ridge-based vessel segmentation in color images of the retina. *IEEE Transactions on Medical Imaging*, 23(4):501–509, 2004.

[110] Farah, M.B., Farah, A., and Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics*, 99 (4):3041–3064, 2020.

[111] Romero-Arellano, A., Moya-Albor, E., Brieva, J., Cruz-Aceves, I., Avina-Cervantes, J.G., Hernandez-Gonzalez, M.A., and Lopez-Montero, L.M. Image encryption and decryption system through a hybrid approach using the jigsaw transform and langton's ant applied to retinal fundus images. *Axioms*, 10(3):215, 2021.

[112] Mehidi, I., Jabri, D., and Belkhiat, D.E.C. Retinal image segmentation u sing clustering methods: Performance analysis. In *2022 19th International Multi-Conference on Systems, Signals & Devices (SSD)*, pages 1058–1066. IEEE, 2022.

[113] Kachouri, R., Akil, M., and Elloumi, Y. Retinal image processing in biometrics. *Hidden Biometrics: When Biometric Security Meets Biomedical Engineering*, pages 167–184, 2020.

[114] Guo, M. and Liu, Y. Image encryption scheme based on chaotic map and dna sequence operations. *Security and Communication Networks*, 2020, 2020.

[115] Zhang, W. and Zhang, Q. A chaos-based image encryption algorithm with dynamic dna coding. *IEEE Access*, 8:124732–124745, 2020.

[116] Rhouma, R. and Belghith, A. Performance analysis of aes and rsa encryption algorithms in multimedia security. *Multimedia Tools and Applications*, 77:11259–11282, 2018.

[117] Al-Anzi, F. and Al-Haidari, M. A comparative study of image encryption algorithms. *Journal of Information Security and Applications*, 45:168–177, 2019.

[118] Hussain, M. and Khan, A.A. A secure image encryption scheme based on chaos and elliptic curve cryptography. *Journal of Ambient Intelligence and Humanized Computing*, 9:1241–1253, 2018.

[119] Chen, L. and Wang, X. Image encryption scheme based on combined chaotic maps and bit-level permutation. *Chaos, Solitons & Fractals*, 139:110022, 2020.

[120] et al., M.B. A new approach based on improved composite chaotic map for image encryption. *Entropy*, 23(11):1383, 2021.

[121] Yu, L. and Zhang, H. Double random phase encoding using fractional fourier transform for image encryption. *Optics Communications*, 389:74–81, 2017.

[122] et al., J.Y. A novel image encryption scheme based on chaotic maps and fractal transformations. *Signal Processing*, 196:108384, 2022.

[123] Gawish, S. and Hamdy, R. Secure image encryption based on chaos and dna encoding. *International Journal of Computer Applications*, 141(12):23–28, 2016.

[124] Amina, S. and Mohamed, F.K. An efficient and secure chaotic cipher algorithm for image content preservation. *Communications in Nonlinear Science and Numerical Simulation*, 60:12–32, 2018. doi: 10.1016/j.cnsns.2017.12.017.

[125] Vaidyanathan, S. and Volos, C. *Advances and applications in chaotic systems*, volume 636. Springer, 2016.

[126] Jensen, R.V. Classical chaos. *American Scientist*, 75(2):168–181, 1987.

[127] Pak, C., Kim, J., An, K., Kim, C., Kim, K., and Pak, C. A novel color image lsb steganography using improved 1d chaotic map. *Multimedia Tools and Applications*, 79(1):1409–1425, 2020.

[128] Trujillo-Toledo, D., López-Bonilla, O., García-Guerrero, E., Tlelo-Cuautle, E., López-Mancilla, D., Guillén-Fernández, O., and Inzunza-González, E. Real-time rgb image encryption for iot applications using enhanced sequences from chaotic maps. *Chaos, Solitons & Fractals*, 153:111506, 2021.

[129] Wang, X., Guan, N., and Yang, J. Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map. *Chaos, Solitons & Fractals*, 150:111117, 2021.

[130] Murillo-Escobar, D., Vega-Pérez, K., Murillo-Escobar, M., Arellano-Delgado, A., and López-Gutiérrez, R. Comparison of two new chaos-based pseudorandom number generators implemented in microcontroller. *Integration*, 96:102130, 2024.

[131] Wang, X. and Chen, X. An image encryption algorithm based on dynamic row scrambling and zigzag transformation. *Chaos, Solitons & Fractals*, 147:110962, 2021.

[132] Salama, G.M., El-Gazar, S., Omar, B., Nassar, R.M., Khalaf, A.A., El-Banby, G.M., Hamed, H.F., El-Shafai, W., and Abd El-Samie, F.E. Cancelable biometric system for iot applications based on optical double random phase encoding. *Optics Express*, 30(21):37816–37832, 2022. doi: 10.1364/OE.466101.

[133] Niu, Y., Zhou, Z., and Zhang, X. An image encryption approach based on chaotic maps and genetic operations. *Multimedia Tools and Applications*, 79(35):25613–25633, 2020. doi: 10.1007/s11042-020-09237-2.

[134] Pei, S.C. and Hsue, W.L. The multiple-parameter discrete fractional fourier transform. *IEEE Signal Processing Letters*, 13(6), 2006. doi: 10.1109/LSP.2006.871721.

[135] Farsana, F. and Gopakumar, K. A novel approach for speech encryption: Zaslavsky map as pseudo random number generator. *Procedia computer science*, 93:816–823, 2016. doi: 10.1016/j.procs.2016.07.302.

[136] Murillo-Escobar, M., López-Gutiérrez, R.M., Cruz-Hernández, C., Espinoza-Peralta, E.E., and Murillo-Escobar, D. Secure access microcontroller system based on fingerprint template with hyperchaotic encryption. *Integration*, 90:27–39, 2023. doi: 10.1016/j.vlsi.2023.01.002.

[137] Mebenga, V.B.E., Kopparthi, V.R., Nzeuga, H.D., Fouda, J.A.E., Dagoumguei, G.M.D., Bitjoka, G.B., Rangababu, P., and Sabat, S.L. An 8-bit integer true periodic orbit prng based on delayed arnold's cat map. *AEU-International Journal of Electronics and Communications*, 162:154575, 2023. doi: 10.1016/j.aeue.2023.154575.

[138] Yahi, A., Bekkouche, T., Daachi, M.E.H., and Diffellah, N. A color image encryption scheme based on 1d cubic map. *Optik*, 249:168290, 2022. doi: 10.1016/j.ijleo.2021.168290.

[139] Chen, Z. and Ye, G. An asymmetric image encryption scheme based on hash sha-3, rsa and compressive sensing. *Optik*, 267:169676, 2022. doi: 10.1016/j.ijleo.2022.169676.

[140] Feng, W., Zhang, J., and Qin, Z. A secure and efficient image transmission scheme based on two chaotic maps. *Complexity*, 2021(1):1898998, 2021.

[141] Khan, M.S., Ahmad, J., Al-Dubai, A., Pitropakis, N., Ghaleb, B., Ullah, A., Khan, M.A., and Buchanan, W.J. Chaotic quantum encryption to secure image data in post quantum consumer technology. *IEEE Transactions on Consumer Electronics*, 2024.

[142] Hua, Z., Zhu, Z., Yi, S., Zhang, Z., and Huang, H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Information Sciences*, 546:1063–1083, 2021. doi: https://doi.org/10.1016/j.ins.2020.09.032.

[143] Zefreh, E.Z. An image encryption scheme based on a hybrid model of dna computing, chaotic systems and hash functions. *Multimedia Tools and Applications*, 79 (33):24993–25022, 2020.

[144] Li, H., Yu, S., Feng, W., Chen, Y., Zhang, J., Qin, Z., Zhu, Z., and Wozniak, M. Exploiting dynamic vector-level operations and a 2d-enhanced logistic modular map for efficient chaotic image encryption. *Entropy*, 25(8):1147, 2023.

[145] Feng, W., Zhao, X., Zhang, J., Qin, Z., Zhang, J., and He, Y. Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform. *Mathematics*, 10(15):2751, 2022.

[146] Feng, W., Yang, J., Zhao, X., Qin, Z., Zhang, J., Zhu, Z., Wen, H., and Qian, K. A novel multi-channel image encryption algorithm leveraging pixel reorganization and hyperchaotic maps. *Mathematics*, 12(24):3917, 2024.