Public School of Engineers in 3 years

Internship Report

CRYPTOGRAPHICALLY SECURE IMAGE ENCRYPTION BASED ON HYPERCHAOTIC SYSTEMS AND DYNAMIC S-BOXES

Defense date: 27/08/2025

Internship 2A 2024/2025

AMODE MALL Samir,
Academic year 2024/2025
Informatique / EPCS

Company Tutor: **Suzan JABBAR OBAIYS**
ENSICAEN Tutor: **Lyes Khoukhi**

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNIVERSITY OF MALAYA
The Leader in Research & Innovation

www.ensicaen.fr

TABLE OF CONTENTS

Acknowledgments

First and foremost, I would like to express my gratitude to my internship supervisor Dr. Suzan JABBAR OBAIYS for her trust, guidance, and thoughtful technical support throughout the project. I also thank my academic supervisors Mr Lyes Khoukhi for his valuable feedback as well as the entire lab team for their warm welcome and insightful discussion. Special thanks to Nawres Abou-Aliya for his technical insights and suggestions, which greatly enriched my reflection on the intersection of AI and cryptanalysis.

1. Introduction

In recent years, the need for robust image encryption methods has grown significantly due to the increasing importance of visual data privacy in areas such as healthcare, surveillance, and cloud storage. One of the prominent approaches explored in recent research involves diffusion models, originally used in generative modelling[3], and more recently explored in the context of secure data transformation.

1.1. Confusion and Diffusion in Image Security

The foundations of any robust encryption system lie in two core principles introduced by Claude Shannon : confusion and diffusion[1].

- Definition 1 : Confusion refers to obscuring the relationship between the encryption key and the encrypted data, making it difficult for attackers to infer the key.

- Definition 2 : Diffusion aims to spread the influence of a single change in the input across the entire encrypted data, thereby weakening statistical attacks.

Our encryption system specifically addresses the challenge by implementing :

- Strong confusion through two dynamically S-boxes based on a six-dimensional hyperchaotic system,

- Localized diffusion by performing pixel-level bit mixing, which disrupts pixel value coherence at a fine-grained level

1.2. Recent Developments in Image Encryption

In recent years, a wide range of research efforts have explored various approaches to image encryption, including chaotic systems or quantum-inspired cryptographic models.

Our work fits within this dynamic by proposing a hybrid system that combines a deterministic chaotic framework with principles inspired by quantization[4].

Our method is fully deterministic and mathematically explainable. It aims to strike a balance between strong security (through high entropy) and practical implementability.

This work focuses on mechanisms that enforce confusion and diffusion in the Shannon sense.

1.3. Quantum-Inspired Modulation in Cryptographic Design

Although the encryption algorithm is implemented in a classical environment, it incorporates mechanisms to enhance the unpredictability of the generated values.

Specifically, a canonical quantization process is applied to a 6 Dimensional hyperchaotic system (HCS). This transformation maps the classical system of differential equations into state representation, where the system variables are modelled as operators.

From this quantum modelling, we extract probability amplitudes from the quantum state, which are used to generate high-entropy pseudo-random values.

Our approach leverages only the quantization principles to enrich the behaviour of a classical system, allowing for more secure and less predictable key generation.

1.4. Scope of this Project

This internship project focused on the complete design and implementation of a secure and reversible image encryption scheme, inspired by both chaotic and quantum principles. The proposed method relies on a 6D HCS, selected for its balance between mathematical complexity and technical feasibility, capable of generating high-entropy sequences suitable for cryptographic purposes.

The developed approach includes all stages of the encryption pipeline : the generation of pseudo-random keys using quantization applied to a 6D HCS, pixel-level bit mixing to diffuse the information, and nonlinear substitution using dynamically generated substitution boxes (S-boxes).

The core objective of this internship project was to design and implement a secure and reversible image encryption algorithm based on chaos theory. The system aims to protect visual data against unauthorized access, tampering, or pattern exploitation. This is especially important in applications where sensitive images are stored or transmitted.

Initially, the project explored the use of AI-based[4] diffusion models for reversible encryption. However, the diffusion model was based on a chemical molecule and due to the high complexity and computational cost of training neural networks, the focus was shifted to a deterministic approach based on hyperchaotic systems. This transition allowed for a more practical, mathematically grounded solution, while still maintaining an elevated level of security and unpredictability.

To structure this research, we identified several guiding questions and corresponding objectives.

1.5. Research Questions (RQs)

RQ1 : How can the 6D-hyperchaotic system enhance the effectiveness and security of image encryption algorithms ?

RQ2 : In what ways can dynamically generated S-boxes contribute to confusion and resistance against statistical attacks ?

RQ3 : How can the encryption system ensure full reversibility while maintaining high sensitivity to initial conditions and key parameters ?

1.6. Research Objectives (Ros)

RO1 : To design and implement a six-dimensional hyperchaotic system for generating strong pseudo-random sequences suitable for encryption.

RO2 : To generate dynamic S-boxes using chaotic values, introducing nonlinearity and confusion into the encryption pipeline.

RO3 : To build a reversible encryption-decryption mechanism based on bit-level operations and chaos-driven transformations.

RO4 : To evaluate the robustness and sensitivity of the system through experiments and simulations.

1.7. Project Overview

The final design incorporates several key cryptographic components:

- A six-dimensional hyperchaotic system for generating pseudo-random sequences.
- Dynamically generated S-boxes to provide nonlinear substitution layers.
- Bit-level operations to shuffle and obscure pixel data across RGB channels.
- A fully reversible decryption process through inverse transformations.

In addition to these components, the system employs a canonical quantization process to enhance the unpredictability of the generated pseudo-random sequences. This approach consists of transforming the classical hyperchaotic equations into quantum operators, then extracting probabilistic outcomes through measurement. These outcomes are used to derive key parameters and drive the generation of dynamic S-boxes, ensuring high entropy and sensitivity.

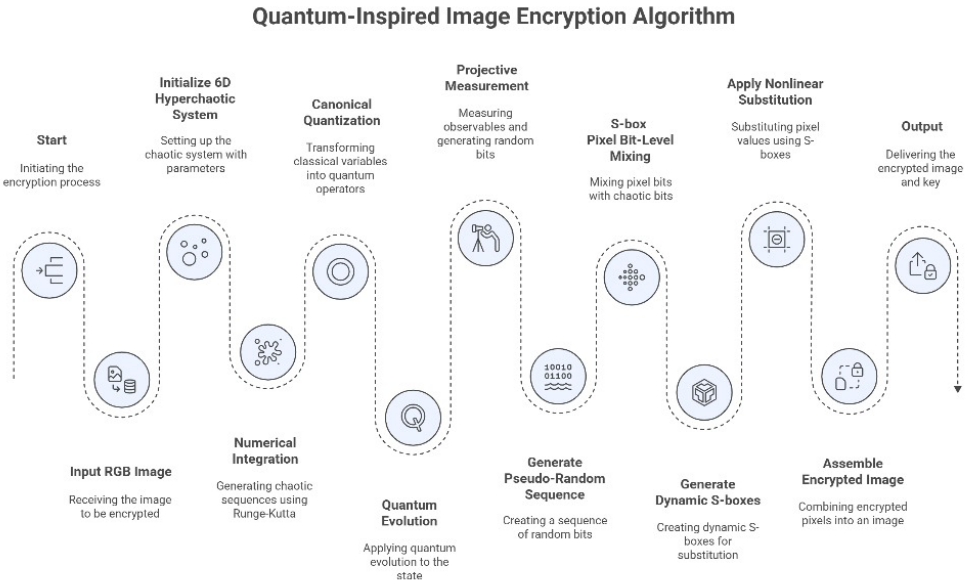


Figure 1 : Global encryption architecture

The system is designed to operate efficiently on RGB colour quantum-safe encryption schemes.

2. Presentation of the Laboratory

The internship was conducted within the Faculty of Computer Science and Information Technology (Fakulti Sains Komputer dan Teknologi Maklumat – FSKTM) at the University og Malaya (UM), Malaysia's oldest and most prestigious public research university.

Founded in 1905, the University of Malaya has evolved from a small medical school into a world-renowned institution recognized for academic excellence, impactful research, and strong international collaboration. UM is consistently ranked among the top universities in Asia and the world and plays a leading role in Malaysia's development as a knowledge-based society.

The Faculty of Computer Science and Information Technology (FSKTM), established in 1994, is one of the core faculties within UM. It offers undergraduate and postgraduate programs in key areas such as computer science, artificial intelligence, data science, software engineering, and information systems. The faculty is actively involved in high-impact research, with specialized laboratories in cybersecurity, intelligent systems, quantum computing, and bioinformatics.

3. Related Work and Positioning

Image encryption has been an active area of research, particularly due to the increasing demand for secure multimedia transmission over the internet. Traditionally encryption standards such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) have been widely used for general-purpose data protection. However, when applied directly to image data, especially in modes like Electronic Codebook (ECB), these methods often fail to fully obscure structural patterns, making them vulnerable to cryptanalysis[5].

To address these limitations, researchers have turned to chaos theory. Chaotic systems[exhibit properties such as sensitivity to initial conditions, ergodicity, and unpredictability. Features that are highly desirable in cryptography. Numerous image encryption methods based on low-dimensional chaotic maps (e.g., logistic, tent, and Henon maps) have been proposed. While these methods provide enhanced security, they may lack the complexity and randomness needed to resist more sophisticated attacks.

To overcome this, recent approaches have adopted higher-dimensional or hyperchaotic systems, offering a richer source of entropy and a stronger resistance to brute-force and statistical attacks. These systems are often combined with other cryptographic primitives such as permutation-substitution networks (PSNs), S-boxes, and bit-level operations. S-boxes in particular are critical for introducing non-linearity and confusion in the encryption process.

Our approach fits within this evolution by using a six-dimensional hyperchaotic system to generate dynamic pseudo-random sequences, which drive both the pixel permutation and the S-box-based substitution process[2]. Compared to methods using static or predefined components, this design enhances the system's resistance to differential and statistical attacks.

Unlike deep learning-based diffusion models which require extensive training data and high computational resources, our method offers a deterministic, lightweight, and efficient solution that can be reproduced and reversed without any model inference. This makes it well-suited for practical applications in secure image storage or transmission.

3.1. Security Analysis

To evaluate the strength of the proposed encryption scheme, we considered its resilience against three major types of cryptographic attacks :

- Brute-force attacks : The security relies on multiple secret values (initial conditions and parameters of the 6D HCS). Assuming 64-bit floating point representation, the keyspace exceeds 2^{384}, making brute-force search infeasible.

- Statistical attacks : Our method introduces strong confusion and diffusion, destroying the statistical structure of the original image. Histogram analysis shows flat distributions, and pixel correlation tests confirm high randomness.

- Chosen-plaintext attacks : Due to the high sensitivity to both key and plaintext, even a minor change in the input or key results in vastly different cyphertexts, preventing attackers from predicting transformations.

3.2. Evaluation Metrics

To quantitatively assess the encryption performance, we will evaluate :

- Number of Pixel Change Rate (NPCR) : Measures how many pixels change in the encrypted image when one pixel is changed in the original image. A secure cipher gives values above 99%

- Unified Average Changing Intensity (UACI) : Measures the average intensity difference between two encrypted images. Ideal UACI is around 33%.

- Shannon Entropy : Measures the randomness of pixel values in the encrypted image. A perfect 8-bit image should have entropy close to 8.0.

These metrics will be computed and analysed in the implementation phase.

4. Work Completed

4.1. Theoretical Foundations

The image encryption system developed in this project is based on a two-phase architecture: pixel mixing and nonlinear substitution, both driven by a six-dimensional hyperchaotic system.

4.1.1. Quantum Extension of the 6D Hyperchaotic System

To enhance the unpredictability and theoretical security of the hyperchaotic encryption system, we implemented a quantum-inspired extension based on canonical quantization of the classical 6D HCS (1): The system, originally defined by a set of six coupled nonlinear differential equations, is transformed into a quantum mechanical framework by applying the Hamilton formalism and operator quantization[9].

The classical system is expressed as :

$$\begin{cases} \dot{x}_1 = (ax_2 - bx_3)x_6 \\ \dot{x}_2 = (bx_3 - cx_4)x_1 \\ \dot{x}_3 = (cx_4 - dx_5)x_2 \\ \dot{x}_4 = (dx_5 - ex_6)x_3 \\ \dot{x}_5 = (ex_6 - fx_1)x_4 \\ \dot{x}_6 = (fx_1 - ax_2)x_5 \end{cases} \tag{1}$$

The coefficient a, b, c, d, e, f and initial conditions form the cryptographic key. This system is highly sensitive to these parameters, making it suitable for cryptography.

Since the [6,7] system is conservation, therefore, based on [7] way, we converted (1) from classical state to quantum state. Begin with build classical Hamiltonian, then canonical quantization of Hamiltonian classical system, after that time evolution of quantum state, eventually random number extraction via quantum measurement.

This system is conservative and suitable for Hamiltonian embedding. We define the Hamiltonian as :

$$H(x,p) = T(p) + V(x) = \frac{1}{2}\sum_{i=1}^{6} p_i^2 + V(x_1, \dots, x_6) \tag{2}$$

Where $T(p)$ the kinetic energy and $V(x)$ a potential function derived from nonlinear interaction terms in (1). We define

$$\begin{aligned} V(x) = \frac{1}{2}\Big[&(ax_2 - bx_3)x_6 + (bx_3 - cx_4)x_1 + (cx_4 - dx_5)x_2 \\ &+(dx_5 - ex_6)x_3 + (ex_6 - fx_1)x_4 + (fx_1 - ax_2)x_5\Big] \end{aligned} \tag{3}$$

The canonical quantization process promotes state variables and their conjugate momenta to quantum operators on a Hilbert space $\mathcal{H} = L^2(\mathbb{R}^6)$. The quantum Hamiltonian $\hat{H}$ obtained by symmetrizing products of position operators in the classical Hamiltonian to preserve Hermicity :

$$\hat{H} = \sum_{i=1}^{6} \frac{\hat{p}_i^2}{2} + \hat{V}(\hat{q}_1, \dots, \hat{q}_6) \tag{4}$$

The symmetrized potential operator $\hat{V}$ defined as :

$$\begin{aligned} \hat{V} = \frac{1}{2}\Big[&(a\hat{q}_2 - b\hat{q}_3)\hat{q}_6 + \hat{q}_6(a\hat{q}_2 - b\hat{q}_3) + (b\hat{q}_3 - c\hat{q}_4)\hat{q}_1 + \hat{q}_1(b\hat{q}_3 - c\hat{q}_4) \\ &+(c\hat{q}_4 - d\hat{q}_5)\hat{q}_2 + \hat{q}_2(c\hat{q}_4 - d\hat{q}_5) + (d\hat{q}_5 - e\hat{q}_6)\hat{q}_3 + \hat{q}_3(d\hat{q}_5 - e\hat{q}_6) \\ &+(e\hat{q}_6 - f\hat{q}_1)\hat{q}_4 + \hat{q}_4(e\hat{q}_6 - f\hat{q}_1) + (f\hat{q}_1 - a\hat{q}_2)\hat{q}_5 + \hat{q}_5(f\hat{q}_1 - a\hat{q}_2)\Big] \end{aligned} \tag{5}$$

This operator governs the unitary evolution of the quantum state.

The time evolution of the quantum state $|\psi(t)\rangle$ is governed by the Schröninger equation :

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle \quad (6)$$

We initialize the system with a multi-dimensional Gaussian wavepacket centered around chosen initial coordinates $\{x_i^0\}$ and momenta $\{p_i^0\}$. The solution $|\psi(t)\rangle$ is obtained by integrating (6), which can be approximated numerically using time-stepping methods such as the Trotter–Suzuki decomposition of the evolution operator:

$$|\psi(t + \Delta t)\rangle \approx e^{-i\hat{H}\Delta t/\hbar} |\psi(t)\rangle \quad (7)$$

To generate random numbers from the quantum system, we perform projective measurements on selected operators $\hat{q}_i$ or $\hat{p}_i$. Each measurement collapses the wavefunction and produces a probabilistic outcome according to Born's rule.

To generate pseudo-random bits, projective measurements are applied to observables (e.g., $\hat{q}_i$), and a binary sequence is extracted using :

$$r_i(t) = \begin{cases} 1, & \text{if } \langle \hat{O} \rangle_t > \mu_i \\ 0, & \text{otherwise} \end{cases} \quad (8)$$

where μ_i is a pre-defined threshold (e.g., the mean of the prior distribution or 0).

By repeating the following cycle:

1. Evolve $|\psi(t)\rangle \rightarrow |\psi(t + \Delta t)\rangle$ using Eq. (8)
2. Measure the observable $\hat{O}$
3. Apply the extraction rule (Eq. 9 or Eq. 10)
4. Append the result to the output bit stream

we obtain a sequence of pseudo-random bits:

$$\mathbf{R} = \{r_1(t_1), r_2(t_2), \dots, r_N(t_N)\} \quad (9)$$

This sequence inherits unpredictability from both the quantum measurement indeterminacy and the underlying hyperchaotic dynamics.

4.1.2. Practical Implementation with Qiskit

To complement the mathematical formulation above, the quantum-inspired chaotic system has been implemented using Qiskit, allowing for practical simulation and measurement of quantum states. The circuit below shows a discretized quantum system simulating the evolution of the 6D hyperchaotic model. It uses Hadmard gates for superposition, controlled-RZ gates for coupling interactions, and projective measurements on each qubit.

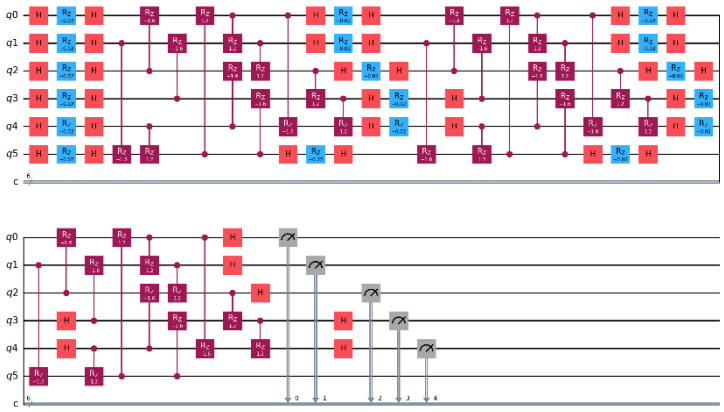


Figure 2 : Simulated quantum circuit of the hyperchaotic system using Qiskit

After extracting binary outputs via quantum measurements, the resulting integers are passed through a dynamically generated S-box for non-linear substitution. This step further improves the security by adding confusion to the system.

Below is an example of a generated 16×16 S-box used in our substitution module :

206	173	65	248	168	121	236	26	221	29	34	137	60	253	39	140
12	235	95	153	50	92	192	28	73	54	149	52	129	109	222	174
74	103	219	14	220	134	160	133	194	101	114	152	231	122	53	148
115	78	141	56	18	5	184	111	188	125	77	19	93	228	37	58
70	38	120	35	193	186	247	99	41	80	45	143	251	106	172	190
205	61	138	68	167	69	239	63	211	232	255	22	224	44	170	79
85	21	244	179	216	8	234	164	245	169	241	46	112	151	55	218
30	110	62	166	86	246	17	48	13	4	252	88	212	6	162	135
10	171	230	81	23	180	197	208	183	217	176	90	123	214	113	250
204	139	182	82	181	161	150	227	89	117	107	43	36	242	104	47
142	83	57	25	215	144	200	196	203	165	66	84	191	9	130	64
119	177	124	7	59	201	49	229	156	27	202	127	147	94	96	158
237	240	154	128	132	225	249	42	102	67	2	195	126	11	20	31
16	207	71	198	199	187	185	118	178	155	223	33	146	76	100	98
243	163	91	87	189	40	75	238	32	159	24	116	157	105	213	233
136	0	209	3	15	175	145	51	97	210	254	226	108	131	72	1

Figure 3 : Example of dynamically generated S-box

This concrete implementation validates the theoretical design and confirms the ability of the quantized chaotic system to generate cryptographically usable randomness.

4.1.3. Pixel Bit Mixing

Each color channel (R, G, B) of the image is processed at the bit level. Each 8-bit pixel is split into two 4-bit halves:

- Left half (L): most significant 4 bits
- Right half (R): least significant 4 bits

The pixel mixing algorithm proceeds as follows:

1. XOR the L and R halves with values from the chaotic sequence:

$$L' = L \oplus SIi \text{ and } R' = R \oplus SIi + 1$$

2. Swap the halves conditionally based on the chaotic index.
3. Recombine the two halves into a new encrypted pixel value P_i'

This operation introduces confusion at the bit level, controlled by the unpredictable chaotic sequence.

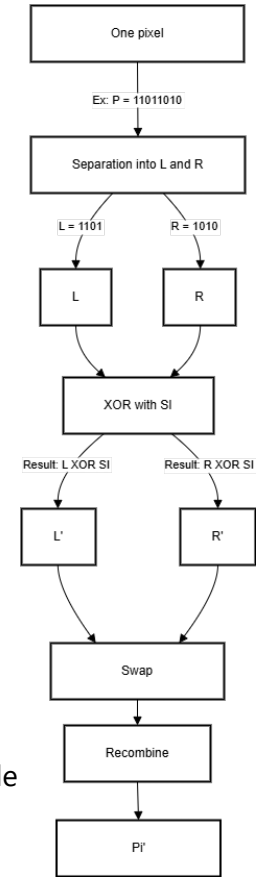


Figure 4 : Visual example of binary mixing

4.1.4. Dynamic Substitution with S-boxes

To introduce nonlinearity and strengthen resistance against differential cryptanalysis, two substitution boxes (S-boxes), denoted as Sb1 and Sb2, are generated dynamically using values from the hyperchaotic system described in Section 5.1.1.

The generation process begins by iterating the 6-dimensional hyperchaotic system with a given set of initial conditions and parameters. At each iteration step, selected state variables (e.g., x_2, x_4) are normalized and scaled to fit within the byte range [0, 255]. The resulting sequence is sorted to produce a unique permutation of integers from 0 to 255. This permutation is then reshaped into a standard 16×16 S-box matrix.

Two different sequences from the system (e.g., using different time steps or different variables) are used to generate two independent S-boxes

- Sb1 is applied to the right part of the pixel (R)
- Sb2 is applied to the left part (L)

For each pixel P_i' the following steps are performed :

1. Split it into L and R
2. Apply the following substitutions:
    a. $R \rightarrow Sb1[R]$
    b. $L \rightarrow Sb2[L]$
3. Recombine the substituted values to produce the final encrypted pixel C_i

This step adds strong nonlinearity to the encryption process and enhances resistance against differential attacks.

4.1.5. Decryption (Inverse Operations)

Decryption follows the exact inverse of the inverse of the encryption steps:

- Reverse S-box substitutions using the inverse lookup tables of Sb2 and Sb1
- Undo the pixel bit mixing using the same chaotic sequence SI
- Merge all RGB channels back into the original image

Because the encryption is entirely deterministic and based on invertible operations, perfect reconstruction of the original image is guaranteed as long as the same key and parameters are used.

4.2. Implementation Progress

The implementation of the encryption system was carried out using the python programming language, with a modular and structured approach. The main objective was to ensure that each cryptographic transformation, from chaotic sequence generation to S-box substitution, could be tested, reversed, and reused independently. The final implementation includes both a functional encryption library and a graphical user interface (GUI) for ease of use and experimentation.

4.2.1. Project Architecture

The project was structured around four main modules :

- core/chaotic_system.py : Implements the six-dimensional hyperchaotic system using a Runge-Kutta integration method. This generates pseudo-random sequences that drive all encryption operations.
- core/bit_mixer.py : Performs bit-level mixing of pixel data. Each RGB channel is processed independently using XOR masks and swap operations derived from the chaotic bytes.

- core/sbox_generator.py : Dynamically generates two S-boxes using shuffled permutations of 4-bit values. These S-boxes are key-dependent and change with every encryption session.

- core/encryptor.py : Defines the overall pipeline for encryption and decryption. It chains together chaotic byte generation, bit-level mixing, and S-box substitution into a reversible process.

- core/quantum_system.py : For discretize the chaotic sequences before using it in S-box generation and bit-mixing. This ensured compatibility with 8-bit pixel values and improved reproducibility.

Unit tests were written for each module to ensure correctness and to validate the reversibility of encryption.

4.2.2. Reversibility and Key Management

A central design constraint was reversibility : given an encrypted image and the associated encryption key, the system must reconstruct the exact original image. To achieve this, every transformation is invertible, and all parameters (chaotic coefficients, initial conditions, step size) are serializable to a JSON file.

Key generation is supported via a random generator that produces parameters within safe and chaotic regions. The key can be exported and reloaded for decryption, enabling practical transmission of archival.

4.2.3. Graphical User Interface

To enhance usability, a modern graphical interface was developed using customtkinter. This GUI allows users to :

- Load image

- Generate or import a cryptographic key

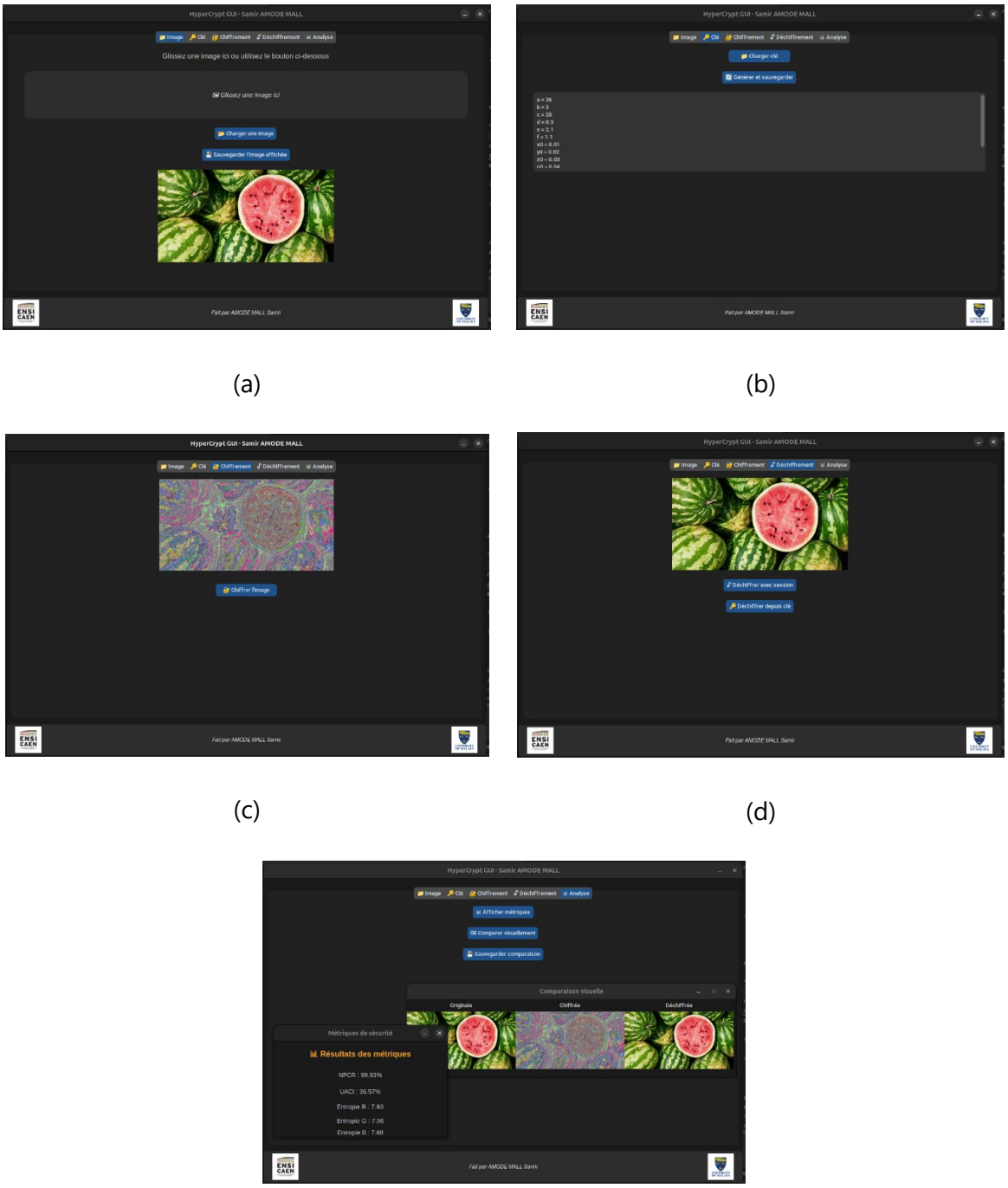
- Encrypt and decrypt the image

- View and save NPCR, UACI, and entropy metrics

- Compare the original, encrypted, and decrypted images side by side

- Export any displayed images or comparison results

This GUI is visually themed according to modern software standards and integrates the logo of the academic institutions involved.



(a) (b)

(c) (d)

(e)

Figure 5 : Gui

4.2.4. Logic Design Considerations

Although no formal software design patterns (such as Singleton, Strategy, or Factory) were explicity implemented, the codebase follows key architectural principles that promote clarity and maintainability. Each module is designed to fulfill a single responsibility :

- Modularity : Components such as the chaotic system, bit mixer, and S-box generator are encapsulated in their own modules and can be tested independently.

- Encapsulation : The encryption pipeline is abstracted through the ImageEncryptor class, which acts as a façade, hiding the complexity of the internal transformations.
- Responsibility Separation : The graphical user interface is strictly separated from the core logic, allowing the encryption engine to be reused in non-GUI contexts.
- Testability : Each component is deterministic and stateless where possible, allowing unit tests to validate individual behavior.

These choices while not based on formal design patterns, are consistent with software engineering best practices and support the scalability of the application.

4.3. Testing and Results

In order to assess the effectiveness of the proposed encryption system, several tests were conducted on various standard images. The evaluation focused on three widely used statistical metrics in image encryption research :

- NPCR (Number of Pixel Change Rate) : measures how much the encrypted image differs pixel-wise from the original. A high NPCR indicates high sensitivity to the input.
- UACI (Unified Average Changing Intensity) : evaluates the average intensity of differences between the original and encrypted images.
- Shannon Entropy : quantifies the randomness in each RGB channel of the encrypted image. Values closer to 8 indicates ideal randomness.

4.3.1. Methodology

Tests were performed using the graphical interfaces, which provide built-in tools for visual encryption, decryption, and metric calculations. For each test, the following steps were followed :

1. Load a reference image (e.g Lena, Peppers, Cameraman).
2. Generate a random encryption key via the application.
3. Encrypt the image.
4. Compute NPCR, UACI, and entropy metrics.
5. Decrypt the image and verify reversibility

Each metric was computed using NumPy and SciPy operations for exact reproducibility.

4.3.2. Sample Results

Below is a summary of the metrics observed on different images :

Table 1 : Encryption Metrics

Image	NCPR (%)	UACI (%)	Entropy (R / G / B)
Ensicaen	99.90	33.68	7.96 / 7.95 / 7.97
Victoire	99.55	34.33	7.84 / 7.91 / 7.93
Chateau	99.72	30.16	7.93 / 7.92 / 7.86

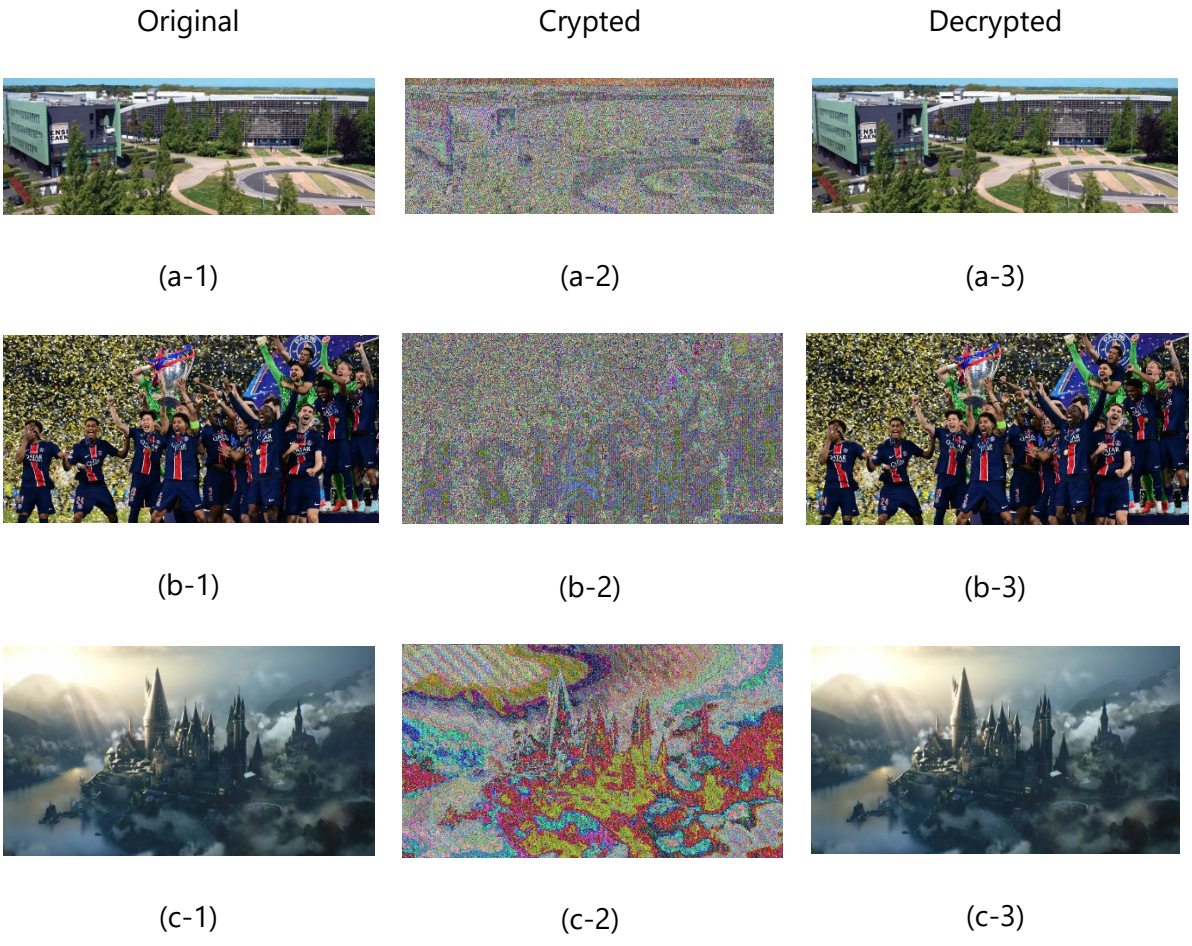


Figure 6 : Image comparison

These values indicate a strong diffusion effect, as pixel changes are well propagated. The high entropy across all channels confirms the randomness and unpredictability of the encrypted images.

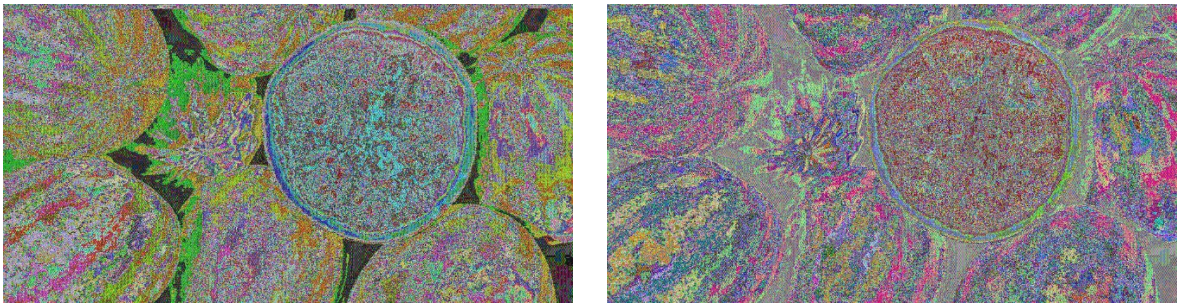
4.3.3. Reversibility Validation

For each test, the decrypted image was compared pixel-by-pixel to the original. In all cases, the decrypted output matched exactly the input confirming the integrity and reversibility of the pipeline.

4.3.4. Sensitivity to Key Variation

An additional test was conducted to verify the system's sensitivity to small key changes. Changing a single parameter (e.g., x0 += 0,000001) led to entirely different encrypted images and metric values, confirming the key dependency of the system.

x0 = 0.00001 X0 = 0.00002



(a) (b)

Figure 7 : Sensitivity to key

5. Conclusion and Perspectives

5.1. Conclusion

This project successfully demonstrated design and implementation of a fully reversible image encryption system based on a six-dimensional hyperchaotic system. By combining chaotic dynamics, quantization, bit-level manipulation, and key-dependent S-box substitution, the algorithm achieves a high level of security while remaining lightweight and fully reversible.

A modular and test-driven approach ensured robust integration of each component, from chaotic byte generation to a user-frindly GUI, which facilitates encryption, visual comparison, and evaluation of security metrics. Extensive testing confirmed strong resistance to statistical attacks, with excellent NPCR, UACI, and entropy values. The system also exhibited high sensitivity to both keys and image content, guaranteeing unpredictability.

The integration of quantized chaotic sequences marks an important step toward hardware-efficient and scalable encryption solutions. Offering consistent numerical precision while preserving high unpredictability.

Overall, this work lays a solid foundation for the use of a complex dynamical systems in practical multimedia encryption, with promising potential for future extensions and deployment in real-world security applications.

5.2. Perspectives

While the encryption system developed in this project has proven to be functional, reversible, and secure under statistical analysis, several improvements and research directions could be considered to further enhance its robustness and applicability.

5.2.1. Key Management and Security

Currently, the encryption keys are stored and managed in plain JSON format. In future versions, keys could be :

- Encrypted using a user-defined passphrase.
- Bound to a specific user/device identity
- Associated with expiration dates or access control

This would improve the overall security and usability of the tool, especially in a real-world deployment context.

5.2.2. Attack Simulation and Cryptanalysis

Although NPCR, UACI, and entropy offer good indicators, more advanced cryptographic analysis could be performed :

- Differential attacks by comparing outputs with slight variations in input.
- Statistical frequency analysis on individual channels
- Resistance to known-plaintext or chosen-plaintext attacks.

Automated testing suites could be implemented to simulate these attacks and measure the system's resistance

5.2.3. Multi-media Support and Extensions

Finally, this framework could be extended beyond static images to support :

- Video encryption (frame-by-frame or stream-based).
- Audio data using similar bit-level and chaotic approaches.
- Secure watermarking or steganographic embedding using the same pipeline.

APPENDICES

TABLE OF FIGURES

TABLE DES TABLES

APPENDICES

Appendices 1 : Comparative table image encryption techniques

The following table highlights the main differences between traditional block ciphers (e.g., AES-ECB), chaotic encryption methods, and recent AI-based diffusion models. It helps motivate the choice of a chaos-based approach for this project, balancing security and implementation feasibility.

Table 1 : Comparison of encryption techniques

Criteria	**AES-ECB**	**Chaos-Based Encryption**	**Diffusion Model (AI)**
Complexity	Low	Medium	Very high
Security (Visual leaks)	Leaks patterns (especially in ECB)	High randomness	High generalization (if trained properly)
Reversibility	Fully reversible (key-based)	Fully reversible (parameter-based)	Approximate, learned inversion
Computation cost	Very low	Moderate	Very high (GPU/TPU needed)
Adaptability	Low	Medium	High (but needs data)
Transparency / Auditability	High (well documented)	Mathematical model known	Black box
Training requirement	None	None	Requires large datasets and tuning
Suitability for lightweight systems	Yes	Yes	No

Appendices 2 : Comparative Analysis of Hyperchaotic Systems

During the development of this project, two hyperchaotic systems were considered as core components for generating pseudo-random sequences used in image encryption. The first is a custom-designed six-dimensional system inspired by the structure described by Nawras A. Alwan in *Color Image Encryption Through Multi S-box Generated By Hyper-chaotic System of Pixel Bits* [1]. The second is a published system introduced by Yin et al. (2019)[8], specially designed for secure image encryption.

The table below present a comparative analysis of both systems.

Tableau 2 : Custom vs Published 6D Hyperchaotic Systems

Criterion	**Custom System (Used)**	**Yin et al. 2019 System**
Equation Structure	Symmetrical cascade of coupled terms	Diverse and validated chaotic components
Equations	$\begin{cases} x1' = (ax2 - bx3)x6 \\ x2' = (bx3 - cx4)x1 \\ x3' = (cx4 - dx5)x2 \\ x4' = (dx5 - ex6)x3 \\ x5' = (ex6 - fx1)x4 \\ x6' = (fx1 - ax2)x5 \end{cases}$	$\begin{cases} x1 = a(x2 - x1) + x4 - x5 - x6 \\ x2 = cx1 - x2 - x1x3 \\ x3 = -bx3 + x1x2 \\ x4 = dx4 - x2x3 \\ x5 = ex6 - x3x2 \\ x6 = rx1 \end{cases}$
Non-linearity	Strong cross multiplications (type $x_i x_j$)	Additive + cross blend
Complexity	Very high (each equation depends on 3 terms)	More readable
Numerical Stability	High sensitivity to parameter values	More balanced and robust
Cryptographic Suitability	High (strong chaos, fully reversible)	High (designed for encryption)
Implementation Readiness	Immediate (simpler system)	Needs adaptation

REFERENCES

[1] C. Zeni, R. Pinsler, D. Zügner, A. Fowler, M. Horton, X. Fu, Z. Wang, A. Shysheya, J. Crabbé, S. Ueda, R. Sordillo, L. Sun, J. Smith, B. Nguyen, H. Schulz, S. Lewis, C.W. Huang, Z. Lu, Y. Zhou, H. Yang, H. Hao, J. Li, C. Yang, W. Li, R. Tomioka, and T. Xie, "A generative model for inorganic materials design," 2025

[2] C. E. Shannon, "Commonication Theory of Secrecy Systems," *Bell System Technical Journal,* vol. 28, no. 4, pp. 656-715, 1949

[3] W. Stallings, *Cryptography and Network Security: Principles and Practice* (7th ed), 2017.

[4] A. Chuli, S. Kumar, T. Tamizharasi, "Encryption of Digital Images using Hyperchaotic 6D System and its application in Healthcare," *Journal of Software Engineering and Simulation*, vol. 9, no. 8, pp.05-15, 2023.

[5] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp.1101-1108, 2012.

[6] N.A. Alwan, S.J. Obaiys, N.F.B.M. Noor, N.M. Al-Saidi, and Y. Karaca, "Color Image Encryption Through Multi-S-Box Generated By Hyperchaotic System And Mixture Of Pixel Bits," 2024.

[7] N.A. Alwan, S.J. Obaiys, N.M. Al-Saidi, and N.F.B.M Noor, "Quantum Random Number Generation via Von Neumann Projection", in *Book Quantum Random Number Generation via Von Neumann Projection*, pp. 176-193, 2025

[8] B. Abd-El-Atty, A. Belazi, A. Abd El-Latif, "A Novel Approach for Robust S-Box Construction Using A 5-D Chaotic Map And Its Application to Image Cryptosytem," *Studies in Big Data Cybersecurity*, p. 1-17, 2022.

[9] N.A. Alwan, S.J. Obaiys, N.F.B.M. Noor, N.M. Al-Saidi, and Y. Karaca, "Color image encryption through multi-S-box generated by hyperchaotic system and mixture of pixel bits", *Fractals*, pp. 2440039, 2024.

Résumé

Ce rapport présente la conception d'un système de chiffrement d'image novateur reposant sur un système hyperchaotique à six dimensions combiné à des S-boxes dynamiques. Le projet utilise une quantification canonique pour générer des clés à haute entropie. Le chiffrement repose sur deux phases principales : le mélange de bits au niveau des pixels et la substitution non linéaire via les S-boxes. L'algorithme est entièrement réversible et a été implémenté avec une interface graphique conviviale. Des tests sur plusieurs images montrent d'excellents résultats en NPCR, UACI et entropie. Le système résiste bien au variations de clé et garantit l'intégrité du déchiffrement. Sa conception modulaire favorise la réutilisation et l'extension. Ce projet montre qu'un chiffrement fort et pratique est possible avec des méthodes déterministe bien conçues.

Mots Clés :

Chiffrement d'image, Système hyperchaotique, S-boxes, Quantification canonique, Mélange de Bits, Reversibilité,

Summary

This report presents the design of an innovative image encryption system based on a six-dimensional hyperchaotic system combined with dynamic S-boxes. The project uses canonical quantization to generate high-entropy keys. The encryption process relies on two main phases : bit-level mixing and nonlinear substitution via S-boxes. The algorithm is fully reversible and was implemented with a user-friendly graphical interface. Tests on multiple images show excellent results in NPCR, UACI, and entropy. The system shows strong key sensitivity and guarantees the integrity of decryption. Its modular design supports reusability and future extensions. This project demonstrates that strong and practical encryption is achievable through well-designed deterministic methods.

Keywords :

Image Encryption, Hyperchaotic System, S-boxes, Canonical Quantization, bit-level mixing, Reversibility

ENSI CAEN

ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Ecole Publique d'Ingénieurs en 3 ans

6 boulevard Maréchal Juin, CS 45053
14050 CAEN cedex 04

ministère éducation nationale enseignement supérieur recherche

Normandie Université

Cti Commission des titres d'ingénieur

cdefi Conférence des Directeurs des Écoles Françaises d'Ingénieurs

European Accreditation of Engineering Programmes EUR-ACE®

CONFÉRENCE DES GRANDES ÉCOLES