



تبسة في 26/06/2026

كلية العلوم و التكنولوجيا
قسم الإلكترونيك والاتصالات

إشهاد

يشهد رئيس لجنة المناقشة الخاصة بمذكرة التخرج لمستوى ماستر الموسومة بـ:

Chaotic Encryption for Secure Image Transmission
in free-space optical systems

من أنجاز الطلبة:

الرقم	الاسم واللقب	الشعبة	التخصص	السنة الجامعية
1	شوق شيماء	Telecommunication	Research Telecommunication	2026/2025
2	حمادي تسريفة			
3				

قد استكملا تصحيح الأخطاء وتقيدا بالملاحظات المقدمة من طرف لجنة المناقشة.

رئيس لجنة المناقشة

Ouacifi Malik





الجمهورية الجزائرية
الديمقراطية الشعبية



People's Democratic Republic of Algeria

وزارة التعليم العالي والبحث
العلمي

Ministry of Higher Education and Scientific Research

جامعة الشهيد لاربي التبسي
التبسي - تبسة

Echahid Cheikh Larbi Tebessi University-Tebessa

Faculty of Science and Technology

Department of Electronics and Communications



Master's Thesis

Submitted for the degree of Academic Master

Field: Telecommunications

Specialty: Networks and Telecommunications

THEME

***Chaotic Encryption for Secure Image Transmission in
Free-Space Optical Systems***

Presented by:

- Chayma CHETTOUH
- Nesrine HARBAOUI

Defended and evaluated on 09 / 06 / 2026 , by the jury composed of:

Mrs.	Malika OUACIFI	MAB	Chair
Mrs.	Hanane DJELLAB	Pr	Supervisor
Mrs.	Chaima AOUICHE	MCB	Reviewer

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Acknowledgements

First and foremost, we express our deepest gratitude to Almighty God for granting us the strength, patience, and perseverance to accomplish this work.

This thesis represents not only the culmination of a significant academic journey, but also the result of sustained effort, dedication, moments of uncertainty, and meaningful discoveries.

It reflects an experience that has profoundly contributed to our intellectual and personal growth.

Our sincere and profound appreciation is extended to our supervisor, **Pr.Djellab Hanane**, whose unwavering support, invaluable guidance, and insightful feedback were essential to the completion of this work. Her professionalism, encouragement, and confidence in our abilities have greatly influenced both the quality of this thesis and our academic development.

Particular thanks are due to **Ms.Allaoua Oumaima** and **Mr.Belhocine Yassin** for their generous assistance, technical expertise, and continuous availability. Their support and valuable contributions played a key role in facilitating the progress and successful realization of this research.

Deep appreciation is also addressed to all professors and lecturers who contributed to our academic formation. Their dedication, knowledge, and commitment to excellence have been instrumental in developing our analytical and critical thinking skills.

We also acknowledge the **Faculty of Science and Technology, especially the Department of Electronics and Telecommunications**, for providing a supportive academic environment and the necessary resources to carry out this work under optimal conditions.

We are equally indebted to the members of the thesis committee for their time, careful evaluation, and constructive remarks that enhanced the quality of this thesis. Finally, our heartfelt gratitude goes to our families and friends for their unwavering support, encouragement, and belief in us. Their presence has been a constant source of motivation and strength throughout this journey.

Dedication

Alhamdulillah,

*For everything... for strength in times of weakness, for patience
through trials,
and for the light that guided my steps until the completion of this work.*

*To myself, I dedicate this graduation project for all the efforts I have
made throughout my studies.*

*This journey was not easy, but through patience, perseverance, and
believing in my abilities,
I overcame every moment of doubt. Today, I'm proud of this major
milestone and the fruition of my dedication.*

*To my dear Father, Hamid, thank you for your unwavering trust,
endless sacrifices,
and for being the strength that kept me going through every challenge.*

*To my dear Mother, Naziha, the dearest person to my heart. Thank
you for your infinite love, endless patience,
and the prayers that guided my way.*

*To the soul of my dear grandmother, Fatima (may Allah have mercy on
her), who was like a second mother and my spiritual support.*

*To my Brothers, Youcef, thank you for bringing joy and laughter into
my life, and for being my happiest distraction during this long journey.*

*To my Sisters, Dihkra and Farah, thank you for being the shoulder I
could always lean on, the one who shares my dreams.*

*To my Family, thank you for endless encouragement and for believing
in my potential every step of my way.*

*To my Friends, for your true companionship, your motivation, and for
sharing every step with me.*

*To my thesis partner, chayma thank you for your strength and
dedication throughout this shared academic journey.*

*And to my supervisor, Ms. Hanane Djellab your guidance, patience,
and encouragement were invaluable. This work carries the mark of
your mentorship.*

Nesrine

Dedication

Alhamdulillah,

*For everything...for strength in times of weakness, for patience through trials,
and for the light that guided my steps until the completion of this work.*

To myself, I dedicate this graduation project for all the efforts I have made throughout my studies.

This journey was not easy, but through patience, perseverance, and believing in my abilities, I overcame every moment of doubt. Today, I'm proud of this major milestone and the fruition of my dedication.

*To my dear Father, Ahmed, thank you for your unwavering trust,
endless sacrifices,
and for being the strength that kept me going through every challenge.*

*To my dear Mother, Sana, the dearest person to my heart. Thank you
for your infinite love, endless patience,
and the prayers that guided my way.*

To my Brothers, Mebarek, Taher, and Zoubir, thank you for bringing joy and laughter into my life, and for being my happiest distraction during this long journey.

To my Sisters Zeyneb, thank you for being the shoulder I could always lean on, the one who shares my dreams.

To my Family, thank you for endless encouragement and for believing in my potential every step of my way.

To my Friends, for your true companionship, your motivation, and for sharing every step with me.

To my thesis partner, Nesrine thank you for your strength and dedication throughout this shared academic journey.

And to my supervisor, Ms. Hanane Djellab – your guidance, patience, and encouragement were invaluable. This work carries the mark of your mentorship.

chayma

Abstract

This work presents a secure Free-Space Optical (FSO) communication system based on a four-dimensional memristor-based hyperchaotic image encryption scheme. The proposed framework combines hyperchaotic cryptography with optical wireless communication to ensure both high-level data security and reliable image transmission under atmospheric disturbances. A 4D hyperchaotic system was designed and analyzed using time-series analysis, phase-space trajectories, and Lyapunov exponents, confirming strong randomness and high sensitivity to initial conditions. Three image encryption methods based on XOR diffusion, arithmetic addition, and QR matrix decomposition were developed and evaluated using entropy, correlation, NPCR, UACI, and key sensitivity analyses. The obtained entropy values reached 7.9987, 7.9983, and 7.9893, while NPCR values exceeded 99.55% and UACI values remained close to 33%, demonstrating excellent security performance and strong resistance against statistical and differential attacks. In addition, the proposed system provided a large key space estimated at approximately (10^{112}). The proposed encryption framework was integrated into an FSO communication system using MATLAB and OptiSystem environments. The obtained results showed that clear weather achieved the best transmission performance, maintaining BER values below (10^{-5} .) and Q-factor values above 4 up to approximately 1.6 km, with a BER of (8.68×10^{-22} .) and a Q-factor of 9.51 at 1 km. Under moderate rain conditions, the acceptable communication range decreased to approximately 1.1 km with a BER of (4.27×10^{-9} .) and a Q-factor of 5.75, while snow conditions reduced the effective range to approximately 0.4 km with a BER of (1.89×10^{-4} .) and a Q-factor of 3.56 due to severe atmospheric attenuation. Overall, the obtained results demonstrate that the proposed QR-based hyperchaotic encryption scheme provides an effective compromise between cryptographic security, diffusion capability, and transmission robustness, making the proposed framework a promising solution for next-generation secure optical wireless communication systems.

Key words: *Free-Space Optical (FSO) Communication , Physical Layer Security (PLS) , Atmospheric Turbulence , 4D Hyperchaotic System , Memristor , Image Encryption, QR Decomposition, Cumulative Modular Addition , Logical XOR , Bit Error Rate (BER).*

Résumé

Ce travail présente un système de communication optique en espace libre (FSO) sécurisé basé sur un schéma de chiffrement d'images hyperchaotique à quatre dimensions utilisant un memristor. Le cadre proposé combine la cryptographie hyperchaotique avec les communications optiques sans fil afin d'assurer à la fois un haut niveau de sécurité des données et une transmission fiable des images sous différentes perturbations atmosphériques. Un système hyperchaotique 4D a été conçu et analysé à l'aide de l'analyse temporelle, des trajectoires de l'espace des phases et des exposants de Lyapunov, confirmant une forte sensibilité aux conditions initiales ainsi qu'un comportement hautement aléatoire. Trois méthodes de chiffrement d'images basées sur la diffusion XOR, l'addition arithmétique et la décomposition matricielle QR ont été développées et évaluées à l'aide de plusieurs métriques de sécurité telles que l'entropie, la corrélation, le NPCR, l'UACI et l'analyse de sensibilité à la clé. Les valeurs d'entropie obtenues ont atteint 7.9987, 7.9983 et 7.9893, tandis que les valeurs de NPCR ont dépassé 99.55% et les valeurs de UACI sont restées proches de 33 %, démontrant d'excellentes performances de sécurité et une forte résistance aux attaques statistiques et différentielles. De plus, le système proposé offre un espace de clés très large estimé à environ (10^{112}). Le schéma de chiffrement proposé a ensuite été intégré dans un système FSO utilisant les environnements MATLAB et OptiSystem. Les résultats obtenus ont montré que les conditions de ciel clair offrent les meilleures performances de transmission, avec des valeurs de BER inférieures au seuil acceptable de (10^{-5} .) et un facteur Q supérieur à 4 jusqu'à environ 1.6 km, avec un BER de (8.68×10^{-22}) et un facteur Q de 9.51 à une distance de 1 km. Sous une pluie modérée, la portée de communication acceptable diminue à environ 1,1 km avec un BER de ($4,27 \times 10^{-9}$) et un facteur Q de 5,75, tandis que les conditions de neige réduisent la portée effective à environ 0,4 km avec un BER de ($1,89 \times 10^{-4}$.) et un facteur Q de 3,56 en raison de la forte atténuation atmosphérique. Globalement, les résultats obtenus démontrent que la méthode de chiffrement hyperchaotique basée sur la décomposition QR offre un compromis efficace entre sécurité cryptographique, capacité de diffusion et robustesse de transmission, faisant du système proposé une solution prometteuse pour les futures communications optiques sans fil sécurisées.

Mots clés: *Communication optique en espace libre (FSO), sécurité de la couche physique (PLS), turbulences atmosphériques, système hyperchaotique 4D, memristor, cryptage d'images, décomposition QR, addition modulaire, taux d'erreur binaire (BER).*

الملخص

يقدم هذا العمل نظام اتصال بصري لاسلكي آمن في الفضاء الحر (FSO) يعتمد على تشفير الصور باستخدام نظام فائق الفوضوية رباعي الأبعاد قائم على الميمريستور. تم تطوير ثلاث تقنيات تشفير تعتمد على الانتشار، XOR والجمع المعياري، وتحليل QR، مع تقييمها بواسطة مؤشرات أمنية متعددة أثبتت كفاءة عالية في مقاومة الهجمات الإحصائية والتفاضلية. أظهرت النتائج قيمة مرتفعة للإنتروبيا قاربت 8، إضافة إلى قيم NPCR تجاوزت 99.55% و UACI قريبة من 33%، مما يؤكد قوة التشفير وحساسيته العالية للمفاتيح الابتدائية. كما تم دمج نظام التشفير ضمن قناة FSO باستخدام MATLAB و OptiSystem لدراسة أداء الإرسال تحت تأثير الظروف الجوية المختلفة. بينت النتائج أن السماء الصافية توفر أفضل أداء مع BER منخفض جداً وعامل Q مرتفع، بينما تؤدي الأمطار والثلوج إلى تقليص مدى الاتصال بسبب التوهين الجوي. وتؤكد الدراسة أن تقنية التشفير المعتمدة على تحليل QR تحقق توازناً فعالاً بين الأمان التشفيري وموثوقية الإرسال، مما يجعلها حلاً واعداً لأنظمة الاتصالات البصرية اللاسلكية الآمنة مستقبلاً.

الكلمات المفتاحية: الكلمات المفتاحية: الاتصالات البصرية في الفضاء الحر، (FSO) أمن الطبقة الفيزيائية، (PLS) الاضطرابات الجوية، نظام فائق الفوضوية رباعي الأبعاد، الميمريستور، تشفير الصور، تحليل QR، الجمع المعياري، معدل خطأ البتات. (BER)

Contents

Abbreviations	ix
General introduction	1
1 Fundamentals of Free-Space Optical Communication and Security	3
1.1 Introduction	3
1.2 FSO System Architecture	4
1.2.1 Overview about FSO communicatio	4
1.2.2 Advantages and Limitation	4
1.2.3 FSO architecture	8
1.2.4 FSO Security	10
1.3 Atmospheric Channel Modeling	11
1.3.1 Atmospheric effects	11
1.3.2 Channel Models	14
1.4 Performance Metrics (BER, SNR, Q-factor)	15
1.4.1 Bit Error Rate (BER)	15
1.4.2 Signal-to-Noise Ratio (SNR)	15
1.4.3 Q Factor	16
1.5 Physical Layer Security	16
1.5.1 Concept of Physical Layer Security	16
1.5.2 Importance of PLS in FSO Systems	17
1.5.3 Working Principle of PLS	17
1.5.4 Techniques Used in PLS	17
1.5.5 Advantages of PLS	18
1.5.6 OWC Security Vulnerabilities	18
1.6 Chaos-Based Encryption in Optical Systems	20
1.6.1 Importance of Chaos/Hyperchaos in FSO	20
1.6.2 Application of Fso	20
1.7 Conclusion	21

2	Memristor-Based 4D Hyperchaotic System&Image Encryption Scheme	22
2.1	Introduction	22
2.2	State of the Art of Chaos and Hyperchaotic Cryptography	23
2.3	Fundamentals of Chaos and Hyperchaos	24
2.3.1	Chaotic systems	24
2.3.2	Hyperchaotic systems	24
2.3.3	Properties of Hyperchaotic systems	24
2.3.4	Comparaison between chaotic and hyperchaotic systems.	27
2.4	Electronic Circuit Realization and Mathematical Model	27
2.4.1	Overview about circuit	27
2.4.2	Derivation of the Mathematical Model	28
2.4.3	Dynamical Analysis	31
2.5	Hyperchaotic Key Generation Mechanism	32
2.5.1	Initialization of the Hyperchaotic System	32
2.5.2	Chaotic Sequence Generation	33
2.6	Proposed Image Encryption Algorithm	33
2.6.1	Method 1 : XOR-Based Diffusion Scheme	34
2.6.2	Method 2: Cumulative Modular Addition-Based Diffusion Scheme	35
2.6.3	Method 3: QR Decomposition Scheme	37
2.7	Cryptographic Performance Evaluation	39
2.7.1	Key Space Analysis	39
2.7.2	Key Sensitivity Analysis	40
2.7.3	Histogram Analysis	40
2.7.4	Correlation of Adjacent Pixels (Horizontal, Vertical, Diagonal) .	40
2.7.5	Information Entropy Analysis	41
2.7.6	Differential Attack Analysis (Primary Criteria: NPCR , UACI)	42
2.7.7	Robustness Against Noise and Data Loss	43
2.7.8	Resistance to Statistical Attacks	43
2.7.9	Randomness	44
2.7.10	Overall Security Evaluation	44
2.8	Conclusion	44
3	Design and Simulation of secure FSO system	46

List of Figures

1.1	A typical block diagram of an FSO system	6
1.2	Mech architecture	9
1.3	Point-to- Multipoint Architecture	10
1.4	Multiple PTP Architecture	10
1.5	Illustration of jamming, eavesdropping, spoofing, DDoS, and other attacks	19
2.1	Illustration of the Butterfly effect	25
2.2	Illustrate the circuit modules implemented based on the system de- scribed by Equation (19): (a) $\tilde{X}_1$, (b) $\tilde{X}_2$, (c) $\tilde{X}_3$, (d) $\tilde{X}_4$ and the memristor circuit module [17]	28
2.3	Bloc A of electronic circuit	29
2.4	Bloc B of electronic circuit	29
2.5	Bloc C of electronic circuit	30
2.6	Bloc D of electronic circuit	31

List of Tables

2.1 Differences between chaos and hyperchaos [23, 24] 27

list of Abbreviations

FSO	Free Space Optics
RF	Radio Frequency
LOS	Line of Sight
NLOS	Non-Line of Sight
BER	Bit Error Rate
SNR	Signal-to-Noise Ratio
OSNR	Optical Signal-to-Noise Ratio
FEC	Forward Error Correction
RX	Receiver
TX	Transmitter
LD	Laser Diode
LED	Light Emitting Diode
PD	Photodiode
APD	Avalanche Photodiode
PIN	Positive Intrinsic Negative Photodiode
PTP	Point-to-Point
PMP	Point-to-Multipoint
LMDS	Local Multipoint Distribution Service
PDF	Probability Density Function
CDF	Cumulative Distribution Function
Q-Factor	Quality Factor
DWDM	Dense Wavelength Division Multiplexing
NRZ	Non-Return-to-Zero
MZM	Mach–Zehnder Modulator
OAM	Orbital Angular Momentum
MIMO	Multiple Input Multiple Output

PLS	Physical Layer Security
OWS	Optical Wireless System
VLC	Visible Light Communication
LiFi	Light Fidelity
LiDAR	Light Detection and Ranging
OCC	Optical Camera Communication
LANs	Local Area Networks
SANs	Storage Area Networks
ISPs	Internet Service Providers
5G	Fifth Generation
6G	Sixth Generation
4D	Four-Dimensional
5D	Five-Dimensional
ROI	Region of Interest
FPGA	Field Programmable Gate Array
MATLAB	Matrix Laboratory
XOR	Exclusive OR
UACI	Unified Average Changing Intensity
NPCR	Number of Pixel Change Rate
LE	Lyapunov Exponent
KCL	Kirchhoff's Current Law
DC	Direct Current
DoS	Denial of Service
DDoS	Distributed Denial of Service
IMS	Information Management System
DSP	Digital Signal Processing

General introduction

The rapid advancement of information and communication technologies has considerably increased the exchange of multimedia data, particularly digital images, over modern communication networks. This evolution has created new challenges for communication systems, which are required to ensure not only high transmission capacity and reliability, but also strong data security. Although traditional Radio Frequency (RF) communication systems remain widely used, they suffer from several limitations such as limited bandwidth, spectrum congestion, and sensitivity to electromagnetic interference. These constraints have motivated researchers to explore alternative wireless communication technologies capable of supporting the increasing demands of next-generation communication systems. Free-Space Optical (FSO) communication has emerged as a promising alternative to conventional RF systems due to its high data rate, large bandwidth, low deployment cost, and immunity to electromagnetic interference. However, the performance and reliability of FSO systems remain highly affected by atmospheric conditions such as fog, rain, snow, scattering, absorption, and turbulence, which can significantly attenuate the optical signal and degrade transmission quality. At the same time, ensuring the security of multimedia information has become a major research challenge. Conventional encryption algorithms may not always be suitable for image encryption because of their computational complexity and limited resistance against advanced cryptographic attacks. Consequently, chaos-based and hyperchaos-based cryptographic techniques have attracted considerable attention in recent years due to their strong randomness, nonlinear behavior, ergodicity, and high sensitivity to initial conditions. These properties make chaotic systems highly suitable for secure image encryption applications. More recently, memristor-based hyperchaotic systems have been introduced as advanced nonlinear dynamical models capable of generating more complex and unpredictable chaotic behavior. Compared with conventional chaotic systems, hyperchaotic systems possess higher dimensional complexity, multiple positive Lyapunov exponents, and larger key spaces, which significantly improve resistance against statistical, differential, and brute-force attacks. Despite the significant progress achieved in both FSO communication and chaos-based cryptography, ensuring reliable and secure image transmission over atmospheric optical wireless channels remains a major challenge. Atmospheric impairments can con-

siderably degrade transmission quality, while weak encryption structures may expose sensitive information to interception and unauthorized access. Therefore, developing an integrated framework capable of simultaneously guaranteeing communication reliability and high-level data security has become an important research issue in modern optical wireless communication systems. Therefore, the main objective of this work is to develop a secure and efficient FSO communication system integrating a four-dimensional memristor-based hyperchaotic image encryption scheme for reliable image transmission under various atmospheric conditions. The principal contributions of this work can be summarized as follows:

- Design and modeling of a four-dimensional memristor-based hyperchaotic system characterized by high dynamical complexity.
- Development of three image encryption methods based on XOR diffusion, arithmetic addition diffusion, and QR matrix decomposition techniques.
- Comprehensive cryptographic performance evaluation using entropy, histogram analysis, correlation analysis, NPCR, UACI, and key sensitivity tests.
- Integration of the proposed hyperchaotic encryption scheme into a secure FSO communication system using MATLAB and OptiSystem environments.
- Performance evaluation of the proposed secure FSO system under different atmospheric conditions using BER, Q-factor, and eye diagram analysis.

The obtained results demonstrated that the proposed system provides strong cryptographic security and reliable FSO transmission performance, even under atmospheric impairments such as rain and snow, with the QR-based encryption method showing superior robustness and diffusion capability. This thesis is organized into three chapters covering the fundamentals of FSO communication systems, the design of the proposed memristor-based hyperchaotic encryption scheme, and the implementation and performance evaluation of the secure FSO communication system under different atmospheric conditions. Overall, this work contributes to the development of next-generation secure optical wireless communication systems combining high transmission efficiency with advanced multimedia data protection.

Chapter 1

Fundamentals of Free-Space Optical Communication and Security

1.1 Introduction

Telecommunication technology has witnessed significant development in recent years, leading to an increasing demand for faster, more reliable, and secure data transmission systems. Despite the widespread use of traditional radio frequency (RF)-based communication technologies, they face challenges such as spectrum congestion and high infrastructure costs, which have prompted researchers to explore more efficient and effective alternatives [1, 3]. Among these alternatives, Free Space Optical (FSO) communication has emerged as a promising solution for modern wireless communications. This technology relies on data transmission using light along a line-of-sight (LOS) path, offering high data rates, ease of installation, and operation within an unlicensed spectrum, making it suitable for various applications such as last-mile connectivity, backhaul links, and inter-building communication [1, 3, 4]. Despite these advantages, the performance of FSO systems remains dependent on environmental conditions, as atmospheric phenomena can affect signal quality and system efficiency [7]. Moreover, although these systems can provide a good level of security, they are still susceptible to certain threats such as eavesdropping, jamming, spoofing, and denial-of-service (DoS) attacks [9]. To address these challenges, advanced techniques have been developed to enhance the security and reliability of data transmission, particularly at the physical layer, by exploiting channel characteristics to improve data confidentiality and reduce the probability of interception [13]. Additionally, there has been a shift towards using encryption techniques based on chaotic and hyperchaotic systems, which provide a high level of security by expanding the key space and increasing resistance to analytical attacks [13, 14]. This chapter provides a clear and concise foundation for understanding Free-Space Optical (FSO) communication and its security aspects. It covers the sys-

tem architecture, including optical transmitters, propagation channels, and receivers, and examines the impact of atmospheric effects such as scattering, absorption, and turbulence on signal quality and performance. Key performance metrics, including bit error rate (BER), signal-to-noise ratio (SNR), and link availability, are discussed, along with physical layer security and chaos-based encryption techniques to protect the confidentiality of transmitted data. Overall, the chapter addresses the central question: how can FSO systems to achieve high- performance, reliability , and security despite atmospheric challenges using chaos-based encryption?

1.2 FSO System Architecture

1.2.1 Overview about FSO communicatio

Free Space Optical (FSO) communications is a wireless communication technology that transmits data using light beams, typically in the form of lasers, through a free medium such as air or vacuum, without requiring physical media like optical fibers. This technology relies on a direct line-of-sight between the transmitter and the receiver, where the optical signal travels directly to convey information [1, 2]. FSO represents an extension of traditional optical communication systems, sharing the principle of using light for data transmission, with the key difference being the propagation medium—where transmission occurs through free space rather than optical fibers. It is also referred to as wireless optical communication or laser communication. FSO can achieve high data rates due to the large bandwidth of the optical spectrum and offers fast and easy deployment compared to wired systems. However, its performance depends primarily on the clarity of the optical path and the absence of obstacles or atmospheric effects [4, 7].

1.2.2 Advantages and Limitation

1.2.2.1 Advantages: FSO communication offers the following advantages

- **High bandwidth:** : FSO offers a bandwidth close to 2000 THz. witch allows the system to transmit a large amount of data and achieve high channel capacity.
- **Narrow optical beam:** In FSO systems, a laser is used at the transmitter. As a result, the transmitted beam is very narrow, which increases security because it is more to intercept compared to RF systems.
- **Operation in the ISM band:** FSO operates in the ISM band, which is unlicensed. Therefore, there is no need to obtain a spectrum license.

- **Low cost of installation:** The installation cost of an FSO system is generally lower than that of RF systems when both operate at the same data rate.
- **Simple and quick deployment:** The system can be installed in a short period of time, sometimes within a few hours. It can also be removed and installed again in another place without difficulty[4].

1.2.2.2 Limitation:

- **Physical obstructions:** Objects such as birds, trees, or tall buildings can occasionally block the line of sight (LOS).
- **Scintillation:** This phenomenon is caused by Temperature variation in air pockets whether due to heat rising from the ground or human related sources such as heating systems.
- **Geometric losses:** Also referred to as optical beam attenuation, these losses occur due to the beam divergence. This results in a reduction in signal powers it travels from the transmitter to the receiver.
- **Absorption:** This effect is caused by the water molecules suspended in the terrestrial atmosphere.
- **Atmospheric turbulence:** This phenomenon is caused by weather conditions and environmental variations. Convection and wind force air parcels to mix at different temperatures, leading to fluctuations in air density. This, in turn, causes the refractive index of the air to vary, affecting signal propagation [5].

FSO Communication System

FSO systems are considered among the most important technologies in modern communication systems. They operate by transmitting data using light over a direct line-of-sight (LOS) path, either through the atmosphere or in outer space. As illustrated in Figure 1.1, an FSO system is composed of three main components: The transmitter (Tx), the propagation channel, and the receiver (Rx). The transmitter is responsible for sending the data, while the receiver detects and processes the received optical signal. Each of these components plays a crucial role in ensuring that the optical signal propagates efficiently and reliably from one point to another [6].

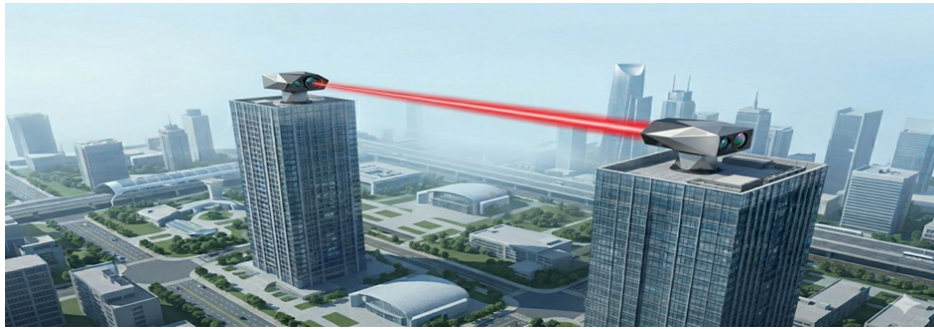


Figure 1.1: A typical block diagram of an FSO system

1.2.3.1 Transmitter Side

1.2.3.1.1 Transmitter

The transmitter is responsible for converting the electrical signal into an optical signal and modulating the laser beam in order to transmit data to the receiver through the atmospheric channel. As illustrated in figure 1.1, the transmitter is composed of four main components: the laser modulator, the driver circuit, the optical source, and the transmitting telescope.

1.2.3.1.2 Optical Modulator

Optical modulation is the process through which information is encoded onto a laser beam. In general, two main modulation techniques are used: internal modulation and external modulation.

- **Direct modulation** :occurs inside the laser resonator. In this method, changes in the internal components alter the intensity of the laser beam according to the transmitted information signal.
- **External modulation** : takes place outside the laser resonator and relies mainly on physical phenomena such as polarization and refractive index variations to encode the information onto the optical signal.

1.2.3.1.3 Optical Source

The optical source can be either a laser diode (LD) or a light-emitting diode (LED). These devices are used to convert electrical signals into optical signals suitable for transmission. A laser diode generates optical radiation through the stimulated emission process, in which photons are emitted from atoms or molecules in a lasing medium that have been excited from a lower energy state to a higher energy level. The emitted light is highly monochromatic and strongly directional, which means it has a narrow spectral width and a very small beam divergence. Moreover, the emitted light waves maintain a constant phase, indicating a high degree of coherence.

1.2.3.1.4 Laser Source Selection Criteria for FSO

The choice of a suitable laser source for Free Space Optical (FSO) communication systems depends on several important factors. These parameters help determine the performance of the optical source in a specific application. The main factors include .

- **Cost and availability of commercial components**
- **Transmission power and operational lifetime**
- **Modulation capability**
- **Eye safety considerations**

1.2.3.1.5 Transmitter Telescope

The transmitting telescope is used to collect, collimate, and direct the optical beam toward the receiver telescope located at the other end of the communication link[7].

1.2.3.2 FSO channel

In Free Space Optical (FSO) communication, the propagation medium is the Earth's atmosphere. The atmosphere can be modeled as a series of concentric gaseous layers surrounding the planet. Within the homosphere, three main atmospheric layers are identified: the troposphere, stratosphere, and mesosphere. These layers are distinguished primarily by their temperature gradients as a function of altitude.

FSO systems are particularly concerned with the troposphere, as it contains most of the weather phenomena that directly affect optical propagation, and FSO links typically operate in the lower portion of this layer. The atmosphere is mainly composed of nitrogen (N_2 , 78%), oxygen (O_2 , 21%), and argon (Ar, 1%), with smaller contributions from other gases such as water vapor (H_2O , 0–7%) and carbon dioxide (CO_2 , 0.01–0.1%). Additionally, the atmosphere contains aerosol particles including dust, haze, fog, and soil particuls, which can impact optical transmission.

The propagation characteristics of FSO links are highly dependent on environmental conditions, particularly weather related effects, which can cause fluctuations and attenuation of the received optical signal. Atmospheric attenuation occurs due to interactions between the laser beam and both air molecules and aerosols particles along the propagation path. The main phenomena affecting FSO performance include absorption, scattering, and scintillation, all of which can significantly degrade the received signal power and reduce overall system reliability.

1.2.3.3 Receiver:

The receiver in an FSO system is responsible for capturing the optical signal from the free-space channel and converting it back into an electrical signal for further processing. The receiver optics typically consist of five main components ,namely: the receiver telescope, optical filter, photodetector, amplifier, and demodulator.

1.2.3.3.1 Receiver Telescope

The receiver telescope collects the incoming optical radiation and focuses it onto the photodetector. A larger telescope aperture is preferred, as it captures multiple uncorrelated rays and averages them, thereby enhancing the effective signal power received by the photo detector.

1.2.3.3.2 Optical Filter

Optical filters are employed to allow primarily the desired wavelength to reach the detector while rejecting unwanted wavelengths. This significantly reduces the impact of solar illumination and background noise thereby improving the quality of the received signal.

1.2.3.3.3 Detector (Photodiode)

The photodetector, commonly a photodiode (PD), is a semiconductor device that converts photon energy into an electrical current. It operates on the principle of photoconductivity, where the conductivity of a p-n junction increases due to absorption of electromagnetic radiation. Photodiodes are generally reverse-biased to enhance performance and are designed to store charge capacitively. The most widely used types in FSO systems are the PIN photodiode and the Avalanche Photodiode (APD), both valued for their high quantum efficiency and commercial availability.

1.2.3.3.4 Amplifier and Demodulator

After detection, the amplifier strengthens the electrical signal, while the demodulator extract(recovers) the transmitted data from the modulated optical signal, completing the reception process [7].

1.2.3 FSO architecture

FSO systems can be designed to operate in various type of network topologies, such as mesh, point-to-point (PTP), point- to-multipoint (PMP), or ring networks. This enables metropolitan service providers the to quickly deployed and easily expand their

networks, while delivering data rates comparables to fiber-optic systems to modern users .

1.2.4.1 Mech architecture

A mesh network consists of multiple interconnected device, where each device can an communicate directly with another device or forward data through intermediate nodes when necessary.As the number of devices increases, the network becomes more robust. It is easy to add new devices, and even if some nodes fail, the network can continue to operate because data can be routed through alternative paths.



Figure 1.2: Mech architecture

1.2.4.2 Point-to-Multipoint Architecture

In this architecture, a node is designated as central transmitter, and multiple links are established. The most common approach is that each free-space optical link is connected to a layer 2 or 3 device in a building communication room. The links are then fiber-coupled and positioned atvarious locations, either on top of a building or inside a room or office. An attempt has been made to sectorize the optical beam to serve multiple customers from a single node, similar to the LMDS system. However, this architecture is limited in power due to regulatory constraints. The Point-to-Multipoint Architecture, as depicted in Figure 1.3, provides cost- effective connectivity and allows easier network expansion, but it offers lower bandwidth compared to point-to-point systems.

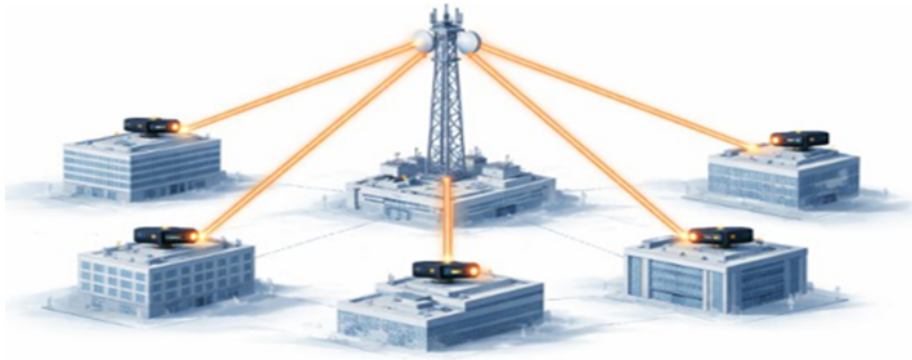


Figure 1.3: Point-to- Multipoint Architecture

1.2.4.3 Multiple PTP Architecture

The multiple PTP architecture depicted in figure 1.4 is used in scenarios where it is necessary to establish an extended communication link path that exceeds the standard transmission range and the recommended weather-constrained distance of a single optical link. This architecture consists of multiple point-to-point links connected in sequence, providing a dedicated communication path with higher bandwidth and improved reliability [3].



Figure 1.4: Multiple PTP Architecture

1.2.4 FSO Security

Free Space Optics has various applications, and one of its important aspects is the associated security considerations. FSO systems operate in unregulated optical spectrum bands, and like all wireless communication technologies, they are subject to various security risks. Data interception is one of the primary concerns. In general, the larger and more dispersed a signal is, the more likely it is to be intercepted by an unauthorized entity. The optical beam is highly directional and narrow compared to conventional wireless communication systems. This beam remains confined throughout the transmission path, thereby reducing the probability of interception. Another advantage of

FSO is that it does not produce side lobes. Side lobes refer to unintended radiation emitted in directions other than the main beam, which may carry the same transmitted information. In traditional wireless systems, these side lobes can be exploited by unauthorized users to intercept data. However, FSO systems significantly minimize or eliminate side lobes, thus enhancing communication security[3].

1.3 Atmospheric Channel Modeling

1.3.1 Atmospheric effects

When light travels through the air in optical wireless systems such as Free Space Optics (FSO) it encounters a complex and often unpredictable medium—the atmosphere. Wireless systems utilizing FSO technology face several challenges due to environmental conditions.. The primary limitation of free-space optical communications is directly related to the atmospheric conditions through which the optical signal propagates.. Although FSO systems are generally resilient to rain and snow, they can be significantly affected by fog and atmospheric fluctuations[3].

1.3.1.1 Atmospheric attenuation

Atmospheric attenuation refers to the phenomenon in which part or all of the electromagnetic wave energy is reduced as it propagates through the atmosphere. Consequently, the atmosphere can cause to signal degradation in FSO link through various mechanisms, such as absorption, scattering, and scintillation. Each of these effects varies over time and depends on local weather conditions. Atmospheric attenuation is commonly modeled using Beer lambert law as expressed in equation (1.1):

$$\tau = \exp(-\beta L) \quad (1.1)$$

Where:

- τ : the atmospheric attenuation.
- L : the distance between (Tx) and (Rx) in kilometer.
- β : is the total attenuation coefficient given as

$$\beta = \beta_{abs} + \beta_{scat} \quad (1.2)$$

- β_{abs} : the molecular and aerosol absorption.
- β_{scat} : the molecular and aerosol scattering.

1.3.1.2 Absorption

Atmospheric absorption occurs when photons from the optical beam interact with particles and molecules present in the atmosphere. These include water vapor, dust, ice crystals, and various suspended compounds. Certain atmospheric gases exhibit strong absorption in the infrared region, particularly H_2O , O_2 , O_3 , and CO_2 . This process reduces the transmitted optical power, thereby decreasing the link margin, limiting the communication range, and degrading the reliability of the FSO link. The absorption coefficient depends mainly on the nature and concentration of atmospheric gases. Molecular absorption is wavelength-dependent and occurs selectively at specific spectral regions. As a result, the atmosphere contains transmission windows, where attenuation is minimal and optical signals can propagate more efficiently. Although nitrogen and oxygen are the dominant atmospheric components, their contribution to infrared absorption is relatively negligible. The absorption coefficient can be estimated using:

$$\beta_{abs} = \alpha_{abs} N_{abs} \left[\frac{1}{km} \right] \quad (1.3)$$

Where:

- α_{abs} : is the effective cross section of the absorption particles km^2 .
- N_{abs} : is the concentration of the absorption particles $\left[\frac{1}{km^3} \right]$.

1.3.1.3 Scattering

Scattering is the process in which an electromagnetic wave is deviated in multiple directions after interacting with atmospheric particles. When a wave encounters a particle, part of its energy is absorbed and then re-emitted in various directions. The scattered radiation maintains the same wavelength as the incident wave and is typically polarized. Atmospheric scattering is classified into three categories: Rayleigh scattering, Mie scattering, and non-selective scattering. The type of scattering that occurs depends mainly on the relationship between the wavelength of the optical signal and the size of the atmospheric particles [7].

1.3.1.3.1 Rayleigh scattering

Rayleigh scattering occurs when light interacts with particles much smaller than the wavelength of the incident wave. This phenomenon is highly wavelength-dependent, with shorter wavelengths being scattered more strongly than longer ones. Its effect decreases rapidly with increasing wavelength and becomes negligible in the infrared region. Therefore, it mainly affects ultraviolet and visible light.

1.3.1.3.2 Mie scattering

Mie scattering occurs when particles size are comparable to the wavelength of the optical signal. In terrestrial FSO communication, it is the primary cause of attenuation for wavelengths between 0.5 μm and 2 μm . Fog and haze significantly weaken optical signals, with fog having the most severe impact. The level of scattering depends on aerosol concentration, size, and distribution, which vary over time and location. Scattering can be estimated using visibility measurements, with higher attenuation occurring under low visibility conditions.

1.3.1.3.3 Rain

Rain consists of droplets whose size and shape vary depending on environmental conditions. Smaller droplets are typically spherical, while larger ones become flattened. Rain-induced scattering is considered non-selective, as raindrop sizes (100–1000 μm) are much larger than the wavelengths used in FSO systems. Therefore, optical beams generally pass through raindrops with relatively low attenuation. Compared to haze, rain has a less significant impact on FSO signals. Interestingly, RF systems operating above 10 GHz are more affected by rain than fog due to wavelength similarity with raindrop size.

1.3.1.4 turbulence

Clear-air turbulence affects optical beams propagation due to random fluctuations in the refractive index caused by variations in temperature, pressure, and wind. The results in phase distortions of the optical wave front(optical aberrations)and intensity fluctuations known as scintillation. Turbulent eddies act like random lenses, causing unpredictable bending of the wave, which leads to both amplitude fluctuations and wave front distortion Scintillation Scintillation is one of the most significant impairments in FSO systems. As light propagates through turbulent regions, its intensity fluctuates rapidly, even over short distances. These fluctuations degrade signal quality and are directly caused by refractive index variations along the propagation path.

- **Beam spreading**

Beam spreading refers to the increase in beam width beyond its diffraction-limited value due to atmospheric turbulence As the beam propagates, turbulence causes it to expand, reducing peak intensity and altering the irradiance distribution at the receiver [7].

1.3.2 Channel Models

The Gamma-Gamma scintillation model, based on doubly stochastic theory, is widely recognized in the scientific literature. This model is commonly used to describe atmospheric turbulence conditions, ranging from weak to strong turbulence regimes. In this model, the probability density function (PDF) of the received intensity I is expressed as the product of two random variables following a Gamma distribution. These two variables represent the intensity fluctuations caused by:

- **small-scale turbulence effects**
- **large-scale turbulence effects**

If these random variables are denoted X and Y , the received intensity can be written as:

$$I = XY \quad (1.4)$$

Where:

- X : represents fluctuations due to small scale turbulent eddies .
- Y : represents fluctuations due to large scale turbulent structures in the atmosphere [10].

1.3.2.1 Log-Normal Model

The Log-Normal channel model is widely used for weak atmospheric turbulence conditions in Free Space Optical (FSO) communication. It assumes that the optical irradiance follows a log-normal distribution, which is suitable for relatively stable weather conditions with minor temperature or wind variations. This model allows the estimation of the scintillation index and the probability of signal fading in the channel .

1.3.2.2 Negative Exponential Model

The Negative Exponential model is applied under strong turbulence or saturation conditions. In this model, the optical irradiance follows an exponential distribution, reflecting large fluctuations in received optical power under extreme weather conditions such as heavy fog or rain. It is particularly useful for analyzing FSO system performance in harsh atmospheric environments [11].

1.3.2.3 Málaga (M-distribution) model

The Málaga (M-distribution) model is a generalized statistical model for FSO channels that can represent all levels of turbulence, from weak to very strong regimes. It includes several simpler distributions as special cases, such as Gamma-Gamma, K-distribution, log-normal, and negative exponential. This model can also account for pointing errors between the transmitter and receiver. Studies have shown that the Málaga model provides a more accurate representation of optical irradiance fluctuations and enables detailed performance analysis, including probability density function (PDF), cumulative distribution function (CDF), bit error rate (BER), outage probability, and ergodic capacity, in realistic FSO environments[12].

1.4 Performance Metrics (BER, SNR, Q-factor)

1.4.1 Bit Error Rate (BER)

This tool (visualizer) is used to automatically calculate and display the Bit Error Rate (BER) of an electrical signal. It can estimate the BER using different algorithms, such as Gaussian and Chi-Square distributions. It also extracts several parameters from the eye diagram, including the Q factor, eye opening, eye closure, extinction ratio, eye height, and jitter. In addition, the system takes into account the effect of Forward Error Correction (FEC), displays BER patterns, and estimates system penalties and operating margins. BER is a measure of the quality of the received signal in digital transmission systems. In an FSO system, BER reflects the reliability of data transmission. The Algorithm parameter specifies the numerical method used to calculate the BER. When Gaussian noise is assumed, with standard deviations σ_0 and σ_1 , the BER is given by [8]:

$$P_e = \left(\frac{M}{N + M} \right) P_{e0} + \left(\frac{N}{N + M} \right) P_{e1} \quad (1.5)$$

1.4.2 Signal-to-Noise Ratio (SNR)

In wireless optical systems, The signal-to-noise ratio for an FSO system is calculated as:

$$SNR_{FSO} = \frac{S}{N} \quad (1.6)$$

Where:

- S :represents the received signal power (typically at a wavelength of $\lambda = 1550$ nm)

- N : represents the total noise power , which may arise from atmospheric turbulence, temperature variations, and other disturbances.

1.4.3 Q Factor

The Quality Factor (Q Factor) measures the level of noise affecting a signal pulse and is mainly used for diagnostic purposes. When using an eye- diagram oscilloscope, the device typically generates a report showing the Q Factor value. The Q Factor indicates the relationship between the signal and noise levels required to achieve a specific bit error rate (BER) for a given signal. In optical systems, the optical SNR (OSNR) is measured in decibels (dB). In general, higher bit rates require a higher OSNR. The Q Factor is an important parameter that reflects the performance of a communication channel. It represents the quality of signal detection in digital optical communication systems and helps evaluate overall system performance. There are two ways to calculate the Q Factor. One method is based on the the BER , as expressed below: where:

$$P_e = \frac{1}{2} \operatorname{erfc} \left(\frac{Q}{\sqrt{2}} \right) \quad (1.7)$$

It can also be calculated from signal levels as follows:

Where:

$$Q = \frac{|\mu_1 - \mu_0|}{\sigma_1 + \sigma_0} \quad (1.8)$$

- μ_1 and μ_0 represent the mean signal levels corresponding to logical “1” and “0”.
- σ_1 and σ_0 represent the standard deviations of the noise for logical “1” and “0”[8].

1.5 Physical Layer Security

1.5.1 Concept of Physical Layer Security

Physical Layer Security (PLS) is a communication security approach that utilizes the physical characteristics of the transmission channel to protect information. Instead of relying solely on conventional cryptographic techniques, PLS exploits the inherent properties of the communication medium. Its main objective is to ensure that an unauthorized listener cannot successfully decode the transmitted data, even if the signal is intercepted [13].

1.5.2 Importance of PLS in FSO Systems

Free Space Optical (FSO) communication systems transmit information through the atmosphere using laser beams. These systems offer several important advantages, including:

- **High data transmission rates**
- **Large bandwidth**
- **Low latency**

However, these advantages also introduce potential security vulnerabilities, which makes the integration of PLS techniques essential to ensure secure communication.

1.5.3 Working Principle of PLS

The operation of Physical Layer Security is based on exploiting the inherent properties of the communication channel., such as:

- **Noise**
- **Fading**
- **Atmospheric turbulence**

By leveraging these characteristics effectively, the signal received by the legitimate receiver can be enhanced, while the signal quality at the eavesdropper is significantly degraded, thereby improving communication security.

1.5.4 Techniques Used in PLS

Various techniques can be employed to enhance security at the physical layer, including:

- **Beamforming**
- **Artificial Noise**
- **Orbital Angular Momentum (OAM)**
- **Multiple-Input Multiple-Output (MIMO)**

These approaches help increase the secrecy capacity of the system and reduce the probability that an eavesdropper can decode the transmitted information [13].

1.5.5 Advantages of PLS

Physical Layer Security offers several advantages, including enhanced communication security with relatively low computational complexity. In addition, it can be combined with conventional encryption methods to provide an additional layer of protection. PLS is therefore considered suitable for modern communication technologies such as FSO system, as well as emerging networks like 5G and 6G [13].

1.5.6 OWC Security Vulnerabilities

1.5.6.1 Risks in LoS and NLoS

In Optical Wireless Communication (OWC) systems, attackers generally need to be within the line-of-sight (LoS) to access the communication link because light propagates in a straight path, which reduces many external attacks. However, security threats still exist in both LoS and non-line-of-sight (NLoS) environments [9].

1.5.6.1.1 Line-of-Sight (LoS) Risks

OWC systems rely on a direct line-of-sight (LoS) between transmitter and receiver, which limits unauthorized access compared to traditional wireless systems. However, if an attacker is within the LoS range, they can intercept or manipulate optical signals and compromise user privacy across technologies such as VLC, LiFi, OCC, FSO, and LiDAR, which consist of a transmitter, optical channel, and receiver[9].

1.5.6.1 Non-Line-of-Sight (NLoS)

In NLoS environments, security risks in optical wireless communication can still occur despite the directional nature of light transmission. Smart lighting devices may leak information through variations in light intensity, reflections, scattered light, or unintended RF emissions. Additionally, malicious software in connected devices can create hidden channels for data extraction, making NLoS scenarios vulnerable to data interception if proper security measures are not implemented.

1.5.6.2 Attack Types in OWC

OWC security threats can be classified based on attack goals (such as jamming, eavesdropping, spoofing, and DDoS), communication channels (side-channel and covert-channel attacks), and targeted system components (transmitter, channel, or receiver).

1.5.6.2.1 Classification by Attack Goals

- **Jamming Attack**

A jamming attack occurs when an attacker intentionally interferes with the communication process to disrupt legitimate data transmission. In OWC systems, this is achieved by emitting high-intensity optical noise or continuous light signals that disturb the original transmitted signal. If the attacker knows the receiver's position, the interference can be directly targeted, making correct data detection difficult and causing communication instability or system failure.

- **Eavesdropping Attacks**

Eavesdropping attacks involve the passive interception of information transmitted through the optical channel without altering the signal. These attacks are more likely in unsecured or public OWC environments where multiple users share the same LoS space. Attackers can use optical sensors or cameras to capture light signals and extract sensitive information, potentially leading to privacy leakage.

- **Spoofing Attacks**

A spoofing attack occurs when an attacker impersonates a legitimate device by falsifying its identity. In OWC systems, weak protection of lighting transmitters can allow attackers to replace or tamper with LED sources, enabling them to transmit fake optical signals. As a result, the receiver may incorrectly trust a malicious source.

- **Other Attacks**

OWC systems may also face additional threats such as message manipulation, replay attacks, packet falsification, hijacking, and membership falsification. In message manipulation, transmitted data is altered to compromise integrity. Replay attacks involve retransmitting previously captured data to deceive the system. These vulnerabilities can significantly affect the reliability and security of optical communication systems [9].

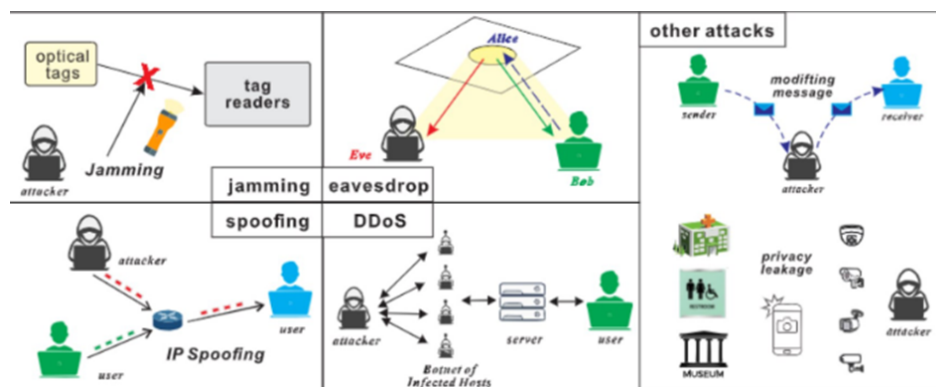


Figure 1.5: Illustration of jamming, eavesdropping, spoofing, DDoS, and other attacks

1.6 Chaos-Based Encryption in Optical Systems

Chaos- and hyperchaos-based encryption relies on complex nonlinear systems characterized by extreme sensitivity to initial conditions and unpredictable behavior, making the encryption keys highly secure and difficult to predict. When applied to Free-Space Optical (FSO) communication systems, which transmit data through the air or space using lasers, this encryption effectively protects signals from interception and enhances their resilience against atmospheric interference, thereby improving the security and reliability of data transmission.

1.6.1 Importance of Chaos/Hyperchaos in FSO

The importance of chaos and hyperchaos in Free Space Optical (FSO) communication lies in several key aspects. Enhanced channel security is achieved since using chaotic systems makes decryption by unauthorized entities extremely difficult. In addition, expanded key space is provided because hyperchaos offers a significantly larger key space than traditional chaos, thereby increasing resistance to attack. Furthermore, improved resistance to noise and interference is obtained, as chaotic encryption helps maintain data integrity even under adverse atmospheric conditions. Finally, increased resistance to cryptanalysis is ensured due to the irregular and unpredictable nature of chaotic signals, which complicates conventional analytical attacks.[15].

1.6.2 Application of Fso

Free-Space Optics (FSO) is used to provide optical links where fiber deployment is difficult or impractical. It is relatively cost-effective and offers a fast return on investment. Although current adoption remains moderate, the increasing demand for high-bandwidth and low-cost optical solutions suggests that FSO will expand more rapidly in the future compared to traditional fiber systems.

Objectives:

- **Network Extension:** FSO can extend existing metropolitan networks or interconnect new networks. These links are typically used in the network core rather than directly serving end users.
- **Enterprise Application:** FSO can interconnect local area networks (LANs), storage area networks (SANs), and campus networks.
- **Last-Mile Connectivity:** FSO can provide connectivity to end users using point-to-point, point-to-multipoint, ring, or mesh network topologies.

- **Fiber Backup:**FSO can serve as a redundant link, ensuring service continuity during fiber outages.
- **Access Links:**FSO can deliver high-speed access services, including gigabit Ethernet, for business applications.
- **DWDM Services:**Combining FSO with wavelength division multiplexing (WDM) enables operators to deploy partial optical networks without full fiber infrastructure.
- **Metro Network Extensions:** FSO can extend urban fiber networks and provide high-speed last-mile access to Internet service providers (ISPs) [3].

1.7 Conclusion

In conclusion, Free-Space Optical (FSO) communication represents a significant advancement in wireless communication technologies, effectively bridging the gap between the high speeds of fiber optics and the flexibility of wireless networking [1]. While the technology offers numerous including high data rates, large unlicensed bandwidth, and rapid deployment, its performance remains inherently dependent on atmospheric conditions and environmental factors that may degrad the optical beam [7]. As security threats continue to evolve, relying solely on the inherent directionality of optical beams is no longer sufficient to guarantee data confidentiality. Therefore, the integration of Physical Layer Security (PLS) techniques and chaos-based encryption methods has become essential to enhance the robustness and security of FSO systems [13]. A comprehensive understanding of FSO architecture ,atmospheric channel modeling, and advanced security mechanisms constitutes a fundamental fondation for the development of next-generation communication systems. These systems must be capable of overcoming both environmental challenges and emerging cyber-physical threats, ensuring reliable, high-performance, and secure data transmission.

Chapter 2

Memristor-Based 4D Hyperchaotic System&Image Encryption Scheme

2.1 Introduction

With the rapid advancement of digital communication technologies and the increasing exchange of multimedia data over networks, ensuring the security of such data has become a significant research challenge in recent years. Traditional encryption methods, while effective in certain applications, may exhibit limitations when applied to structured data such as digital images. This limitation has motivated the development of more robust and efficient encryption techniques. In this context, chaotic and hyperchaotic systems have emerged as promising tools in cryptography due to their unique dynamical properties, such as high sensitivity to initial conditions, pseudo-random behavior, and strong nonlinearity. These features make them particularly suitable for generating secure encryption keys that are difficult to predict or reproduce. This chapter aims to design and analyze a four-dimensional (4D) hyperchaotic system based on a memristor, which introduces additional nonlinearity and enhances the overall dynamical complexity of the system. A precise mathematical model is derived from the corresponding electronic circuit using Kirchhoff's laws, providing a deeper understanding of the system's behavior. Furthermore, this chapter explores the use of the generated chaotic sequences as encryption keys for digital images. The process involves several steps, including generation, normalization, quantization, and key stream construction. These keys are then employed in permutation and diffusion processes to effectively eliminate the statistical structure of the original image. In addition, an image encryption algorithm based on permutation and diffusion mechanisms is proposed[19]. Three different diffusion strategies are investigated to improve security performance while maintaining a balance between computational complexity and efficiency.. Finally, the effectiveness of the proposed system is evaluated using standard security metrics such

as entropy, NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity), and correlation analysis. These evaluations aim to assess the system's resistance against statistical and differential attacks and to demonstrate its suitability for secure digital image.

2.2 State of the Art of Chaos and Hyperchaotic Cryptography

In recent years, the security of digital image transmission has become a critical research topic, particularly with the rapid growth of multimedia communications and cloud-based data exchange. Chaos-based and hyperchaos-based encryption techniques have proven effective due to their strong nonlinear dynamics, high sensitivity to initial conditions, and pseudo-random behavior. In this context, Inam and al. [16] proposed a quantum color image encryption scheme based on a 4D hyperchaotic Lorenz system combined with a Quantum Fibonacci Transform, achieving $entropy \approx 7.999$, $NPCR = 99.64\%$, $UACI = 33.56\%$, very low correlation, and a large key space of approximately (10^{140}) thus providing strong resistance against statistical and brute-force attacks. Similarly, Kopp and Samuilik[17] introduced a 4D memristor-based hyperchaotic system characterized by multiple positive Lyapunov exponents and a Kaplan–Yorke dimension of 3.1, reflecting high dynamical complexity. When applied to image encryption, it achieved $entropy \approx 7.999$, $NPCR \approx 99\%$, and $UACI \approx 33\%$, and its practical feasibility was validated using Arduino hardware. Furthermore, Subathra and Thanikaiselvan[18] developed a hybrid approach combining a 5D hyperchaotic system with U-Net-based deep learning segmentation to generate dynamic keys for medical images. Their method achieved obtaining $entropy \approx 7.9971$, $NPCR = 99.61\%$, $UACI = 33.49\%$, a large key space of (2^{500}) , and successfully passed NIST randomness tests. In addition, Wang et al. [19] proposed a 4D hyperchaotic system incorporating Region of Interest (ROI) encryption, achieving similar metrics while enabling selective protection of sensitive image regions. . Moreover, Yang and al. [20] implemented a hyperchaotic memristor circuit with multiple positive Lyapunov exponents and a Kaplan–Yorke dimension between 4.0 and 4.9, validated via FPGA. Overall, these studies demonstrate that hyperchaotic systems are capable of achieving near-ideal encryption performance in terms of entropy, NPCR, and UACI metrics. Among these approaches, the system proposed by Kopp and Samuilik[17] has been selected for the present work due to its high dynamical complexity, multiple positive Lyapunov exponents, and elevated Kaplan–Yorke dimension, along with its experimentally validated implementation, making it well-suited for balancing robust security and practical applicability. Nevertheless, achieving an optimal trade-off between computational efficiency

and security remains a and significant challenge.

2.3 Fundamentals of Chaos and Hyperchaos

2.3.1 Chaotic systems

A nonlinear chaotic system is a deterministic dynamical system governed by nonlinear equations that exhibits complex and seemingly unpredictable behavior due to its extreme sensitivity to initial conditions and control parameters. Even very small changes in the initial state can lead to significantly different system trajectories over time, a property commonly referred to as the butterfly effect. These systems generate pseudo-random sequences characterized by ergodicity, randomness, and non-periodicity, which enhance their suitability for cryptographic applications, particularly in secure image encryption[21].

2.3.2 Hyperchaotic systems

The first four-dimensional hyperchaotic system was discovered by O.E. Rössler in 1976 and is characterized by at least two positive Lyapunov exponents, indicating that the system dynamics diverge exponentially in multiple directions of the phase space. In contrast, a classical chaotic system typically which has only one positive Lyapunov exponent and generally requires at least three dimensions to exhibit chaotic behavior. As a result, hyperchaotic systems possess higher dynamical complexity and exhibit greater unpredictability than conventional chaotic systems. In the field of secure communications, standard chaotic signals may sometimes be partially reconstructed or predicted due to their relatively limited dynamical structure. In contrast, hyperchaotic systems offer enhanced security performance owing to their increased randomness, higher dimensionality, and stronger sensitivity to initial conditions, making them more resistant to various cryptanalytic attacks.

2.3.3 Properties of Hyperchaotic systems

Hyperchaotic systems exhibit highly complex dynamics and intricate dynamical behavior. Although they are governed by deterministic nonlinear equations, they produce extremely unpredictable and irregular trajectories. These distinctive properties make them particularly suitable for applications in encryption and secure communications. The following are the key characteristics that define hyperchaotic systems:

2.3.3.1 sensitivity to initial conditions

Chaotic systems are characterized by an extreme sensitivity to initial conditions, a property widely known as the butterfly effect, first introduced by meteorologist Edward Lorenz. Even infinitesimally small differences in the initial state of a chaotic system can lead to significantly divergent trajectories over time. Consequently, despite the deterministic nature of these systems, it becomes practically impossible to predict their long-term behavior with high accuracy; only statistical or probabilistic predictions can provide meaningful insights. The study of such phenomena is conducted within the framework of dynamical systems, theory, where the state of the system is described by a set of time-dependent variables:

$$x(1), x(2), x(3).....x(n)$$

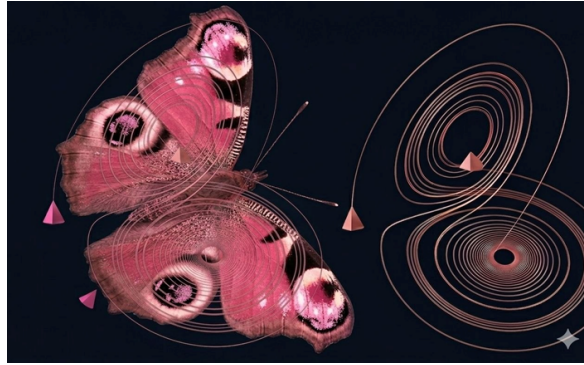


Figure 2.1: Illustration of the Butterfly effect

2.3.3.2 sensitivity to parameters

The behavior of a chaotic system is highly sensitive to variation in its control parameters; even even very small changes can lead to significantly different system trajectories even when starting from the same initial conditions. This property the crucial role of control parameters in determining the system's dynamics and stability, as slight modifications may cause the system to transition to entirely different dynamical regimes, such as periodic, quasi-periodic, or chaotic behavior[21].

2.3.3.3 Lyapunov exponents

Lyapunov exponents are used to quantify the sensitivity of a dynamical system to initial conditions by measuring the average exponential rate of divergence or convergence of nearby trajectories in phase space. A positive Lyapunov exponent indicates that small differences in initial conditions grow exponentially over time, which is a fundamental signature of chaotic behavior. In the case of a strange attractor, at least one Lyapunov exponent is positive, reflecting the system's intrinsic unpredictability,

whereas is in non-chaotic systems, all Lyapunov exponents are negative, indicating convergence toward stable states.. A positive Lyapunov exponent therefore implies that the distance between two initially close trajectories increases exponentially over time , which characteristic of chaotic dynamics. In a phase space of dimension P , there exist P Lyapunov exponents, each corresponding to the rate of divergence along a principal direction of the system.. These exponents are typically determined using the Jacobian matrix of the system function f evaluated at a given point, along with its eigenvalues. The Lyapunov exponent for a one-dimensional discrete system can be computed as follows :

$$\lambda = \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{i=1}^k \ln |f'(x_{i-1})| \quad (2.1)$$

The dynamical behavior of the system can be characterized according to the value of the Lyapunov exponent λ , leading to three possible cases:

- $\lambda < 0$: the distance between two nearby trajectories decreases over time, which indicating that the system converges toward a stable fixed point.
- $\lambda > 0$: the distance between nearby trajectories grows exponentially, revealing strong sensitivity to initial conditions and indicating chaotic behavior.
- $\lambda=0$: the distance between trajectories remains approximately constant, corresponding to periodic or quasi-periodic behavior[21].

2.3.3.4 Attractor

A dynamical attractor is a set or region in phase space toward which the trajectories of a system asymptotically evolve over time. The phase space represents all possible states of the system, and its dimension corresponds to the number of state variables required to describe the system. Depending on the system's behavior, motion in phase space can be regular, random, or chaotic. In the case of regular motion, trajectories form simple and predictable structures, such as fixed points or periodic cycles. In contrast, purely random motion leads to trajectories that fill the space without any identifiable structure.. In chaotic systems, trajectories may initially appear irregular and scattered, but over time, they tend to organize into a complex geometrical structure known as a strange attractor, which is a key signature of chaotic dynamics. These attractors are typically characterized by fractal geometry and sensitive dependence on initial conditions. The simplest type of attractor is a fixed point representing a stable steady state of the system, while more complex attractors include periodic orbits and quasi-periodic structures. In chaotic systems, trajectories converge toward strange attractors, highlighting both the underlying order and the inherent unpredictability of the system.[22]

2.3.4 Comparaison between chaotic and hyperchaotic systems.

Table 1 presents a comparative analysis of chaotic and hyperchaotic systems. Highlighting their fundamental differences in terms of dynamical properties., including the number of positive Lyapunov exponents, phase space dimension, sensitivity to initial conditions, complexity, typical applications, and trajectory patterns. The comparison includes key characteristics such as the number of positive Lyapunov exponents, phase space dimension, sensitivity to initial conditions, system complexity, typical applications, and trajectory patterns. This comparison facilitates a clearer understanding of how hyperchaotic systems extend the behavior of conventional chaotic systems, offering higher levels of unpredictability, complexity, and randomness, which makes them particularly suitable for applications requiring enhanced security, such as advanced image encryption and secure communications.

Table 2.1: Differences between chaos and hyperchaos [23, 24]

<i>Feature</i>	<i>Chaos</i>	<i>Hyperchaos</i>
<i>Lyapunov Exponents</i>	One positive exponent	Two or more positive exponents
<i>Minimum Phase Space Dimension</i>	3D for continuous systems	4D or higher for continuous systems
<i>Sensitivity to Initial Conditions</i>	Occurs mainly along one principal direction	Occurs simultaneously along multiple directions
<i>Trajectory Complexity</i>	Moderate complexity; confined to a chaotic attractor	Higher complexity; occupies a hyperchaotic attractor with richer structure
<i>Applications</i>	Chaotic encryption, secure communications	Hyperchaotic encryption, advanced secure communications
<i>Trajectory Pattern</i>	Irregular behavior with divergence in a dominant direction	Highly disordered behavior with divergence in multiple directions

2.4 Electronic Circuit Realization and Mathematical Model

2.4.1 Overview about circuit

Figure 2.2 The memristive hyperchaotic circuit is a four-dimensional (4D) nonlinear dynamical system that incorporates a flux-controlled memristor as its core nonlinear element. The circuit is structured into four functional blocks (A, B, C, and D): blocks

A–C are responsible for processing the first three state variables through linear feedback mechanisms, while block D integrates the memristor to generate the fourth state variable. This configuration enables the system to exhibit hidden attractors and hyperchaotic behavior characterized by multiple positive Lyapunov exponents, thereby significantly enhancing the complexity and unpredictability of the generated signals. Moreover, the circuit is described by a relatively simple mathematical model consisting of only seven terms, which makes it practically implementable using standard analog electronic components. These components include capacitors for integration, operational amplifiers for feedback and arithmetic operations, analog multipliers for nonlinear interactions, and resistors for parameter adjustment. Due to its rich and complex state-space dynamics, this circuit is particularly well-suited for applications in secure communications and digital image encryption, where high randomness and strong sensitivity to system parameters are essential.

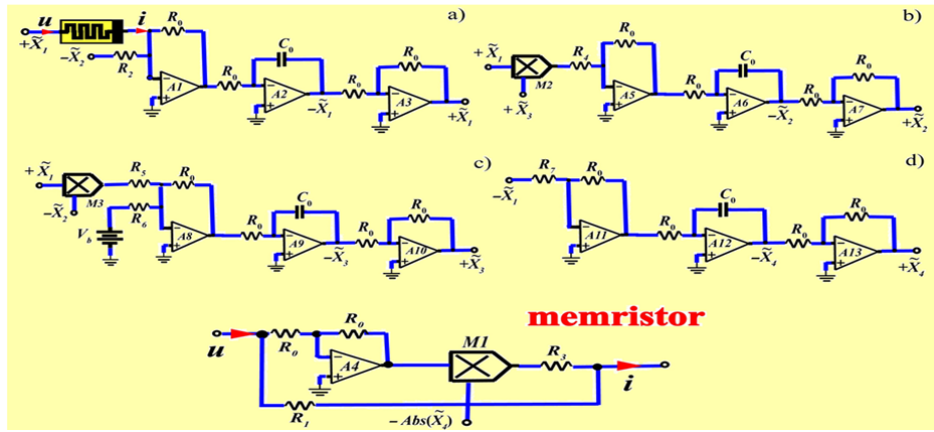


Figure 2.2: Illustrate the circuit modules implemented based on the system described by Equation (19): (a) $\tilde{X}_1$, (b) $\tilde{X}_2$, (c) $\tilde{X}_3$, (d) $\tilde{X}_4$ and the memristor circuit module [17]

- **Electronic components**

The circuit is composed of standard analog electronic components, including resistors (R) and capacitors (C), as well as diodes D1 and D2 (1N4001). It also utilizes analog multipliers (M1 to M3, AD633) and operational amplifiers (A1 to A16, TL084ACN), all powered by a dual supply voltage of ± 15 V [17].

2.4.2 Derivation of the Mathematical Model

The derivation is based on the assumption of ideal operational amplifiers (Op-Amps), where the input currents are negligible ($i_+ = i_- = 0$) and the input voltages are equal ($V_+ = V_-$). Since the non-inverting terminals are connected to ground, the inverting input nodes operate as virtual grounds.

- **Analysis of Block A of electronic circuit (Characterization of X_1)**

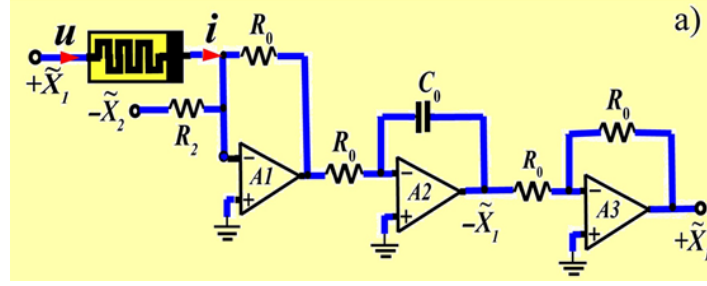


Figure 2.3: Bloc A of electronic circuit

Block A consists of three main components: an inverting summing amplifier (A1), an integrator (A2), and an inverter (A3). By applying Kirchhoff's Current Law (KCL) at the inverting input node of the first stage, we obtain:

$$i_+ + i_- = i_f \quad (2.2)$$

By expressing these currents in terms of the input voltage u , the state variable X_2 , and the resistors R_1 and R_2 , and by introducing the integrator scaling factor ($1/C_0 = 100k$), the following differential equation is obtained:

$$\frac{d\tilde{X}_1}{dt} = - \left(\frac{100k}{R_1} u - \frac{100k}{R_2} \tilde{X}_2 \right) \quad (2.3)$$

By substituting the memristor relation $u = X_1 + \frac{|X_4|}{10}$, the final expression of the differential equation for the first state variable becomes:

$$\frac{d\tilde{X}_1}{dt} = \frac{100k}{R_2} \tilde{X}_2 - \left(\frac{100k}{R_1} + \frac{100k}{R_s} |\tilde{X}_4| \right) X_1 \quad (2.4)$$

- **Analysis of Block B of electronic circuit (Characterization of X_2)**

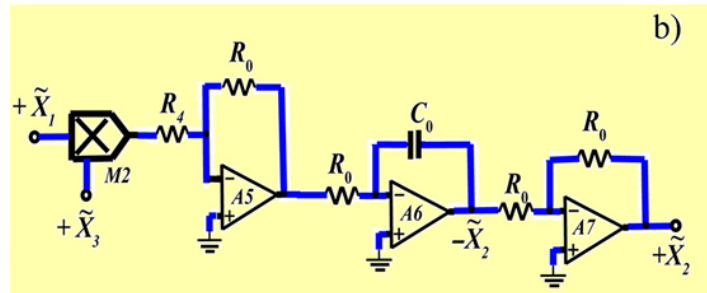


Figure 2.4: Bloc B of electronic circuit

Block B is designed to generate the second state variable X_2 . It utilizes an analog multiplier combined with an inverting integrator to introduce nonlinear coupling between the first and third state variables. By applying Kirchhoff's Current Law (KCL) at the

inverting input node of the integrator stage, we obtain:

$$i_{M2} + i_f = 0 \quad (2.5)$$

By expressing the current i_{M2} in terms of the multiplier output $V_{M2} = \frac{X_1 X_3}{10}$ and the resistor R_4 , and by substituting the integrator scaling factor ($1/C_0 = 100k$), we obtain:

$$\frac{d\tilde{X}_2}{dt} = -\frac{1}{R_4 C_0} \left(\frac{\tilde{X}_1 \tilde{X}_3}{10} \right) \quad (2.6)$$

Thus, the final differential equation governing the second state variable can be written as follows:

$$\frac{d\tilde{X}_1}{dt} = -\frac{100k}{10R_4} \tilde{X}_1 \tilde{X}_3 \quad (2.7)$$

- **Analysis of Block C of electronic circuit(Characterization of X_3)**

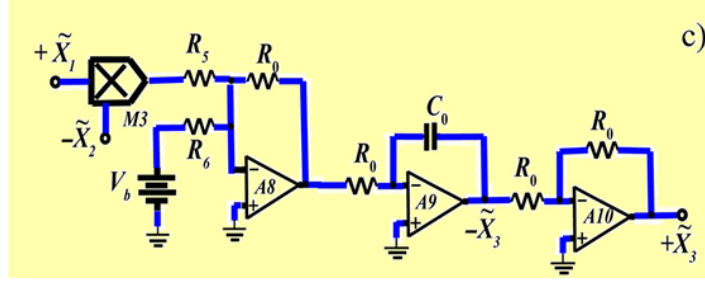


Figure 2.5: Bloc C of electronic circuit

Block C characterizes the third state variable X_3 . This block integrates a nonlinear product term with a constant DC bias voltage V_b , which serves as the system's bifurcation parameter. By applying Kirchhoff's Current Law (KCL) at the summing junction of the integrator:

$$i_{M3} + i_b + i_f = 0 \quad (2.8)$$

By expressing these currents in terms of the multiplier output $V_{M3} = \frac{X_1 X_2}{10}$, the bias voltage V_b , and the resistors R_5, R_6 , while incorporating the integrator scaling factor ($1/C_0 = 100k$), we obtain:

$$\frac{d\tilde{X}_3}{dt} = -\left(\frac{100k}{R_5} \frac{\tilde{X}_1 \tilde{X}_2}{10} + \frac{100k}{R_6} V_b \right) \quad (2.9)$$

Assuming a phase-correcting stage is utilized to align with the dynamic model, the final differential equation for the third state variable is:

$$\frac{d\tilde{X}_3}{dt} = \frac{100k}{10R_5} \tilde{X}_1 \tilde{X}_2 - \frac{100k}{R_6} V_b \quad (2.10)$$

- **Analysis of Block D of electronic circuit(Characterization of X_4)**

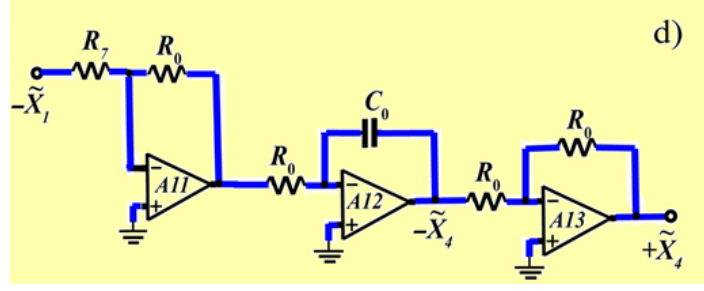


Figure 2.6: Bloc D of electronic circuit

Block D defines the fourth state variable X_4 , which physically represents the internal state (magnetic flux) of the memristor. This block provides the necessary dimensionality for hyperchaos. By applying Kirchhoff's Current Law (KCL) at the inverting input of the integrator:

$$i_{x1} + i_f = 0 \quad (2.11)$$

By expressing these currents in terms of the state variable X_1 and the resistor R_7 , and substituting the scaling factor ($1/C_0 = 100k$), we obtain the following relationship:

$$\frac{d\tilde{X}_4}{dt} = -\frac{1}{R_7 R_0} \tilde{X}_1 \quad (2.12)$$

The final differential equation for the fourth state variable is:

$$\frac{d\tilde{X}_4}{dt} = \frac{100k}{R_7} \tilde{X}_1 \quad (2.13)$$

• Final System of Equations

The chaotic system implemented by the analog circuit can therefore be expressed in the form of a set of coupled nonlinear differential equations, given as follows:

$$\frac{d\tilde{X}_1}{dt} = \frac{100k}{R_2} \tilde{X}_2 - \left(\frac{100k}{R_1} + \frac{100k}{10R_s} |\tilde{X}_4| \right) \tilde{X}_1 \quad (2.14)$$

$$\frac{d\tilde{X}_2}{dt} = -\frac{100k}{10R_4} \tilde{X}_1 \tilde{X}_3 \quad (2.15)$$

$$\frac{d\tilde{X}_3}{dt} = \frac{100k}{10R_5} \tilde{X}_1 \tilde{X}_2 - \frac{100k}{R_6} V_b \quad (2.16)$$

$$\frac{d\tilde{X}_4}{dt} = \frac{100}{R_7} \tilde{X}_1 \quad (2.17)$$

2.4.3 Dynamical Analysis

The proposed memristive system can be described by the following set of coupled nonlinear differential equations, which define its dynamical behavior in a four-dimensional

phase space:

$$\frac{d\tilde{X}_1}{dt} = K_2\tilde{X}_2 - (K_1 + K_3|\tilde{X}_4|)\tilde{X}_1 \quad (2.18)$$

$$\frac{d\tilde{X}_2}{dt} = -K_4\tilde{X}_1\tilde{X}_3 \quad (2.19)$$

$$\frac{d\tilde{X}_3}{dt} = K_5\tilde{X}_1\tilde{X}_2 - K_6V_b \quad (2.20)$$

$$\frac{d\tilde{X}_4}{dt} = K_7\tilde{X}_1 \quad (2.21)$$

These equations represent a four-dimensional nonlinear dynamical system, where the constants $K_1, K_2, \dots, K_7$ are system parameters determined by the circuit components (resistances, capacitances, and scaling factors). The system exhibits strong nonlinear coupling between state variables, particularly through the multiplicative terms $\tilde{X}_1 \tilde{X}_2$ and $\tilde{X}_3 \tilde{X}_4$, as well as the non-smooth term $\tilde{X}_4$, which contributes to the enhanced complexity of the dynamics.

2.5 Hyperchaotic Key Generation Mechanism

The security of the proposed image encryption scheme heavily relies on the generation of high-quality pseudo-random sequences. In this work, a hyperchaotic system is utilized as a key generator due to its extreme sensitivity to initial conditions and highly complex nonlinear dynamics. These properties enable the system to produce unpredictable and statistically robust sequences, which are well-suited for cryptographic applications, particularly in secure image encryption [17].

2.5.1 Initialization of the Hyperchaotic System

The hyperchaotic system is initialized with the following initial conditions, derived from the dynamical system equations:

$$X_1(0) = 0.1, X_2(0) = 0.2, X_3(0) = 0.1, X_4(0) = 0.1$$

The system parameters are defined as follows:

$$\left(\begin{array}{l} K_1 = -\frac{100k}{R_1}, K_2 = \frac{100k}{R_2}, K_3 = -\frac{100k}{10R_3}, K_4 = -\frac{100k}{10R_4}, \\ K_5 = \frac{100k}{10R_5}, K_6 = -\frac{100k}{R_6}, K_7 = \frac{100}{R_7} \end{array} \right)$$

2.5.2 Chaotic Sequence Generation

In this work, chaotic sequences are generated from a four-dimensional (4D) hyperchaotic system derived from an electronic circuit implementation, as illustrated in Figure 2.2. The circuit is composed of operational amplifiers, resistors, capacitors, analog multipliers, and a memristor, which introduces strong nonlinear behavior into the system. Each subcircuit corresponds to a state variable, where integrator blocks implement the differential equations, while multipliers and the memristor ensure nonlinear coupling between variables. Based on Kirchhoff's laws, the circuit is modeled by a system of nonlinear differential equations, which is numerically solved using the MATLAB ode45 solver. This process generates four continuous chaotic signals exhibiting hyperchaotic dynamics. To eliminate the transient behavior, the first N_0 samples are discarded, ensuring that only the steady-state regime is considered.

2.6 Proposed Image Encryption Algorithm

The effectiveness of any digital image cryptosystem depends on its ability to achieve a high degree of confusion and diffusion, ensuring that the original information is securely protected against statistical and differential attacks. In this work, we propose a hybrid image encryption framework based on the complex dynamical properties of a four-dimensional (4D) hyperchaotic system. This system is selected due to its strong nonlinearity, complex trajectories, and extreme sensitivity to initial conditions, which together provide a large key space, making the scheme robust against brute-force attacks. The main contribution of this study lies in the design and evaluation of a "Smart Diffusion" stage. Instead of relying on a single diffusion mechanism, three distinct algorithmic strategies are developed and integrated within the proposed framework. This comparative approach aims to determine the optimal trade-off between security performance and computational efficiency. The proposed encryption methodology is structured into three main phases:

- **Generation Phase:** The 4D hyperchaotic system is used to generate high-quality pseudo-random sequences by solving the associated nonlinear differential equations, ensuring strong unpredictability and sensitivity.
- **Permutation Phase (Confusion):** The pixel positions are rearranged (scrambled) based on the chaotic sequences, effectively breaking the spatial correlation between adjacent pixels and concealing the structural information of the image.
- **Comparative Diffusion Phase:** This phase represents the core of the proposed encryption scheme, where three independent diffusion algorithms are im-

plemented and analyzed. Each approach aims to modify pixel intensity values in a way that maximizes security while maintaining computational efficiency.

2.6.1 Method 1 : XOR-Based Diffusion Scheme

The XOR method is a lightweight cryptographic technique based on the Exclusive-OR logical operation. It is widely used in encryption systems due to its simplicity, efficiency, and ability to provide data confidentiality when combined with secret keys. Secure image transmission is performed using an XOR-based diffusion scheme, where the plaintext image is encrypted into a cipher image using a chaotic-system-generated secret key (Algorithm 1).

Algorithm 1: Proposed Encryption Process

Input: Plain image I of size $M \times N$, initial conditions x_0

Output: Encrypted image C

Step 1: Solve the 4D hyperchaotic system using `ode45`

Step 2: Generate chaotic sequences x_1, x_2, x_3, x_4

Step 3: Interpolate sequences to match image size

Step 4: Normalize sequences to $[0, 1]$

Step 5:

$$K_i = \text{mod}(\lfloor |X_i \times 10^{14}| \rfloor, 256) \quad (2.22)$$

Step 6:

$$S = K_1 \oplus K_2 \oplus K_3 \oplus K_4 \quad (2.23)$$

Step 7: Convert image into vector P

Step 8: Generate permutation index π

Step 9:

$$P_{\text{perm}} = P(\pi) \quad (2.24)$$

Step 10:

$$C(1) = P_{\text{perm}}(1) \oplus S(1) \quad (2.25)$$

For $i = 2$ to L :

$$C(i) = P_{\text{perm}}(i) \oplus S(i) \oplus C(i - 1) \quad (2.26)$$

Step 11: Reshape C into image form

At the receiver side, the inverse XOR operation is applied in order to reconstruct the original image from the received cipher image. The following Algorithm 2 details the decryption process, which relies on the same secret key to ensure correct recovery of the transmitted data.

Algorithm 1 Proposed Decryption Process**Input:** Encrypted image C , initial conditions x_0 **Output:** Decrypted image I **Step 1:** Regenerate chaotic sequences using same x_0 **Step 2:** Recompute key sequences K_1, K_2, K_3, K_4 **Step 3:** Generate Super Key S **Step 4:** Convert encrypted image into vector**Step 5:**

$$P_{\text{perm}}(1) = C(1) \oplus S(1) \quad (2.27)$$

For $i = 2$ to L :

$$P_{\text{perm}}(i) = C(i) \oplus C(i-1) \oplus S(i) \quad (2.28)$$

Step 6:

$$P = P_{\text{perm}}(\pi^{-1}) \quad (2.29)$$

Step 7: Reshape to original image

2.6.2 Method 2: Cumulative Modular Addition-Based Diffusion Scheme

The Addition method is a diffusion-based encryption technique that modifies data values through modular arithmetic operations. It is commonly employed to increase randomness and enhance the security of encrypted information.

The encryption process based on the Addition diffusion scheme is described in Algorithm 1.

Algorithm 2 Proposed Encryption Process**Input:** Plain image I of size $M \times N$, initial conditions x_0 **Output:** Encrypted image C **Step 1:** Solve the 4D hyperchaotic system using `ode45` with initial conditions x_0 **Step 2:** Convert image to grayscale if needed**Step 3:** Reshape image into vector:

$$P = \text{reshape}(I, L) \quad \text{where } L = M \times N \quad (2.30)$$

Step 4: Compute modulation factor:

$$\text{mod_factor} = \text{mod} \left(\frac{\sum P}{255 \times L}, 1 \right) \quad (2.31)$$

Step 5: Generate key streams:

$$S_{\text{perm}} = \text{mod} \left(\lfloor (x_{\text{seq}} + \text{mod_factor}) \times 10^{14} \rfloor, L \right) + 1 \quad (2.32)$$

$$S_{\text{diff1}} = \text{mod} \left(\lfloor (y_{\text{seq}} + \text{mod_factor}) \times 10^{14} \rfloor, 256 \right) \quad (2.33)$$

$$S_{\text{diff2}} = \text{mod} \left(\lfloor (z_{\text{seq}} + \text{mod_factor}) \times 10^{14} \rfloor, 256 \right) \quad (2.34)$$

$$S_{\text{diff3}} = \text{mod} \left(\lfloor (w_{\text{seq}} + \text{mod_factor}) \times 10^{14} \rfloor, 256 \right) \quad (2.35)$$

Step 6: Permutation stage:

$$\pi = \text{argsort}(S_{\text{perm}}) \quad (2.36)$$

$$P'(i) = P(\pi(i)), \quad \text{for } i = 1, 2, \dots, L \quad (2.37)$$

Step 7: Diffusion stage:

$$C(1) = \text{mod} (P(1) + S_{\text{diff1}}(1) + S_{\text{diff2}}(1) + S_{\text{diff3}}(1), 256) \quad (2.38)$$

For $i = 2$ to L :

$$C(i) = \text{mod} (P(i) + S_{\text{diff1}}(i) + S_{\text{diff2}}(i) + S_{\text{diff3}}(i) + C(i-1), 256) \quad (2.39)$$

Step 8: Reshape encrypted vector

$$C_{\text{img}} = \text{reshape}(C, M, N) \quad (2.40)$$

Return C_{img}

The corresponding decryption process, which reconstructs the original data using the inverse Addition operation, is presented in Algorithm 2.

Algorithm 3 Proposed Decryption Process

Input: Encrypted image C_{img} , initial conditions x_0 **Output:** Decrypted image I **Step 1: Reshape encrypted image**

$$C = \text{reshape}(C_{img}, L) \quad (2.41)$$

Step 2: Regenerate chaotic sequences using the same initial conditions and system parametersGenerate chaotic sequences x_{seq} , y_{seq} , z_{seq} , and w_{seq} .

Regenerate the modulation factor using the same initial condition.

Step 3: Reconstruct key streamsReconstruct the same key streams: S_{perm} , S_{diff1} , S_{diff2} , and S_{diff3} .**Step 4: Perform inverse diffusion**

$$P'(1) = \text{mod}(C(1) - S_{diff1}(1) - S_{diff2}(1) - S_{diff3}(1), 256) \quad (2.42)$$

For $i = 2$ to L :

$$P'(i) = \text{mod}(C(i) - S_{diff1}(i) - S_{diff2}(i) - S_{diff3}(i) - C(i-1), 256) \quad (2.43)$$

Step 5: Apply inverse permutation

$$P(\pi(i)) = P'(i) \quad (2.44)$$

Step 6: Reshape the decrypted vector into image form

$$I = \text{reshape}(P, M, N) \quad (2.45)$$

Return I

2.6.3 Method 3: QR Decomposition Scheme

The QR method is an encryption approach that utilizes QR matrix decomposition, a mathematical technique from linear algebra. It is used to introduce additional complexity and improve the scrambling capability of cryptographic systems. The encryption process based on the QR decomposition-based scheme is described in Algorithm 1. The method exploits matrix factorization to introduce strong permutation and diffusion effects, enhancing the scrambling capability of the encryption system.

Algorithm 4 Proposed Encryption Process

Input: Original image I of size $M \times N$ **Output:** Encrypted image C_{img} **Step 1:** Generate a chaotic signal using a nonlinear dynamic system.**Step 2:** Normalize the chaotic signal to the range $[0, 255]$ to obtain the key stream (key_stream).**Step 3:** Convert the image into a vector:

$$I_{\text{vec}} = \text{vectorize}(I) \quad (2.46)$$

Step 4: Perform pixel permutation:

- Generate permutation indices from key_stream

$$\text{mixed_vec} = I_{\text{vec}}(\text{perm_index}) \quad (2.47)$$

Step 5: Reshape the permuted vector into an image:

$$I_{\text{mixed}} = \text{reshape}(\text{mixed_vec}) \quad (2.48)$$

Step 6: Divide the image into four blocks:

$$B_1, B_2, B_3, B_4$$

Step 7: For each block:

- Generate a chaotic key.
- Apply QR decomposition to obtain matrix Q .
- Encrypt the block:

$$B_{\text{enc}} = B \times Q \quad (2.49)$$

Step 8: Concatenate the encrypted blocks:

$$I_{\text{conc}} = \text{combine}(B1_{\text{enc}}, B2_{\text{enc}}, B3_{\text{enc}}, B4_{\text{enc}}) \quad (2.50)$$

Step 9: Apply a second permutation using another chaotic key.**Step 10:** Apply diffusion process:

- Perform XOR with an additional key.
- Apply chaining between pixels.

Step 11: Output the encrypted image:Return C_{img}

At the receiver side, the decryption process reconstructs the original image by reversing the QR-based transformation. The following Algorithm 2 details the inverse procedure, which relies on the same decomposition structure to ensure accurate recovery of the transmitted data.

Algorithm 5 Proposed Decryption Process

Output: Decrypted image I **Step 1:** Regenerate the same chaotic keys using identical initial conditions.**Step 2:** Reverse the diffusion process:

- Undo XOR operations
- Reverse pixel chaining

Step 3: Apply inverse permutation:

- Restore original pixel order

Step 4: Divide the image into four blocks:

$$B_1, B_2, B_3, B_4$$

Step 5: For each block:

- Recompute matrix Q using the same chaotic key.
- Decrypt the block:

$$B = B_{\text{enc}} \times Q^T \quad (2.51)$$

Step 6: Concatenate the decrypted blocks:

$$I_{\text{block}}$$

Step 7: Apply inverse of the first permutation:

- Restore the original image structure

Step 8: Output the recovered image: Return I

2.7 Cryptographic Performance Evaluation

The security performance of the proposed image encryption scheme is evaluated using a set of widely accepted cryptographic metrics, including NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity), information entropy, and correlation analysis. These metrics provide a comprehensive assessment of the encryption strength, allowing the evaluation of the system's resistance against statistical and differential attacks, as well as its ability to produce highly random and decorrelated encrypted images.

2.7.1 Key Space Analysis

The key space of a cryptographic system represents the total number of possible key combinations that can be generated from its parameters, taking into account both

their value ranges and numerical precision. A sufficiently large key space is essential to ensure strong resistance against brute-force attacks, in which an adversary attempts to exhaustively test all possible keys [29]. The detailed calculation and quantitative evaluation of the key space will be presented in Chapter 3.

2.7.2 Key Sensitivity Analysis

Key sensitivity refers to the ability of an encryption algorithm to produce significantly different ciphertexts in response to minimal changes in the secret key. This property is fundamental to ensuring strong cryptographic security, as it guarantees that even infinitesimal variations in the key lead to drastically different encrypted outputs, thereby making brute-force and key-guessing attacks highly ineffective. Mathematically, key sensitivity can be quantified using specific evaluation metrics and expressed through the following formulations [28]:

$$\text{If } K \rightarrow K' \text{ with } |K - K'| \approx \varepsilon \quad (2.52)$$

$$\text{Then } I_{enc} = E_K(I) \text{ and } I_{enc'} = E_{K'}(I) \quad (2.53)$$

where $E_K(.)$ denotes the encryption function using key K , and I is the original image. The resulting encrypted images I_{enc} and $I_{enc'}$ should exhibit negligible correlation, indicating complete statistical decorrelation resulting from small perturbations in the key. The detailed calculation and quantitative evaluation of key sensitivity will be presented in Chapter 3.

2.7.3 Histogram Analysis

Histogram analysis is a widely used technique in digital image processing to evaluate the distribution of pixel intensity values. It represents the frequency of occurrence of each intensity level in the form of a histogram, allowing for the assessment of important image characteristics such as contrast, uniformity, and randomness [30].

2.7.4 Correlation of Adjacent Pixels (Horizontal, Vertical, Diagonal)

To evaluate the statistical security of the proposed encryption algorithm, the correlation between adjacent pixels is analyzed in the horizontal, vertical, and diagonal directions. In natural images, adjacent pixels are typically highly correlated, which makes them vulnerable to statistical attacks and information leakage. An effective encryption scheme should significantly reduce this correlation, ideally producing correlation coefficients close to zero, thereby ensuring high randomness and strong resistance

to statistical analysis. The correlation coefficient r_{ab} between two adjacent pixels a and b is defined as follows [25]:

$$r_{ab} = \frac{cov(a, b)}{\sqrt{D(a) \cdot D(b)}} \quad (2.54)$$

where the covariance and variance are computed as

$$cov(a, b) = \frac{1}{T} \sum_{j=1}^T (x_j - E(a)) (b_j - E(b)) \quad (2.55)$$

$$E(a) = \frac{1}{T} \sum_{j=1}^T x_j \quad (2.56)$$

$$D(a) = \frac{1}{T} \sum_{j=1}^T (a_j - E(a))^2 \quad (2.57)$$

Where:

- $cov(a, b)$ is the covariance between two adjacent pixels a and b
- $D(a)$ and $D(b)$ are the variances of a and b , respectively
- $E(a)$ and $E(b)$ denote the mean values
- a_i and b_j represent the intensity values of neighboring pixels
- T is the total number of sampled pixel pairs

2.7.5 Information Entropy Analysis

Information entropy, commonly referred to as Shannon entropy, is a fundamental statistical measure used to quantify the degree of randomness or unpredictability in an information source. In the context of image encryption, a high entropy value indicates that the encrypted image exhibits a nearly uniform distribution of pixel intensities, making it extremely difficult for an attacker to extract meaningful statistical information or identify underlying patterns. In this study, the encrypted image is modeled as a discrete memoryless information source, denoted by mmm , and the entropy $E(p)$ is computed as follows [26]:

$$E(p) = \sum_{i=0}^{T-1} p(p_i) \log \frac{1}{p(p_i)} \quad (2.58)$$

Where:

- T denotes the total number of possible symbols (i.e., grayscale levels, typically 256)
- $p(p_i)$ represents the probability of occurrence of the symbol p_i

- p_i corresponds to the pixel intensity value
- The logarithm is typically taken in base 2, and the entropy is expressed in bits

2.7.6 Differential Attack Analysis (Primary Criteria: NPCR, UACI)

The primary security criteria for evaluating image encryption schemes are based on their resistance to differential attacks, which is commonly assessed using NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity). These metrics measure the sensitivity of the encryption algorithm to small changes in the input image, ensuring that a slight modification (such as a single pixel change) results in a significant and widespread alteration in the encrypted image

2.7.6.1 NPCR (Number of Pixel Change Rate)

NPCR quantifies the percentage of differing pixels between the original image I_{orig} and its corresponding encrypted image I_{enc} . A high NPCR value (close to 100%) indicates strong sensitivity to small changes in the input image, ensuring that minor variations in the plaintext lead to significantly different ciphertexts.

The NPCR is computed as follows [27]:

$$NPCR = \sum_{i,j} \frac{M(r,c)}{N} \times 100 \quad (2.59)$$

where:

$$M(r,c) = \begin{cases} 0 & \text{if } I_{orig}(r,c) = I_{enc}(r,c) \\ 1 & \text{if } I_{orig}(r,c) \neq I_{enc}(r,c), \end{cases}$$

Where:

- $I_{orig}(r,c)$ and $I_{enc}(r,c)$ denote the pixel values at position (r,c) in the original and encrypted images, respectively
- $M(r,c)$ is a binary indicator function that identifies whether the pixels differ
- N represents the total number of pixels in the image

2.7.6.2 UACI (Unified Average Changing Intensity)

UACI measures the average intensity difference between two encrypted images corresponding to slightly different plaintexts. It evaluates the strength of the diffusion pro-

cess, indicating how significantly pixel values are altered during encryption. A higher UACI value reflects stronger diffusion and better resistance to differential attacks.

The UACI is computed as follows [27]:

$$UACI = \frac{1}{M \times N} \sum \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\% \quad (2.60)$$

where:

- $C_1(i, j)$ and $C_2(i, j)$ are the pixel values at position (i, j) in two encrypted images obtained from slightly different input images
- $M \times N$ represents the image dimensions
- 255 is the maximum pixel intensity value for 8-bit images

Ideal Values:

- $NPCR \approx 99.6\%$
- $UACI \approx 33\%$

These values indicate a strong avalanche effect and effective diffusion, confirming that the encryption algorithm is highly sensitive to small changes in the input image and robust against differential attacks.

2.7.7 Robustness Against Noise and Data Loss

To evaluate the robustness of the proposed encryption scheme, different types of noise, such as salt-and-pepper noise (e.g., 1%), are intentionally introduced into the encrypted image. The corresponding decryption results demonstrate that the original image can still be partially recovered with acceptable visual quality, indicating that the proposed method exhibits strong robustness against noise interference and transmission errors.

2.7.8 Resistance to Statistical Attacks

The combination of a uniform histogram distribution, low correlation coefficients, and high entropy values ensures that the encrypted image does not reveal any exploitable statistical information. This significantly enhances the system's resistance to statistical attacks.

2.7.9 Randomness

The chaotic sequences used for key generation exhibit pseudo-random behavior, ensuring that the generated key values are highly unpredictable and do not follow any discernible patterns. This property is crucial for preventing attackers from exploiting statistical regularities in order to compromise the encryption scheme.

2.7.10 Overall Security Evaluation

The proposed encryption scheme combines hyperchaotic key generation with multiple diffusion mechanisms, including XOR-based diffusion and cumulative modular addition. This hybrid architecture enhances the overall security of the system by ensuring:

- High sensitivity to initial conditions
- Strong nonlinear dynamics
- Effective confusion and diffusion properties
- Robust resistance to differential and statistical attacks

Furthermore, the QR decomposition-based approach is theoretically expected to provide stronger diffusion capability compared to both the XOR-based method and the cumulative modular addition method, due to its higher mathematical complexity and multidimensional transformation properties[31].

2.8 Conclusion

In this chapter, a comprehensive analysis of a four-dimensional (4D) memristor-based hyperchaotic system has been presented, along with an in-depth study of its dynamical properties and its application to digital image encryption. The advantages of hyperchaotic systems over conventional chaotic systems have been clearly demonstrated, particularly in terms of their higher dynamical complexity and stronger sensitivity to initial conditions, which significantly enhance the security level of cryptographic schemes. A mathematical model of the proposed system has been derived from its electronic circuit implementation, establishing a strong connection between theoretical modeling and practical realization[2]. Furthermore, the process of chaotic sequence generation and their transformation into discrete cryptographic keys has been thoroughly described, ensuring high randomness, uniform distribution, and suitability for encryption purposes. The proposed encryption framework is based on two fundamental stages: permutation (confusion) and diffusion. In particular, three distinct diffusion strategies have been designed and analyzed to improve the overall security performance

and efficiency of the system. The obtained results demonstrate that these approaches provide a high degree of confusion and diffusion, as well as strong sensitivity to slight variations in both the secret key and input image. Moreover, the evaluation of security metrics—including information entropy, correlation coefficients, NPCR, and UACI—confirms that the proposed scheme achieves near-ideal performance, indicating strong resistance against statistical and differential attacks. Additionally, the large key space ensures a high level of protection against brute-force attacks. Based on these findings, it can be concluded that the proposed system constitutes an effective, robust, and secure solution for digital image encryption. It also offers significant potential for further optimization and adaptation, making it suitable for modern secure communication systems and advanced information security applications[27, 30].

Chapter 3

Design and Simulation of secure FSO system

Hanane.djellab@univ-tebessa.dz

General conclusion

This work focused on the development and evaluation of a secure Free-Space Optical (FSO) communication system integrating a four-dimensional memristor-based hyperchaotic image encryption scheme. The main objective was to ensure both reliable optical transmission and high-level multimedia data security under different atmospheric conditions. First, the dynamic analysis of the proposed memristor-based hyperchaotic system confirmed the existence of complex nonlinear behavior characterized by high randomness, strong sensitivity to initial conditions, and multiple positive Lyapunov exponents. These properties make the proposed system highly suitable for secure cryptographic applications and robust key generation. Three image encryption techniques based on XOR diffusion, arithmetic addition, and QR matrix decomposition were then developed and evaluated. The obtained results demonstrated excellent cryptographic performance for all proposed methods. The entropy values reached 7.9987, 7.9983, and 7.9893 for the XOR, arithmetic addition, and QR methods, respectively, which are very close to the theoretical ideal value of 8. In addition, the NPCR values exceeded 99%, while the UACI values were close to 33%, confirming strong diffusion capability and high resistance against differential attacks. Furthermore, the proposed hyperchaotic system provided a large key space estimated at approximately (10^{112}), ensuring strong resistance against brute-force attacks. The proposed encryption framework was successfully integrated into an FSO communication system using MATLAB and OptiSystem environments. The transmission performance was evaluated under clear weather, moderate rain, and snow conditions using BER, Q-factor, and eye diagram analysis. Under clear weather conditions, the system achieved excellent performance with a BER of $8.68 \times (10^{-22})$. and a Q-factor of 9.51 at a transmission distance of 1 km. In contrast, atmospheric attenuation caused by rain and snow degraded the transmission quality, resulting in BER values of $4.27 \times (10^{-9})$. and $1.89 \times (10^{-4})$., respectively. The obtained results also demonstrated that the proposed system maintained acceptable communication performance up to approximately 1.6 km under clear weather conditions, 1.1 km under moderate rain, and 0.4 km under snow conditions. Moreover, the visual analysis confirmed that the encrypted images remained completely noise-like during transmission, while the decrypted images were successfully reconstructed even under degraded atmospheric conditions. Among the in-

investigated encryption methods, the QR matrix decomposition approach provided the best compromise between cryptographic security, diffusion capability, and transmission robustness. Its higher mathematical complexity and stronger pixel decorrelation significantly improved the resilience of secure image transmission over atmospheric FSO channels. Overall, the obtained results confirm that the integration of memristor-based hyperchaotic encryption with FSO communication technology provides an efficient and reliable solution for secure multimedia transmission in optical wireless networks. The proposed system ensures two complementary levels of protection: cryptographic security through hyperchaotic encryption and physical-layer robustness through FSO transmission optimization. Therefore, the developed framework represents a promising solution for next-generation secure optical wireless communication systems. As future work, real-time hardware implementation using FPGA or DSP platforms, intelligent atmospheric compensation techniques based on artificial intelligence, and the extension of the proposed framework to video encryption and hybrid optical wireless communication systems may be investigated.

Bibliography

- [1] M. M. Roshdy, A. H. Elghandour, and K. M. Hassan, “Free Space Optical Communications: Challenges, Mitigation Techniques, Classification Framework, and Standardization,” *Future Engineering Journal*, vol. 5, no. 1, Jan. 2025.
- [2] A. G. Alkholidi and K. S. Altowij, “Free Space Optical Communications – Theory and Practices,” in *Contemporary Issues in Wireless Communications*. InTech, 2014, pp. 159–192. doi: 10.5772/58884.
- [3] “White Paper on Free Space Optics (FSO): A Communication Technology,” *FreeSpaceOptics.com*, 2014. [Online]. Available: www.freespaceoptics.com
- [4] A. Essar, “Performance Analysis of Free Space Optical Communication System,” in *2018 International Conference on Optical Wireless Technologies (OWT)*, 2018.
- [5] A. Malik and P. Singh, “Free Space Optics: Current Applications and Future Challenges,” *International Journal of Optics*, vol. 2015, Art. ID 945483, 2015. doi: 10.1155/2015/945483.
- [6] I. A. Alimi and P. P. Monteiro, “Revolutionizing Free-Space Optics: A Survey of Enabling Technologies, Challenges, Trends, and Prospects of Beyond 5G Free-Space Optical (FSO) Communication Systems,” *Sensors*, vol. 24, no. 24, p. 8036, 2024. doi: 10.3390/s24248036.
- [7] A. Alkholidi and K. Altowij, “Effect of Clear Atmospheric Turbulence on Quality of Free Space Optical Communications in Western Asia,” in *Optical Communications Systems*, M. S. Ismail, Ed. Rijeka, Croatia: IntechOpen, 2012, pp. 41–76. doi: 10.5772/30925.
- [8] S. Burdah, O. N. Samijayani, A. Syahriar, R. Ramdhani, and R. Alamtaha, “Performance Analysis of Q Factor Optical Communication in Free Space Optics and Single Mode Fiber,” *Universal Journal of Electrical and Electronic Engineering*, vol. 6, no. 3, pp. 167–175, 2019. doi: 10.13189/ujee.

- [9] X. Zhang, G. Klevering, X. Lei, Y. Hu, L. Xiao, and G.-H. Tu, “The Security in Optical Wireless Communication: A Survey,” *ACM Computing Surveys*, vol. 55, no. 14s, Art. 329, Jul. 2023. doi: 10.1145/3594718.
- [10] K. Kaur, R. Miglani, and J. S. Malhotra, “The Gamma-Gamma Channel Model – A Survey,” *Indian Journal of Science and Technology*, vol. 9, no. 47, Dec. 2016. doi: 10.17485/ijst/2016/v9i47/106796.
- [11] S. Thakur and R. Thakur, “Free Space Optical Communication: Review Paper,” *International Journal of Engineering and Science Invention (IJESI)*, vol. 7, no. 10, pp. 58–67, 2018.
- [12] A. A. Ibrahim, S. Özgür Ata, E. Erdoğan, and L. Durak-Ata, “Performance Analysis of Free Space Optical Communication Systems over Imprecise Málaga Fading Channels,” *Optics Communications*, vol. 457, p. 124694, Feb. 2020. doi: 10.1016/j.optcom.2019.124694.
- [13] S. S. Patil, C. Joseph, D. T. Varpe, and A. A. Bazil Raj, “A Comprehensive Review on Security in Free-Space Optical Communication,” *International Journal of Engineering Research and Reviews*, vol. 12, no. 3, pp. 150–180, Jul.–Sep. 2024. doi: 10.5281/zenodo.13851700.
- [14] P. Zhang, J. Jie, Z. Liu, and K. Dong, “Chaotic Image Encryption System as a Proactive Scheme for Image Transmission in FSO High-Altitude Platform,” *Photonics*, vol. 12, no. 7, p. 635, 2025.
- [15] Y. Liu, Z. Jiang, X. Xu, F. Zhang, and J. Xu, “Optical Image Encryption Algorithm Based on Hyper-Chaos and Public-Key Cryptography,” *Optics & Laser Technology*, vol. 127, p. 106171, Jul. 2020. doi: 10.1016/j.optlastec.2020.106171.
- [16] S. Inam, S. Kanwal, R. Amir, A. Ksibi, and I. Matloob, “Quantum color image encryption using a novel 4D hyperchaotic Lorenz system and Fibonacci transform,” *Scientific Reports*, vol. 15, no. 41439, 2025. doi: 10.1038/s41598-025-25760-4.
- [17] M. I. Kopp and I. Samudik, “Hidden attractors in a new 4D memristor-based hyperchaotic system: dynamical analysis, circuit design, synchronization, and its applications,” *Mathematics*, vol. 13, no. 17, p. 2838, Sep. 2025. doi: 10.3390/math13172838.
- [18] S. Subathra and V. Thanikaiselvan, “Enhanced security for medical images using a new 5D hyper chaotic map and deep learning based segmentation,” *Scientific Reports*, vol. 15, no. 22628, 2025. doi: 10.1038/s41598-025-04906-4.

- [19] L. Wang, Z. Chen, X. Sun, and C. He, “Color image ROI encryption algorithm based on a novel 4D hyperchaotic system,” *Physica Scripta*, vol. 99, no. 1, p. 015229, 2024. doi: 10.1088/1402-4896/ad14d1.
- [20] G. Yang, X. Zhang, and A. J. Moshayedi, “Implementation of the Simple Hyperchaotic Memristor Circuit with Attractor Evolution and Large-Scale Parameter Permission,” *Entropy*, vol. 25, no. 203, 2023. doi: 10.3390/e25020203.
- [21] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 7, no. 4, pp. 520–543, 1997. <https://doi.org/10.1063/1.166278>.
- [22] K. A. Korba, “La Sécurité des Réseaux de Capteurs sans fil Multimedia par des Systemes Chaotiques,” PhD thesis, Université 08 mai 45 Guelma (Algérie), 2022.
- [23] O. E. RöSSLer, “An Equation for Hyperchaos,” *Physics Letters A*, vol. 71, no. 2–3, pp. 155–157, 1979.
- [24] G. Pérez and H. A. Cerdeira, “Extracting Messages Masked by Chaos,” *Physical Review Letters*, vol. 74, no. 11, pp. 1970–1973, 1995.
- [25] R. V. Ravi, S. B. Goyal, C. Djeddi, and V. Kustov, “Colour image encryption based on HACS and Knuth-Durstenfeld algorithm,” in *Proc. Int. Conf. Computing, Intelligence and Data Analytics (ICCIDA)*, Lecture Notes in Networks and Systems, vol. 643, pp. 332–343, 2023. doi: 10.1007/978-3-031-27099-4_26.
- [26] D. Qiu, T. Zhang, J. Liu, S. Liu, and P. He, “An innovative image encryption algorithm based on the DNAS box and hyperchaos,” *Entropy*, vol. 27, no. 3, p. 239, 2025. doi: 10.3390/e27030239.
- [27] F. Meng, G. Wu, and J. Zhang, “A novel color image encryption algorithm based on fractional-order conservative memristive hyperchaotic system and extended zig-zag transform,” *J. King Saud Univ. – Comput. Inf. Sci.*, vol. 37, p. 151, 2025. doi: 10.1007/s44443-025-00163-7.
- [28] S. Akraam, “A chaos-based image encryption scheme using multiple chaotic maps,” *Mathematical Problems in Engineering*, vol. 2023, Article ID 2003724, 15 pages, 2023. doi: 10.1155/2023/2003724.
- [29] M. A. Hosny et al., “Efficient colour image encryption algorithm using a new fractional-order memcapacitive hyperchaotic system,” *Electronics*, vol. 11, no. 9, p. 1505, Sep. 2022. doi: 10.3390/electronics11091505.

-
- [30] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, “A new chaos-based fast image encryption algorithm,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 4, pp. 321–325, 2010.
- [31] H.-B. Li and X. Yang, “Componentwise Perturbation Analysis of the QR Decomposition,” *Mathematics*, vol. 10, no. 24, p. 4687, Dec. 2022. doi: 10.3390/math10244687.