**FIRAT UNIVERSITY**
**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**
**TÜRKİYE**

# IMPROVEMENT OF A ROBUST IMAGE ENCRYPTION ALGORITHM FOR SECURITY OF DIGITAL IMAGES

**Aina'u SHEHU MUHAMMED**

Master's Thesis

DEPARTMENT OF SOFTWARE ENGINEERING

JULY 2021

**FIRAT UNIVERSITY**
**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**
**TÜRKİYE**

Department of Software Engineering

Master's Thesis

# IMPROVEMENT OF A ROBUST IMAGE ENCRYPTION ALGORITHM FOR SECURITY OF DIGITAL IMAGES

Author
**Aina'u SHEHU MUHAMMED**

Supervisor
Assoc. Prof. Dr. Fatih ÖZKAYNAK

JULY 2021
ELAZIG

**FIRAT UNIVERSITY**
**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**
**TÜRKİYE**

Department of Software Engineering

Master's Thesis

| | |
|---|---|
| Title: | Improvement of a Robust Image Encryption Algorithm for Security of Digital Images |
| Author: | Aina'u SHEHU MUHAMMED |
| Submission Date: | 07 June 2021 |
| Defense Date: | 07 July 2021 |

# THESIS APPROVAL

This thesis, which was prepared according to the thesis writing rules of the Graduate School of Natural and Applied Sciences, Fırat University, was evaluated by the committee members who have signed the following signatures and was unanimously approved after the defense exam made open to the academic audience.

*Signature*

| | | |
|---|---|---|
| Supervisor: | Assoc. Prof. Dr. Fatih ÖZKAYNAK<br>Fırat University, Faculty of Technology | Approved |
| Chair: | Assist Prof. Dr. Soner KIZILOLUK<br>Turgut Özal University, Faculty of Engineering and Natural Sciences | Approved |
| Member: | Assist Prof. Dr. Yaman AKBULUT<br>Fırat University, Faculty of Technology | Approved |

This thesis was approved by the Administrative Board of the Graduate School on

..... / ..... / 20 .....

*Signature*

Associated Prof. Dr. Kürşat Esat ALYAMAÇ
Director of the Graduate School

# DECLARATION

I hereby declare that I wrote this Master's Thesis titled “Improvement of a Robust Image Encryption Algorithm for Security of Digital Images” in consistent with the thesis writing guide of the Graduate School of Natural and Applied Sciences, Firat University. I also declare that all information in it is correct, that I acted according to scientific ethics in producing and presenting the findings, cited all the references I used, express all institutions or organizations or persons who supported the thesis financially. I have never used the data and information I provide here in order to get a degree in any way.

07 July 2021

**Aina’u SHEHU MUHAMMED**

# PREFACE

One of the topics that have successful applications in engineering technologies and computer science is chaos theory. The remarkable area among these successful applications has been especially the subject of chaos-based cryptology. Many practical applications have been proposed in a wide spectrum from image encryption algorithms to random number generators, from block encryption algorithms to hash functions based on chaotic systems. In this thesis study, it is aimed to achieve various advances in both theoretical and practical fields by proposing a new image encryption algorithm that focuses on chaotic systems.

This thesis was supported by the project number **TEKF.20.13** by Firat University Scientific Research Projects Coordination Unit (FÜBAP) and project number **120E444** by the Scientific and Technological Research Council of Turkey (TÜBİTAK).

**Aina'u SHEHU MUHAMMED**
ELAZIG, 2021

# TABLE OF CONTENTS

Page

# ABSTRACT


## Improvement of a Robust Image Encryption Algorithm for Security of Digital Images

**Aina'u SHEHU MUHAMMED**

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Software Engineering

July 2021, Page: x + 34

One of the general problems in modern digital society is undoubtedly the information security topic. It is critical to ensure the security of information transferred, processed, and stored throughout digital channels. Among this information, digital images draw attention in terms of frequency of use in digital channels. In this thesis study, a new image encryption algorithm is proposed to address the security problems of digital images. The aspect that differentiates the proposed algorithm from thousands of image encryption algorithms in the literature is that it is designed within the framework of the provable security design principle. The provable security design approach has ensured that the proposed algorithm is theoretically secure with mathematical proof techniques. In addition to addressing the proposed architecture security concerns, the hybrid random number generator used as the key generator constitutes another unique aspect. This generator, which was designed using chaotic systems, physical unclonable functions, and optimization algorithms, stands out as the innovative aspect of the thesis study. The statistical randomness properties of the proposed random number generator were tested using the NIST SP 800-22 Statistical Test Suite. Successful results were obtained for 15 tests in the test package. In addition, the success of these outputs was tested on a new image encryption algorithm. The security of the proposed algorithm was tested from different angles using various experimental analyzes and a 12-step provable security analysis roadmap. Successful analysis results and performance measurements indicate that the proposed cryptographic components can be used in many information security applications and many future designs.

.



**Keywords:** Chaos; Image encryption; Key generation; Random number generator,

# ÖZET

## Sayısal Görüntülerin Güvenliği için Gürbüz Bir Görüntü Şifreleme Algoritmasının Geliştirilmesi

**Aina'u SHEHU MUHAMMED**

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Yazılım Mühendisliği Anabilim Dalı

Temmuz 2021, Sayfa: x + 34

Modern dijital toplumun genel sorunlarından biri de kuşkusuz bilgi güvenliği konusudur. Dijital kanallar üzerinden aktarılan, işlenen ve saklanan bilgilerin güvenliğini sağlamak kritik önem taşır. Bu bilgiler arasında sayısal kanallarda kullanım sıklığı açısından sayısal görüntüler dikkat çekmektedir. Bu tez çalışmasında, sayısal görüntülerin güvenlik problemlerini gidermek için yeni bir görüntü şifreleme algoritması önerilmiştir. Önerilen algoritmayı literatürdeki binlerce görüntü şifreleme algoritmasından ayıran özellik, kanıtlanabilir güvenlik tasarımı ilkesi çerçevesinde tasarlanmış olmasıdır. Kanıtlanabilir güvenlik tasarımı yaklaşımı, önerilen algoritmanın matematiksel ispat teknikleri ile teorik olarak güvenli olmasını sağlamıştır. Önerilen mimari güvenlik endişelerini ele almanın yanı sıra, anahtar üreteci olarak kullanılan hibrit rasgele sayı üreteci başka bir özgün yönü oluşturmaktadır. Kaotik sistemler, fiziksel klonlanamayan fonksiyonlar ve optimizasyon algoritmaları kullanılarak tasarlanan bu üreteç, çalışmanın yenilikçi yönü olarak öne çıkmaktadır. Önerilen rastgele sayı üretecinin istatistiksel rastgelelik özellikleri, NIST SP 800-22 İstatistiksel Test Paketi kullanılarak test edilmiştir. Test paketindeki 15 test için başarılı sonuçlar elde edilmiştir. Ayrıca bu çıktıların başarısı yeni bir görüntü şifreleme algoritması üzerinde test edilmiştir. Önerilen algoritmanın güvenliği, çeşitli deneysel analizler ve 12 adımlı kanıtlanabilir bir güvenlik analizi yol haritası kullanılarak farklı açılardan test edilmiştir. Başarılı analiz sonuçları ve performans ölçümleri, önerilen kriptografik bileşenlerin birçok bilgi güvenliği uygulamasında ve gelecekteki birçok tasarımda kullanılabileceğini göstermektedir.

**Anahtar Kelimeler:** Kriptoloji, Kaos; Görüntü şifreleme; Anahtar üreteci; Rastgele sayı üreteci

# LIST OF FIGURES

Page

# LIST OF TABLES

Page

# ABBREVIATIONS

## Abbreviations

| | |
|---|---|
| NPCR | : The number of changing pixel rate |
| UACI | : The unified averaged changed intensity |
| PUF | : Physical Unclonable Function |
| XOR | : Xclusive OR |
| RNG | : Random Number Generator |
| TRNG | : True Random Number Generator |
| PRNG | : Pseudo Random Number Generator |
| DE | : Differential Evolution (DE) algorithm |
| PSO | : Particle Swarm Optimization algorithm |
| SOS | : Symbiosis Organisms Search (SOS) algorithm |
| GSA | : Gravitational Search Algorithm |
| HSA | : Harmony Search Algorithm |
| TRNG | : Golden Sine Algorithm II |
| API | : Application Programming Interface |
| NIST | : National Institute of Standards and Technology |

# 1. INTRODUCTION

Developments in digital transformation have significantly changed our lives [1]. The effect of this change continues to increase exponentially. This effect has changed and continues to change many processes [2]. Even wars are now associated with cyberattacks on critical infrastructures [3]. Thus, more than ever, information security concepts have gained importance. Therefore, how to ensure the security of the huge information set called big data is now a serious problem for everyone [4]. Strong cryptographic algorithms are needed to address this problem [5, 6]. However, cryptology is a difficult discipline. It is not sufficient to simply demonstrate that certain security requirements are met. As new attacks are developed, new cryptographic algorithms and countermeasures should be constantly investigated [7]. One of the outstanding topics among these researches involves design studies based on nonlinear dynamics [8–12]. The number of studies on this subject in recent years is in the thousands [13]. Although this quantitative size is an indication of how hot the subject is, the security problems of these studies and the difficulties that may occur in practical applications reveal another aspect of the subject that should be addressed. The original aspect of this proposal is the development of a cryptographic key generator module and practical applications that can address security concerns in digital channels within the framework of provable security principles.

## 1.1. Related Works

The existence of chaos-based random number generators (CBRNGs) is known in the literature. In this section, some basic studies published in the last 3 years are discussed, and the general features of the CBRNG literature are discussed. The prominent feature of RNG proposed by Datcu et al. [14] is the shaping of the entropy source with chaotic systems. Hua et al. [15] implemented a new model and hardware realization in order to use the effect of chaotic systems on the quality of the entropy source more effectively. Yang and Chien [16] examined the success of the hardware realization of chaotic systems for the four-dimensional chaotic system and combined the obtained outputs with AES in an image encryption algorithm. Natiq et al. [17] proposed a random number generator based on the chaotic behavior of the plasma model. Özkaynak [18] has shown that, by using the fractional order model of the chaotic Chen system, the randomness requirements can be improved, and this can be a positive effect for cryptographic purposes. Li et al. [19] showed that the randomness requirements can be improved with white chaos and deep learning. Moysis et al. [20] aimed to improve the randomness properties by using a new two-parameter model for the logistics map. Stoller and Campbell [21] aimed to create a memristor-based entropy source for a more effective randomness. Demidova et al. [22] aimed to improve the

randomness characteristics by using optimization algorithms. Chai et al. [23] proposed an image encoding system using automata and a chaos-based system. Tsafack et al. [24] proposed a design using a 4D chaotic circuit in the design of the image encryption algorithm. Ramasamy et al. [25] aimed to ensure the security of images on the basis of a system designed using a logistic and tent map.

Another successful study field that can be considered as a practical application of CBRNG is chaos-based image encryption algorithms. A general projection for all chaos-based image encryption algorithms is tried to be presented. This projection is given in Figure 1.1.

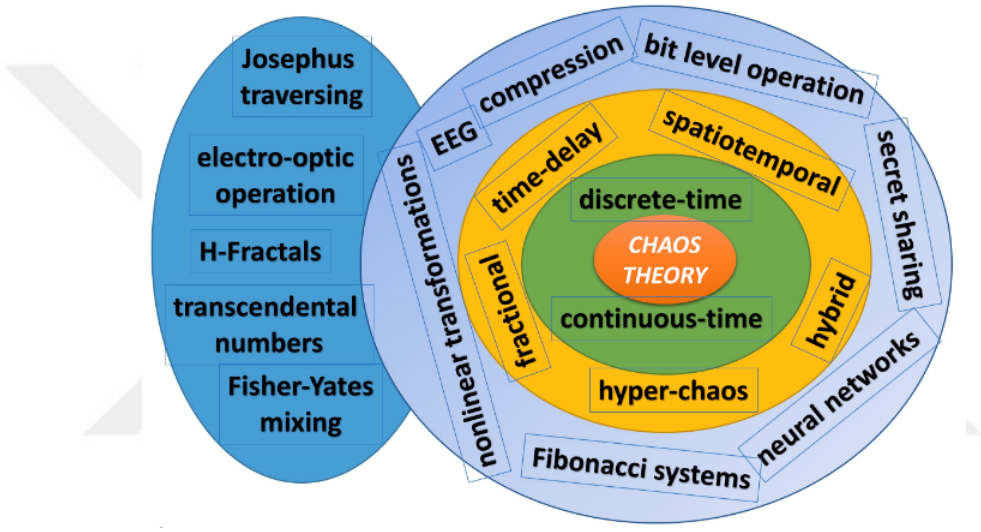


**Figure 1.1.** A general projection for chaos based image encryption algorithms

As can be seen from the Figure 1.1, chaotic systems are at the center of image encryption algorithms. In the literature, the effect of the chaotic system on the success of the encryption algorithm has been investigated by using different types of chaotic systems. Different designs are aimed with different chaotic systems such as hyper, fractional, time delay and spatiotemporal. The general view is that a stronger entropy source can be created with the increasing complexity of the chaotic system [1]. However, a recently published study showed that the transformation algorithm used in the cryptographic design process is more important than chaotic behavior. Therefore, DNA encoding, additional conversion algorithms and quantum structures have been used in the design process of image encryption algorithms.

If a more detailed examination of these design studies is made, it is aimed to improve the success of the encryption algorithm by using various additional algorithms. Wang et al [2] designed an algorithm using Josephus Traversing. Xingyuan et al [3] used dynamic coupling coefficient for the logistic map used in the image encryption algorithm. The different aspect of Diab's work [4] is the permutation and diffusion blocks used in encryption architecture. The prominent point in Zhu et al [5] study attracts attention as compression. In the encryption algorithm proposed by Ping et al [19], permutation and diffusion operations are performed at digit level. Transcendental numbers are used together with chaotic systems in the García et al [6] algorithm. In Ge et al [7] image encryption algorithm, the operations are performed at the bit level. Aslam et al [8] study aimed to increase the success of the image encryption algorithm by increasing the degree of the chaotic system. Sharafi et al [9], on the other hand, proposed an image encryption algorithm to minimize power consumption, which is a remarkable problem today. Hilbert Curves and H-Fractals have been used in the design process of the Zhang et al [10] algorithm. Wang et al [11] utilized the dynamic diffusion process to make the algorithm more secure. In another study, it was aimed to improve the confusion feature of the algorithm by using a five-dimensional system [12]. The difference of Ma et al [13] studies from other studies is that chaotic systems are used in the production of a random sequence. They used a hybrid electro-optic structure in Shao et al [14] encryption algorithm. Multiple secret sharing method has been developed by using Guo et al [15] chaotic image encryption algorithm. Yang et al [16] proposed an image encryption algorithm using fractional-order systems. Zhu et al [17] used two different chaotic systems in their hybrid way. Zhu et al [18] designed an image encryption algorithm using quadratic polynomial maps. In Song et al [19] encryption architecture, they developed an image encryption algorithm using a different structure in the key design protocol. The unique aspect of Thoms et al [20] image encryption algorithm is that it improves the key design process by taking advantage of neural networks structure. In the study of Hua et al [21], Josephus problem has been used. Huang [22] has developed a design that uses two-dimensional maps in his algorithm. Guo et al [23] proposed an image encryption algorithm that uses the logistic and fibonacci systems together. In the Hu et al [24] image encryption algorithm, chaos and matrix transformations are used together. If these studies are summarized in a sentence, the common point is that the strong randomness properties of chaotic systems are improved by various processes, and the confusion and diffusion features are shown to be met for cryptographic purposes.

## 1.2. Definition of Problem and Our Contribution

***Definition of Problem:*** Security analysis of image encryption algorithms based on chaos theory should be focused on the methods presented with mathematical proofs. A recently proposed

algorithm has shown that this requirement can be met by using the robust primitives of modern cryptology. In the proposed algorithm the powerful components such as DES, AES and SHA3, which are considered secure in modern cryptology have been used and these primitives are combined with the advantages of the nonlinear nature of chaotic systems. New encryption systems with similar design logic are required to develop secure applications for information privacy. Thanks to applications that support the Internet of Things and 5G infrastructure, more image data is processed in unsafe environments. The security of these data is an imperative, especially in the context of the security of medical personal data. It is thought that new algorithms whose security has been proven with mathematics proof techniques will become increasingly important to meet these requirements.

***Purpose of Thesis:*** The aim of the thesis is to design an image encryption algorithm whose security has been proven with mathematical proof techniques. In conjunction with security requirements, criteria such as NPCR and UACI statistics metrics, a user-friendly interface and encryption / decryption time will be other design parameters to be used in the development process. The practical application of the image encryption algorithm to be developed as a result of the thesis will be shown on the security of the medical data. It is thought that this practical application may have a widespread effect within the scope of the law on protection of personal data.

The common point of all these studies is the use of chaotic systems as an entropy source in the center of the design. It can be observed that the joint effort of researchers has been to search for new alternatives to improve the statistical randomness characteristics of the entropy source. The most important innovation that distinguishes this proposal from similar ones is that the most appropriate entropy source is obtained in terms of cryptographical requirements with the help of optimization algorithms. Providing the requirements for randomness in the most appropriate way is an important challenge. The idea to consider this problem as an optimization problem was proposed by Tanyıldızı and Özkaynak. In [26], the initial conditions and control parameters describing all statistical tests for four different chaotic systems were determined using different heuristic optimization algorithms. A similar study was conducted by Jiang et al. [27] for chaotic systems. Açıkkapı and Özkaynak [28] showed how different initial conditions can be determined by presenting an approach with a simpler structure compared to the optimization algorithms. Using the approaches suggested in these studies, an ideal entropy pool was formed by obtaining many different initial conditions. Experimental studies were carried out using the initial conditions published in previous studies. Other initial conditions that can be used to feed the entropy pool are not shared, because they are covered by the patent application and there are a large number of them. References [26,28] can be examined in detail for alternative initial conditions for use in practical

applications. The corresponding author can be contacted for initial conditions that can be selected for commercial or more professional needs.

It is an undeniable fact that both hardware and software generators designed using entropy resources based on chaotic systems have many advantages. Following the generation of the ideal entropy source, the strong building blocks of modern cryptology can be combined with the unique features of chaos theory, and the architecture to be designed can address security concerns with a provable security approach. The goal of our study was to most suitably improve the entropy source rather than show the shortcomings of CBRNGs, whose general properties were listed in Section 1.1. This output was merely the result of the study. Our main goal was to use this successful output in an effective image encryption algorithm, because even the most successful cryptographic components can be easily broken if used in a bad scenario. Since an attacker will always target the weakest point of the system, combining strong cryptographic components in a way that allows no openness is a difficult task. The architecture proposed in this study aimed to address this purpose. Transforming all these outputs into a practical application can provide an opportunity to evaluate the success of the outputs from a different perspective. An image encryption algorithm as a practical application was designed. This image encryption algorithm was designed to meet the requirements such as security level, speed, effective solution proposal for resource constrained platforms, and easy usability, representing further original contributions of the proposal.

The thesis study is organized as follows: in Section 2, a detailed expression of the problem is given by presenting an analysis of the current literature. This section also emphasizes the original contributions of the proposed approach to address these problems. The details of the proposed architecture are explained in Section 3. In Section 4, analysis and test results are given. In the last section, the results are discussed and suggestions are made for future studies.

# 2. STATEMENT OF PROBLEM

The basic components expressing the scope of the proposal are shown in Figure 2.1. For these three main components related to the proposal, the current problems in the literature, how these problems are addressed with the approach suggested in the proposal, and the original contributions of the proposal are detailed in this section.

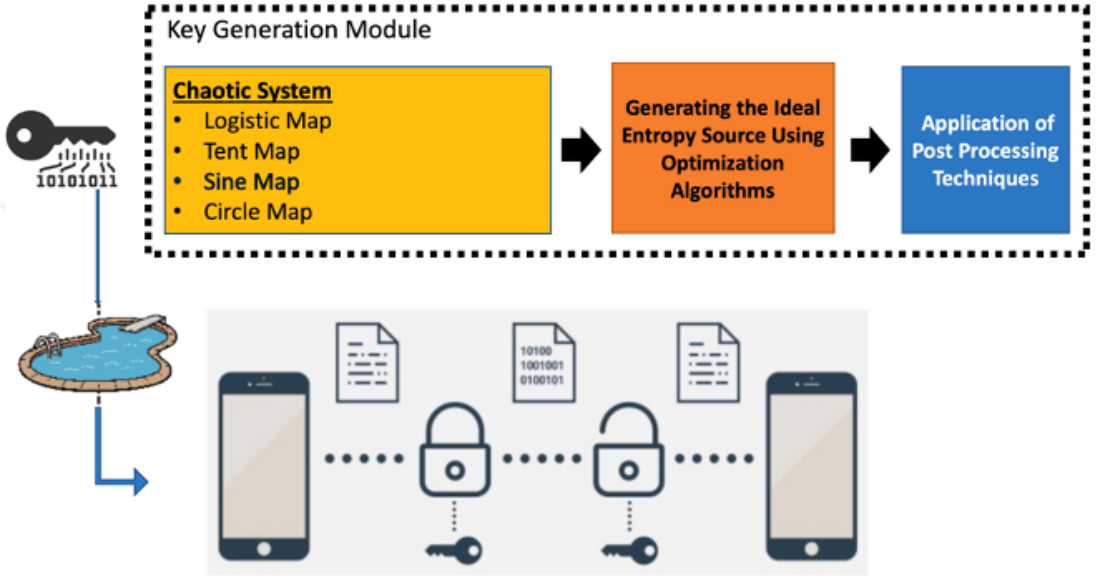


**Figure 2.1.** The basic components expressing the scope of the proposal.

## 2.1. Chaos Theory

The first topic of the proposal is related to chaos theory. The general properties of chaotic systems are visualized in Figure 2.2.

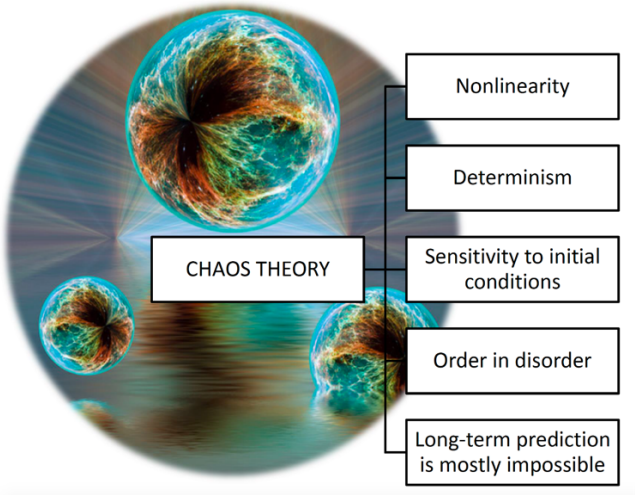


**Figure 2.2.** The key features of chaotic systems.

Chaos theory, whose five key features are illustrated in Figure 2.2, has many successful applications. some of the prominent application areas are shown in Figure 2.3.

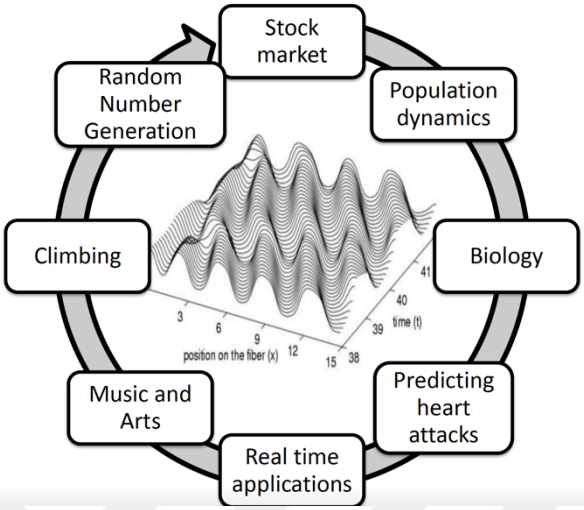


**Figure 2.3.** The prominent application areas of chaotic systems.

The basic element used to meet the cryptographic requirements in the proposed architecture constitutes chaotic systems. Chaotic systems are used in order to provide the need for confusion (mixing). The proposed architecture was developed with the assumption that the unpredictable nature of chaotic systems could be a very powerful element for shaping an ideal entropy source [29, 30]. The general structure of practical cryptology applications based on chaotic systems as entropy sources in the literature is shown in Figure 2.4.

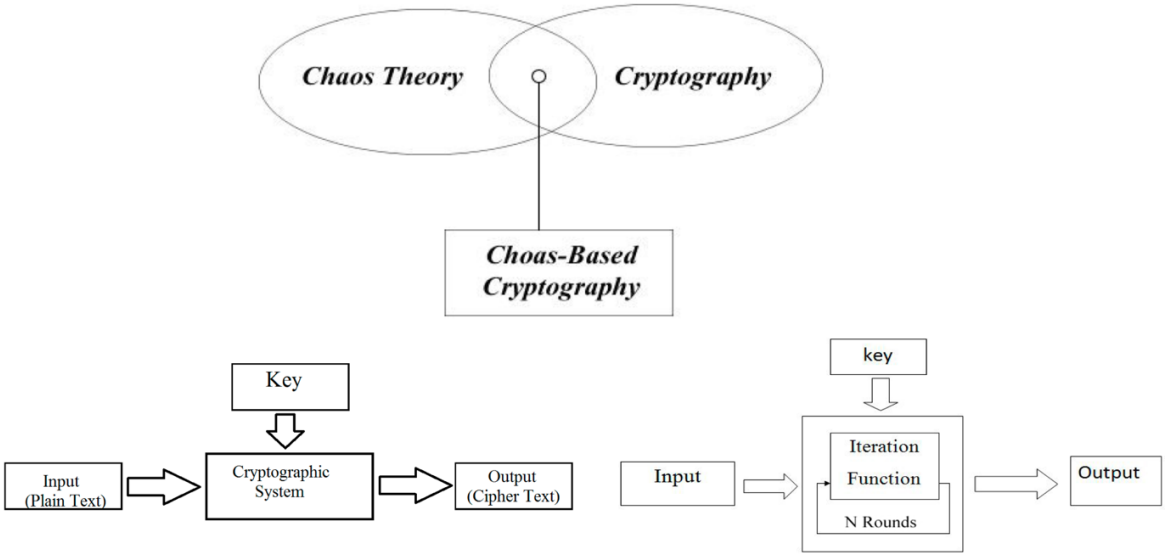


**Figure 2.4.** The general structure of practical cryptology applications based on chaotic systems.

In the study, the ideal entropy source for four different discrete-time chaotic systems was obtained with the help of six different heuristic optimization algorithms. The general structure of the approach used to obtain substitution box structures in the previous study is presented in Figure 2.5 and Figure 2.6. In this study, based on the outputs presented in the previous study, a robust entropy source was created and used as a random number generator.

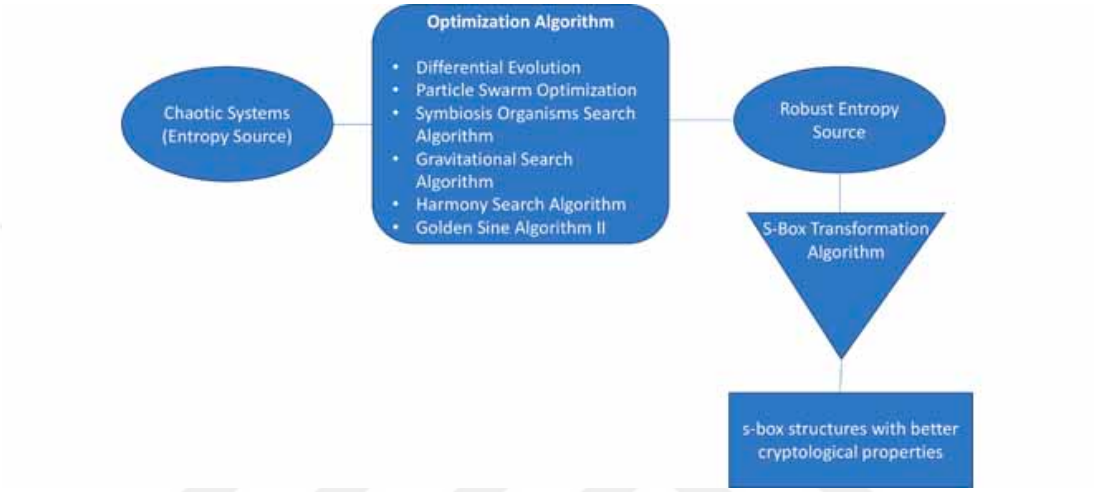


**Figure 2.5.** The approach of determining the most suitable initial conditions for chaotic systems with optimization algorithms.

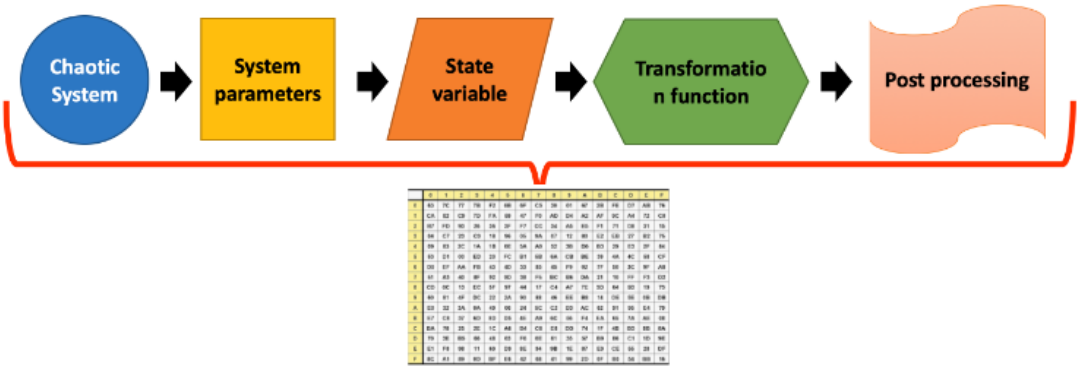


**Figure 2.6.** The general flow for chaos-based cryptography studies.

In a system, the necessary conditions for observing complex dynamics defined as strange attractors are as follows:

- The system must contain nonlinear element(s),
- The system must be sensitive to the initial condition.

These conditions are necessary for the existence of chaos in a system. However, this is not enough. If the system is a continuous time system, the system grade must be at least three, because chaos is not observed in nonlinear systems with a system degree of less than three. Such a condition is not required for discrete-time systems. Chaos can be observed even in a first-order system (logistic map). Therefore, discrete-time chaotic systems are preferred in many practical applications of chaos. The most important reason for this type of preference is that discrete-time chaotic systems have a simpler structure compared to continuous-time and hyperchaotic systems [30]. In the preliminary study, four different discrete-time chaotic systems were used due to this simple structure [26].

## 2.2. Key Generation Module

The other topic that constitutes the proposal is related to the postprocessing techniques that can be used for true random number generators (TRNGs) to be used for cryptographical purposes [19, 21, 22]. Because strong key design is a difficult task, demonstrating that cryptographical applications meet the randomness requirements is not an easy process. These requirements can be grouped under two main headings: showing good statistical properties (R1) and unpredictability (R2). In some sources, these requirements are detailed in more detail under four main headings. Essentially, requirements expressed as R3 and R4 are detailed forms of the R2 requirement. The most widely accepted randomness requirements according to Werner Schindler [31] are briefly described below.

- R1: Random numbers should not show any statistical weakness.
- R2: Knowing the subsets of random numbers should not allow the calculation or prediction of predecessor and consecutive random numbers.
- R3: It should not be possible to calculate previous random numbers if the internal state value of RSU is known, even if the internal state value is not known.
- R4: It should not be possible to calculate future random numbers if the internal state value of RSU is known, even if the internal state value is unknown.

According to the level of security that different applications need, the requirements listed above may vary. For example, it is sufficient to meet the R1 requirement for applications such as simulation, modeling, and games of chance, while all requirements must be met in order to guarantee the confidentiality of sensitive information. However, it is not easy to guarantee unpredictability while providing good statistical features. For example, while random number generators such as linear congruential generator, middle square method, and linear feedback shift

register (LFSR) show good statistical properties, the deterministic structures of these generators make them easier to predict. Designs such as radioactive decay, noise in electrical circuits, and chaotic systems do not show good statistical properties, but their predictability is difficult [32]. Developing a design that simultaneously meets all requirements is the main problem facing researchers working in this field.

Various statistical tests are available to check that the R1 requirement is met. These tests are used as the objective function of the optimization algorithm. It is ensured that the resulting entropy source has a uniform distribution and that any attacker will be unable to make a better statistical inference than a blind guess. However, as stated earlier, statistical randomness is only one of four requirements. It alone is not enough. Therefore, it has to be verified that the proposed generator has an unpredictable nature (R2 requirement). The sensitive nature of chaotic systems to the initial conditions and control parameters can guarantee a wide key space. In the process of determining this initial condition and control parameters, the use of physical unclonable functions specific to the device/hardware is another element that meets the R2 requirement of the generator. Although the condition that the previous and subsequent subsequences of random numbers are unpredictable, which are the other two requirements (R3 and R4) that random number generators must meet, is related to the second requirement, it is planned to use hash functions in the proposed architecture to guarantee these requirements. The one-way nature of hash functions mathematically makes invertibility impossible (requirement R3). Again, the additional physical unclonable inputs can provide additional security for the R4 requirement.

The second leg of the proposal is the practical application of the key generator module. The device (mobile phone or computer) provides feeding of an entropy pool by using device-dependent (physically unclonable) parameters. Allowing the entropy pool to be differentiated according to security requirements can provide an important advantage to ensure the security/ease of use balance. The strong cryptographical keys generated can be used in the image encryption algorithm of the proposed architecture. The advantage of the practical application presented herein is the use of the space-filling curve transformation approach to solve the correlation problem specific to digital images.

# 3. PROPOSED IMAGE ENCRYPTION ARCHITECTURE

The proposed architecture consists of five main parts. In this section, the details of these parts are separately given. The general view of the proposed architecture is given in Figure 3.1.

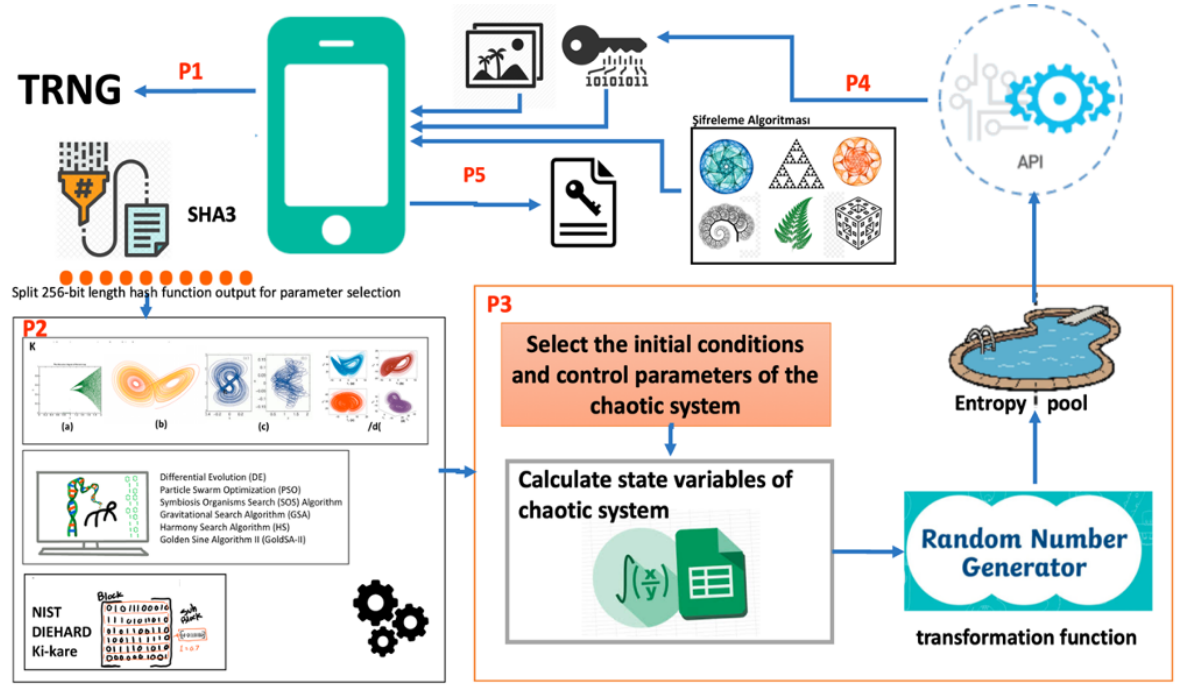


**Figure 3.1.** The general view of the proposed architecture.

## 3.1. Physical Unclonable Function Module

True random number generators (TRNGs) are critical in cryptographic designs to ensure unpredictability. In the proposed architecture, the hardware as an entropy source shown in Figure 3 was chosen as the TRGN structure. There are many advantages to choosing this hardware. Low cost, easy integration into mobile devices via USB port, and meeting statistical randomness requirements are some of these advantages [33]. A mobile device or computer is used to feed this entropy source. Thus, the hardware is used as a physical unclonable function (PUF) in the proposed architecture. The PUF module is very important for the provable security perspective since, according to the cryptanalysis scenario, the user of a system is a potential privileged attacker [34–36]. For example, the user can reverse-engineer the logic of the algorithm by storing the single-use passwords that come to him. PUFs without user control have been used to address this attack scenario and contribute to the unpredictable nature of the generator. In fact, it is known in the literature that there are more effective PUF structures than the hardware in Figure 3.2 and Figure

3.3 [6]. This hardware is used only to explain the design logic through an example. In future studies, different PUF structures will be used.

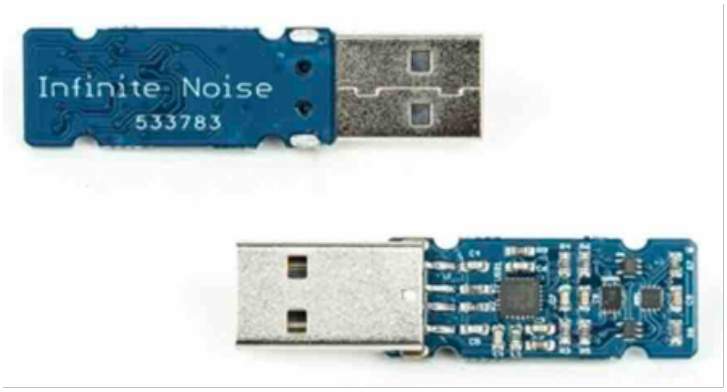


**Figure 3.2.** Crowd Supply Infinite Noise TRNG

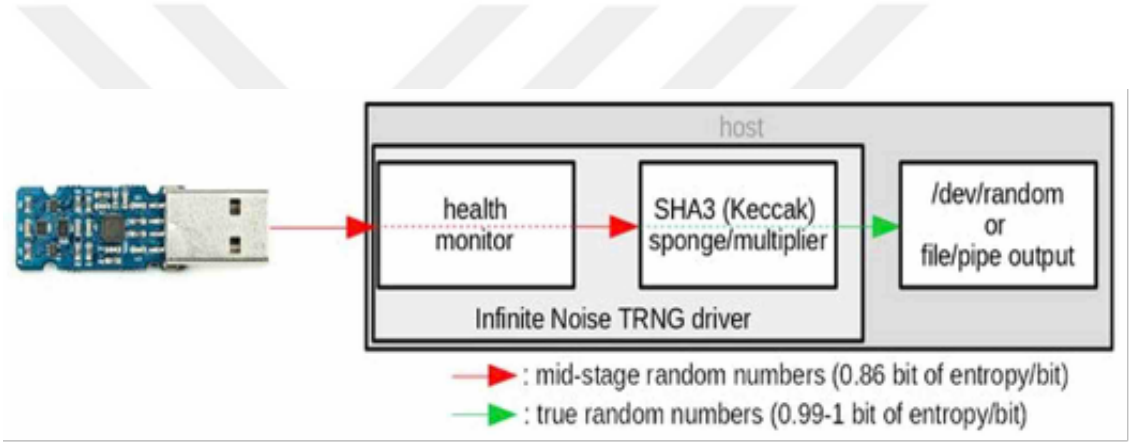


**Figure 3.3.** The working architecture of Crowd Supply Infinite Noise TRNG

Outputs of the PUF hardware are given as input to the cryptographic hash function. Hash functions are used to address cryptanalysis scenarios associated with chosen/known plaintext attacks. In the proposed architecture, it is planned to use the SHA3 algorithm [37]. Such a choice was made because it is the latest hash function standard, with a 256 bit value are the output. It was divided into seven sections with the help of a fragmentation algorithm to be used in parameter selection. It was converted into numerical values using the mod function for each part. These numerical values were used in determining the selection parameters required in other parts of proposed architecture.

## 3.2. Determination of Initial Conditions and Control Parameters of Chaotic Systems Module

Outputs of PUF module of the proposed architecture can be used as selection parameters. By using the determined selection parameters, the chaotic system type, the optimization function to be

used, the statistical test approach to be selected as the objective function, the population size, the number of iterations, and other necessary parameter values for the optimization algorithm are assigned. In the proposed architecture, four different chaotic systems, seven different optimization algorithms, and three different statistical test scenarios can be used. In Table 3.1, the main features of the probable options and their effects on system success are discussed.

**Table 3.1.** Main features of probable options.

| **Option Group** | **Options** |
|---|---|
| Chaotic system type | Discrete-time systems (logistic, tent, sine, circle);<br>continuous-time systems (lorenz, rossler, chua, chen);<br>hyperchaotic (hyper_lorenz, hyper_rossler, hyper_chua, hyper_chen);<br>fractional-order systems |
| Optimization algorithm | Differential Evolution (DE),<br>Particle Swarm Optimization (PSO),<br>Symbiosis Organisms Search (SOS) algorithm,<br>Gravitational Search Algorithm (GSA),<br>Harmony Search Algorithm (HS),<br>Golden Sine Algorithm II (GoldSA-II) |
| Statistical test approach | NIST; AIS; chi-square |

After determining the selection parameters for this module, the initial conditions and control parameters of the chaotic system were determined for the selected statistical test requirements with the help of the optimization algorithm. The probable options listed in Table 3.1 provide ideas for different future studies. The reason for using discrete-time systems in experimental studies is their simple structure. Similarly, there are many different optimization algorithms that can be used in the literature. Different alternatives can be chosen instead of the optimization algorithms listed in Table 1. Reference [26] can be examined for the effect of currently used algorithms on performance, design parameters, and other details.

## 3.3. Random Number Generator Module

Depending on the chaotic system type chosen, the chaotic system can have more than one state variable. In Figure 3.1, this detail is shown using the examples of a (a) discrete-time chaotic system, (b) continuous-time chaotic system, (c) hyperchaotic system, and (d) fractional-order chaotic system in the P2 block. If a generalization is made between chaotic system types, it is observed that the system complexity from (a) to (d) increases. It was analyzed in the literature that this complex structure positively affects the entropy source. In order to benefit from these differences of chaotic system classes in the best way, it is proposed to use three different scenarios at the beginning to determine which state variables are selected. Details of these possible scenarios are discussed in Table 3.2.

**Table 3.2.** Scenarios to be used in the process of choosing state variables.

| Scenarios | Explanation |
|---|---|
| **Option 1** | Let X be the number of state variables of the chaotic system. By applying mode X to the proposed random number generator system outputs, it is decided which state variable is selected by generating a value in the range [0, X]. |
| **Option 2** | Classical rnd() function can be used to decide which state variable is selected by generating a value in the range of [0, X]. |
| **Option 3** | It is decided which state variable is selected by generating value in the range of [0, X] using PUF outputs. |
| **Option 4** | More than one state variable can be selected at the same time. |
| **Option 5** | Direct selection of specific case variables in line with the best practice samples |

State variables of chaotic systems are rationally valuable. Therefore, the selected state variable must be converted to random bit values. Three different scenarios are proposed for this transformation process. Details of the scenarios are discussed in Table 3.3. The scenarios presented in these tables are presented for guidance only. It is planned to achieve a more stable model by analyzing both current and different scenarios in future studies.

**Table 3.3.** State variable/random bit conversion scenarios.

| Scenarios | Explanation |
|---|---|
| **Option 1** | The calculated state variable value of chaotic system is compared with a fixed value. If the state variable value is less than the specified fixed value, a value of 0 is generated; if the state variable is greater than or equal to the specified fixed value, a value of 1 is generated. In this way, state variable values are converted into bit values. |
| **Option 2** | The first three digits after the comma of the calculated state variable value of the chaotic system are selected (can be selected with different values). The selected three-digit values are converted to numerical values between 0 and 255 by applying mod 256. Using the obtained value, an 8 bit length random array of bit values is generated. |

A more detailed representation of the random number generator (RNG) module in P3 is given in Figure 3.4. Actually, Figure 3.4 reflects the general architecture of hybrid RNGs [32].

Initial conditions and control parameters of the chaotic system are used as the seed value. The function f, shown as the state transition function, is related to which of the approaches suggested in Table 3.2 is used in connection with the mathematical model of the chaotic system. The output function represents the transformation function suggested in Table 3.3. The outputs obtained in addition to this function are passed through the cryptographical hash functions and transferred to the entropy pool. Depending on the security requirements of the application, it can

be used for additional inputs when it comes to the security of sensitive data, with the help of these additional inputs to be obtained from PUF modules.

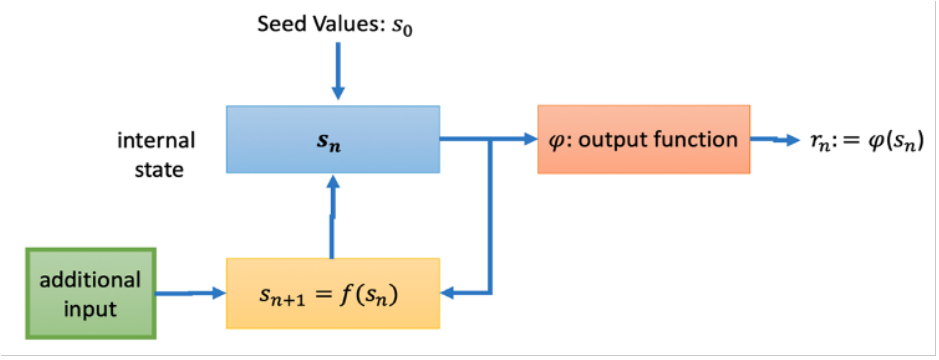


**Figure 3.4.** Detailed representation of the random number generator (RNG) module.

## 3.4. Application Programming Interface

The API (application programming interface) performs the process of generating keys according to user requirements. One of the most important factors for the success of this module is the effective meeting of the security/ease-of-use balance. Selection parameters have an important role among the factors that affect this balance. For example, the chi-square test can be used as an objective function to generate faster key values. This choice indicates that only the chi-square test can be used instead of the NIST test in an optimization process where 15 tests are provided together for applications whose security level is not critical. Similarly, simple mathematical models of discrete-time chaotic systems can be used to quickly achieve the desired goals. On the other hand, when a security-critical image needs to be encrypted, prediction using additional structures can be carried out such as hyperchaotic or fractional-order chaotic systems, using PUF-based additional inputs in the RNG architecture, updating the seed value at regular intervals, state transition functions, and dynamic selection of output functions. The aim is to address security concerns by providing a structure that is more difficult to achieve.

## 3.5. Encryption Module

The image encryption module inputs consist of the key sent by the API module and the original image. It is ensured that both color and gray images are used in the encryption process. To meet this requirement, the selected image is transformed into a one-dimensional array. The value of each cell of the array ranges from 0–255. If the image to be encrypted is a gray-level image, it is in an array of (1 × MN) size, whereas a color image is in an array of (1 × 3MN) size. Here, M represents the number of rows and N represents the number of columns.

One of the most important problems arising in the encryption of digital images is the correlation problem. Therefore, classical encryption algorithms may fail in the encryption process.

One of the most known examples of this is shown in Figure 3.5. Although the problem in Figure 3.5 is related to the processing modes of block ciphers, the fact that the values of neighboring pixels have similar numerical values creates a weakness in terms of cryptanalysis.

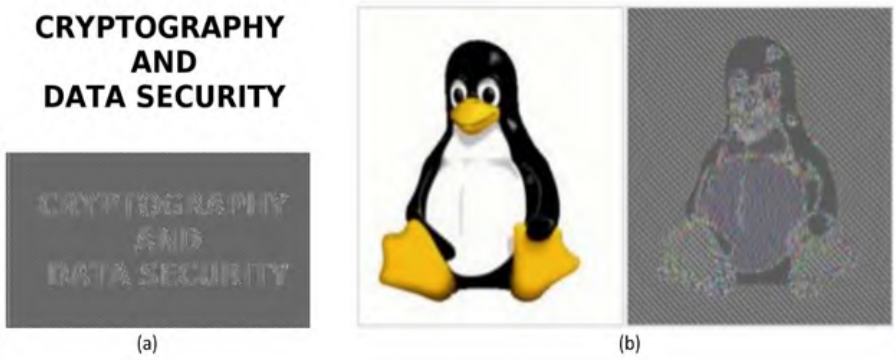


**Figure 3.5.** Correlation problem in the process of encrypting digital images. (a) test image1, (b) test image2

One of the most important original aspects of the proposal is that the space-filling curves approach has been proposed to overcome this correlation problem. The space-filling curve approach uses some patterns when transforming digital images into one-dimensional arrays. Some sample space-filling curves are shown in Figure 3.6 as an example. More effective suggestions have been used in the future studies.

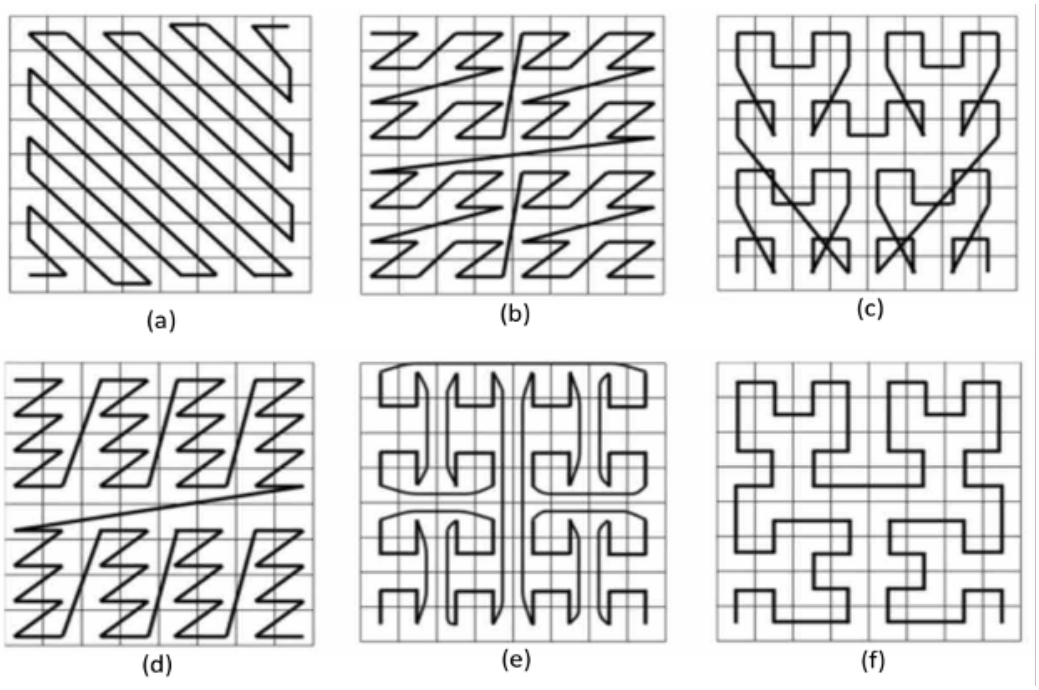


**Figure 3.6.** Six different space-filling curves that can be used in the transformation phase.

# 4. SIMULATION AND ANALYSIS RESULTS

A flowchart is given in Figure 4.1 to better explain the working of the proposed encryption architecture. As stated in the flowchart, the three basic components of the proposed architecture are the PUF, chaotic system, and XOR operator. It is known that there are various suggestions in the literature designed based on these components. For example, various proposals that meet the confusion and diffusion requirements in the encryption process of an image using only chaotic permutations are some of the widely accepted design types [38–43]. Using the DNA encoding and shuffling approach in addition to chaotic permutations is another common type of alternative design [44–48]. Design types based on chaotic permutations are generally included in the classification known as secret key (symmetric) cryptography. Various design suggestions that make use of public key (asymmetric) encryption techniques were presented in some recent studies [49–51]. Similar to the design logic proposed in the study, other design studies have highlighted the key generator [52–54] and used best practices of modern cryptology science [55–57]. Quantum systems [58,59], fractional systems [60–62], and medical encryption algorithms [63–65], which have attracted attention recently, are other current topics related to design proposals.

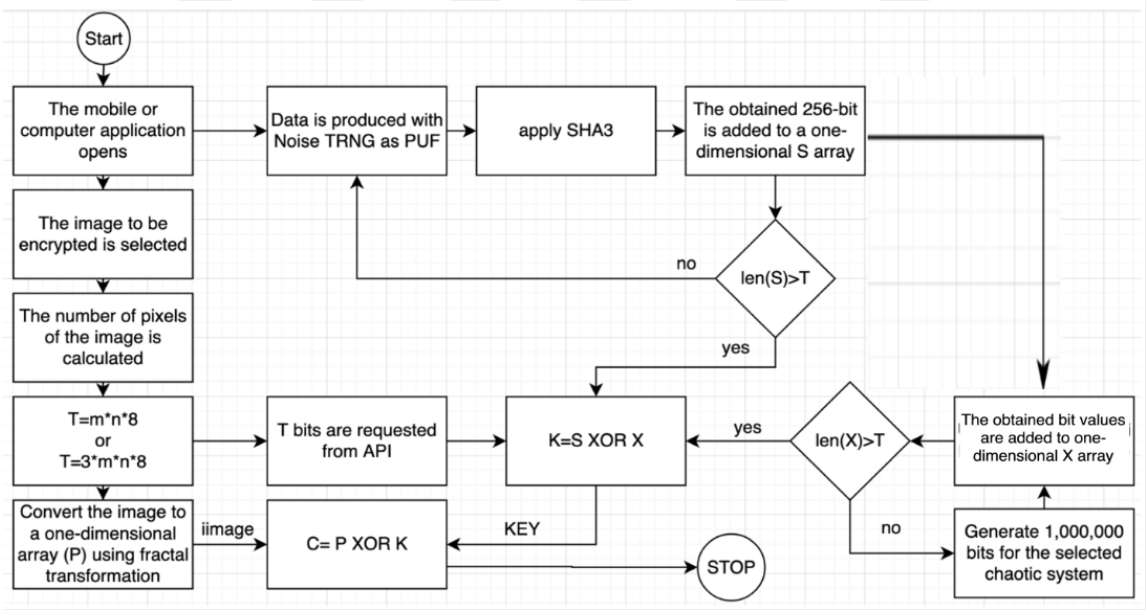


**Figure 4.1.** The basic components expressing the scope of the proposal.

The encrypted images obtained for the sample test images in Figure 4.2 using the proposed algorithm are given in Figure 4.3. One of the most important advantages of the proposed algorithm is that it offers many options. The options listed in Table 4.1 were used in analyzing this section.

**Table 4.1.** State variable/random bit conversion scenarios.

| **Option** | **Value** |
|---|---|
| Chaotic system | Logistic Map |
| Initial value | 0.468326113906509 |
| Control parameter | 4 |
| Optimization algorithm | Golden Sine Algorithm II |
| Statistical test | NIST |
| State variable selection | Logistic map has only one state variable |
| Transformation function | Threshold function (Table 3, option 1, threshold value = 0.5) |
| Space-filling curve pattern | Figure 6a |

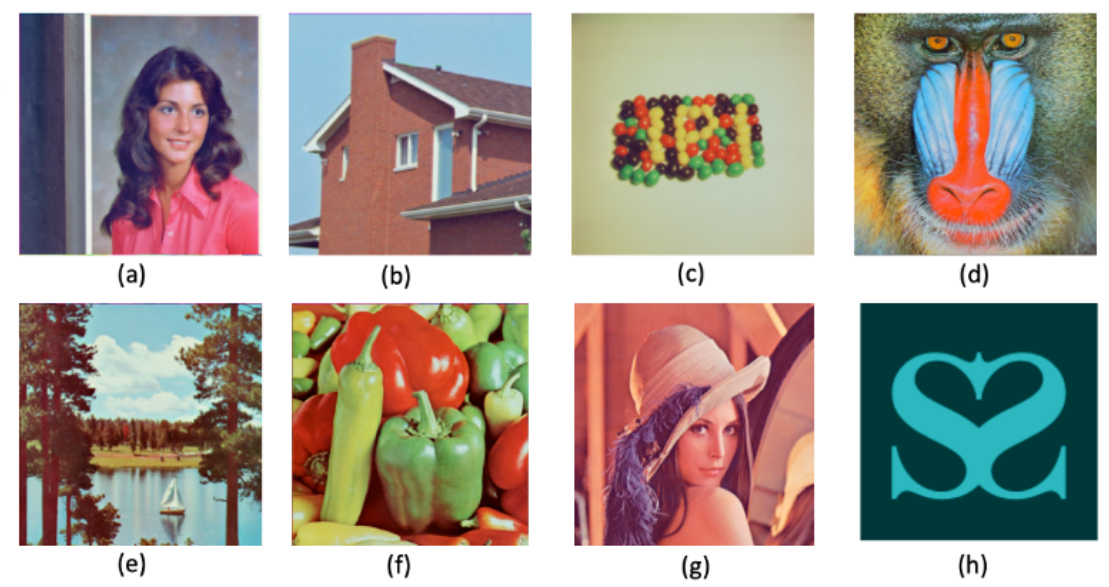


**Figure 4.2.** The eight different sample test images.

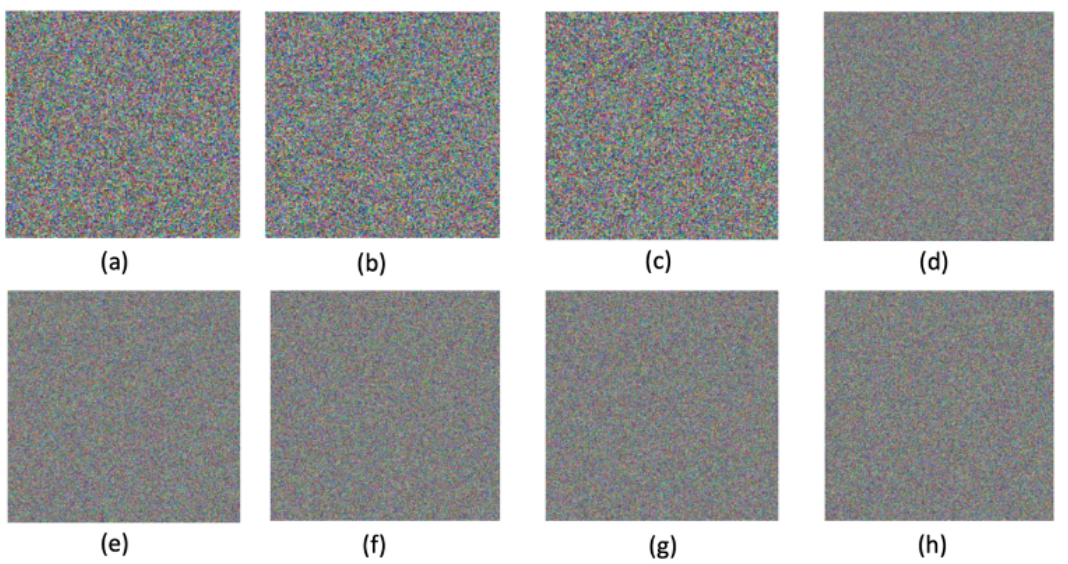


**Figure 4.3.** The encrypted version of each image in Figure 4.2. Each image is given in the same order.

## 4.1. Statistical Analysis Results

One of the analysis tools widely used in the cryptanalysis process of chaos-based encryption algorithms is statistical evaluation. In this section, first of all, various statistical analyses are presented, and the drawbacks of safety evaluations made using only these analyses are discussed. Various statistical tests are given in Figures 4.4 and 4.5. While histogram analysis results are given in Figure 4.4, correlation analysis results are shown in Figure 4.5.

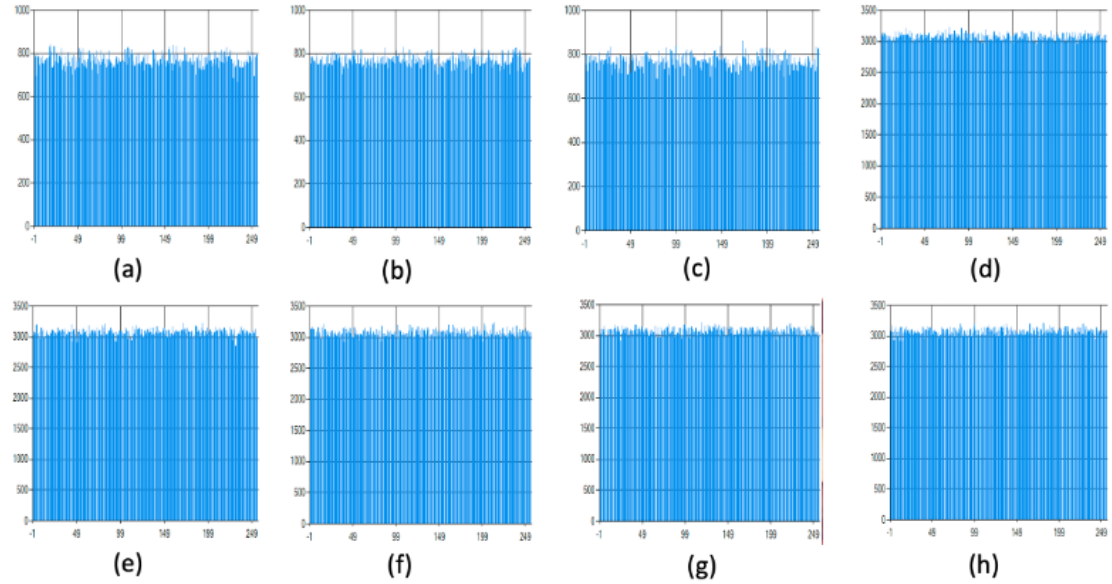


**Figure 4.4.** Histogram analysis for each image in Figure 4.3. Each analysis is given in the order used in Figure 4.3.

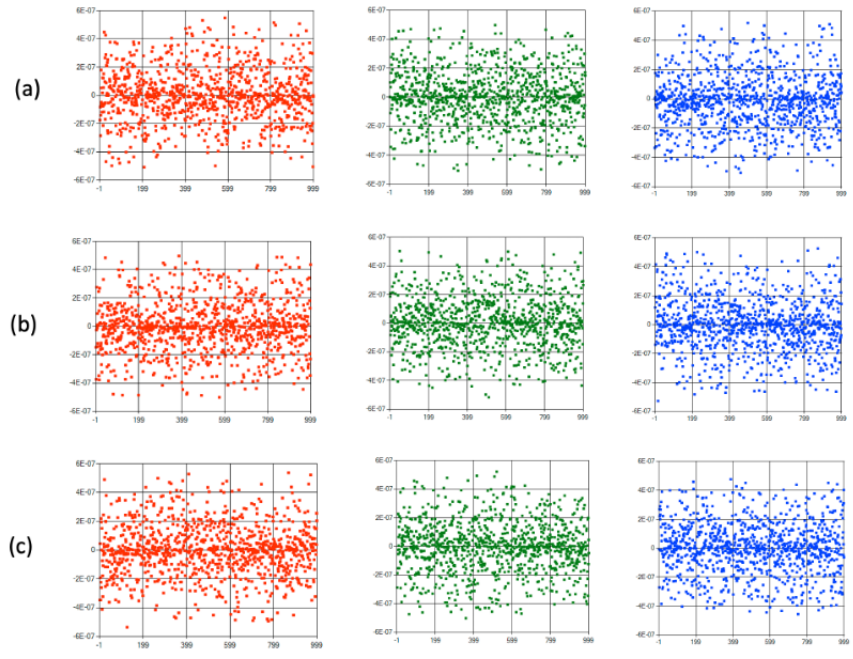


**Figure 4.5.** Horizontal (a), vertical (b), and diagonal (c) axis correlation analysis of RGB components for Figure 4.4a.

It can be observed that the histogram analysis of the original images has a normal distribution, while the encrypted images have a uniform distribution. A similar inference can be made in correlation analysis. In addition to these two measurements, the results of NPCR (number of pixels change rate) and UACI (unified average changing intensity) analysis, which are other supplementary statistical tests, are shown in Table 4.2. Reference [66] can be examined for further details on how the calculations are made for NPCR and UACI tests. A value of 0.99 for the NPCR test and a value of 0.33 for UACI are interpreted as success criteria. In many studies, such results are accepted as an indication that the encryption process does not allow statistical attacks (deductions).

**Table 4.2.** NPCR and UACI test results for images in Figure 4.3.

| **Image** | **(a)** | **(b)** | **(c)** | **(d)** | **(e)** | **(f)** | **(g)** | **(h)** |
|---|---|---|---|---|---|---|---|---|
| **NPCR** | 0.9960 | 0.9957 | 0.9959 | 0.9961 | 0.9960 | 0.9959 | 0.9960 | 0.9959 |
| **UACI** | 0.3349 | 0.3349 | 0.3341 | 0.3346 | 0.3347 | 0.3344 | 0.3351 | 0.3342 |

In fact, this type of analysis is used as security analysis in many studies. For example, it was discussed in detail by Whu et al. [66] that the values accepted as successful test results in the literature for NPCR and UACI tests are actually open to misinterpretation. Therefore, statistical tests are required in the cryptanalysis scenario. However, this is not enough to qualify an encryption algorithm as secure. It has been shown in various studies that many studies based on such a false hypothesis can be easily broken. Since the aim of this study was to address security concerns in the most effective way, it focused on analyzing more comprehensive analysis scenarios rather than giving a more statistical test approach. For the security analysis of the proposed algorithm, the analysis roadmap proposed in [7] was used.

## 4.2. Provable Security Analysis

When designing a cryptographical algorithm in the provable security design approach [67], the boundaries of each component are shown mathematically. The algorithm is considered secure as long as the maximum computational capacity the attacker can reach is lower than the computational capacity required to break the cryptographic component [68]. However, this is not an easy process to demonstrate. In some studies, various analysis roadmaps were designed to overcome this difficulty [69–74]. A sample analysis roadmap was presented in [7]. This analysis roadmap consists of a 12-step attack scenario allowing a comprehensive evaluation of any encryption algorithm. Some steps consist of various subheadings. In this section, each of these steps (analysis questions) is analyzed, and the security level of the proposed encryption algorithm is discussed in detail.

***Step 1:*** The encryption algorithm has to be expressed mathematically and analyzed.

***Analysis Step 1:*** The classification showing the general taxonomy of cryptology science is given in Figure 4.6.

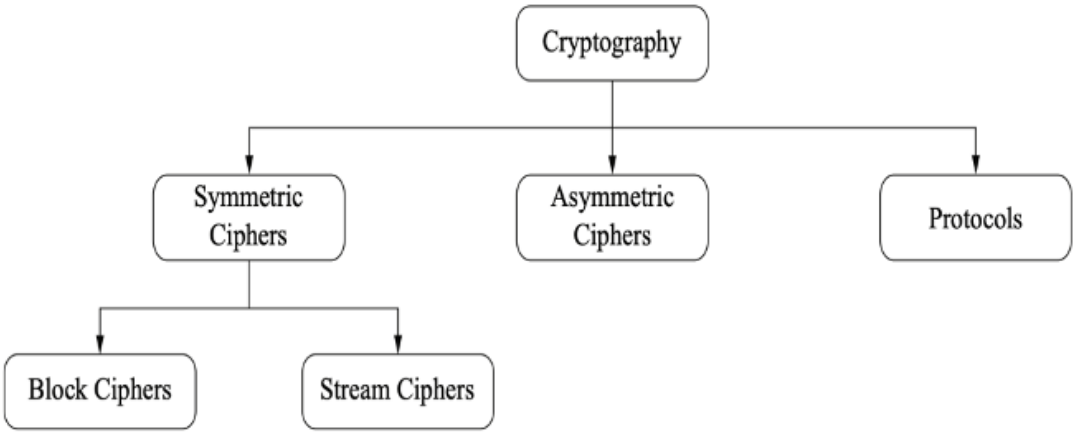


**Figure 4.6.** The general taxonomy of cryptology science.

The proposed encryption algorithm is a stream encryption algorithm. The design architecture is based on the one-time password mechanism proposed by Vernam [75,76]. This architectural ward is known to be safe. It has a very simple mathematical model as expressed in Equation (4.1).

$$C = P \text{ XOR } K. \tag{4.1}$$

This simple structure provides a great advantage in speed. As a result, the security of the algorithm is related to the quality of the keys to be produced. The analysis of the security of the key is discussed in detail in other stages.

***Step 2:*** It is expected that the mathematical expression of the components in the algorithm is given.

***Analysis of Step 2:*** As can be understood from the flowchart given in Figure 4.1, the general structure of the architecture is based on the XOR logic as given in Equation (1). Analysis of all other components is discussed in more detail in the later steps.

***Step 3:*** Mathematical proof of the proposed architecture is required within the framework of the provable security approach.

***Analysis of Step 3:*** A simplified representation of the proposed architecture from a different perspective is shown in Figure 4.7.

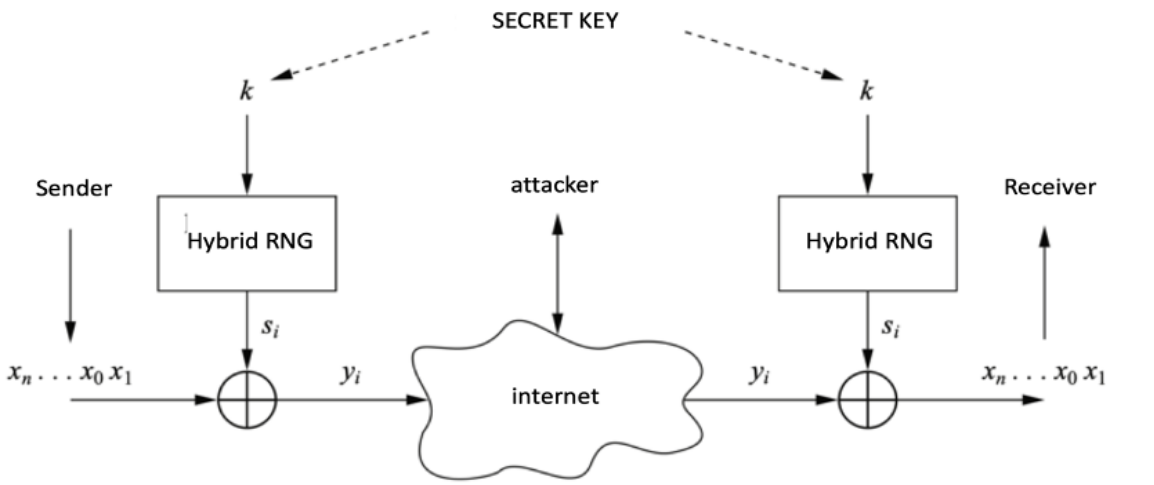


**Figure 4.7.** A simplified representation of the proposed architecture.

The key generator and XOR function draw attention in this architecture. Analyses related to the key generator are given later. The XOR function has a special role in the design of cryptographical algorithms. Because the probability of the output values is 1/2, as can be deduced from the truth table, this process is similar to flipping a coin. Therefore, it is known that the proposed architecture is unconditionally secure, provided that a different key is used in each encryption process.

***Step 4:*** In order to test whether it is compatible with the given mathematical expression, a flow chart of the proposed architecture should be given.

**Analysis of Step 4:** The flowchart of the algorithm is given in Figure 4.1. The flowchart and the mathematical expression given in Equation (1) are compatible. Any negatives during the analysis process were detected.

***Step 5:*** The proposed architecture is expected to be designed in accordance with Kerckhoffs's principle.

***Analysis of Step 5:*** According to Kerckhoffs's principle, there should not be any hidden parameters other than the secret key in the encryption architecture. Even if the attacker has the maximum computing power and maximum expert knowledge, they should not be able to break the architecture. As listed in Table 4.1, there are many options that can be used when creating the ciphertext to be obtained as a result of the algorithm. This wide range of options allows successfully fulfilling Kerckhoffs's principle as it can guarantee different keys each time.

**Step 6:** Which design approach is used in the proposed architecture (cryptanalysis-driven design or provable security design approach)?

***Analysis of Step 6:*** The provable security design approach was used.

,

***Step 7:*** Which components are used to meet the confusion and diffusion properties?

***Analysis of Step 7:*** The XOR function was used for the confusion properties. In the confusion requirement, the relationship between the key and the ciphertext is desired to be as complex as possible. The ciphertext is obtained as a result of applying the XOR operation to the key and plaintext. Hence, it is theoretically not possible to deduce the relationship between them because the probability of inference is exactly 1/2. Since this is no better than a blind guess, the proposed architecture is unconditionally safe if each key is used only once. Since the generated set of keys has a statistically uniform distribution, the ciphertext also has a uniform distribution after XOR processing. As a result, the diffusion feature is also guaranteed.

***Step 8:*** What is the computational complexity of the proposed algorithm?

***Analysis of Step 8:*** Since the proposed encryption algorithm is classified in the stream cipher category, the most important advantage over other encryption algorithm architectures is that the encryption process can be implemented quickly. This advantage is most clearly observed in complexity analysis. The encryption process of the algorithm is realized by applying two one-dimensional arrays of length T to the XOR operation. Thus, the overall complexity of the algorithm can be expressed as O(T) or O(n) in the commonly known form.

One point to be analyzed at this stage is the computational difficulty required for optimization algorithms and PUF structures in the key generator process of the algorithm. However, an entropy pool is proposed in the chosen design architecture. The ability to feed the entropy pool offline allows this calculative difficulty to be ignored.

***Step 9:*** What is the algorithm's complexity class?

***Analysis of Step 9:*** The complexity class of the algorithm is P. The complexity class of the heuristic optimization algorithm used for the selection of control parameters and the initial conditions of chaotic systems in connection with the previous step is NP.

**Step 10:** Analysis of key generation module.

***Analysis of Step 10:*** Since one of the unique aspects of the study is the key generator module, this analysis step was handled more comprehensively as a separate section.

**Step 11:** The numerical deterioration problem of chaotic systems must be analyzed.

***Analysis of Step 11:*** The problem of numerical deterioration is related to the fact that the chaotic system state variables show a periodic behavior depending on the computational sensitivity of the computer where the encryption algorithm is implemented, and where the structure that is taken as the entropy source can no longer meet the randomness requirements. The initial conditions obtained through optimization algorithms must have a certain sensitivity value. Therefore, the proposed algorithm should have a configuration that can implement only the specified initial conditions. This dependency eliminates the numerical deterioration problem. In addition, since the use of hash functions at various stages of the proposed architecture allows mapping the output to a fixed length regardless of the input data, an additional measure is taken to address the problem of numerical deterioration. These choices indicate that possible attacks that can be associated with numerical deterioration are addressed.

***Step 12:*** The effects of implementation attacks should be analyzed.
***Analysis of Step 12:*** It was examined in previous studies that chaos-based designs can provide an advantage over algebraic techniques. It was evaluated that the presence of chaotic structures in the proposed architecture may provide an advantage against side-channel attacks.

## 4.3. Analysis of Key Generation

Random number generators (RNGs) have application areas not only in cryptology but also in games, modeling, and simulations. Each application area has its own specific requirements. There is a general classification for random numbers associated with these requirements. This classification is shown in Figure 4.8.

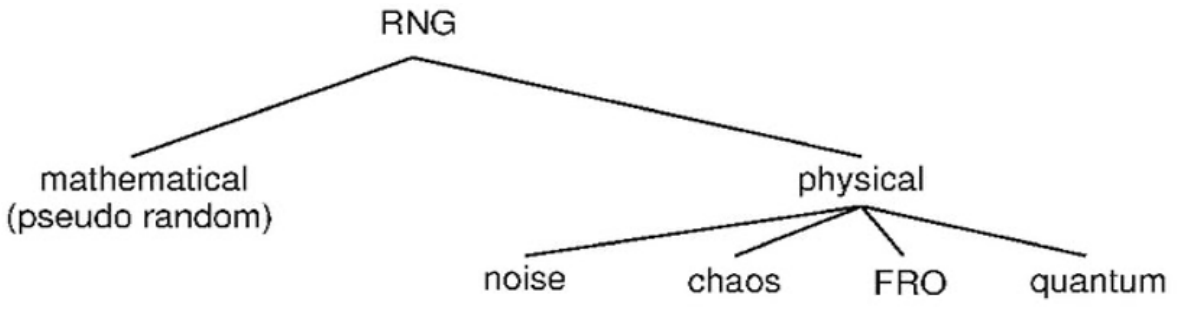


**Figure 4.8.** A classification for random number generators [77].

The class known as DRNGs (mathematical/pseudo random) generates random numbers with the help of an algorithm. Good statistical properties and speed are the most important advantages of this class of generators. However, the predictability of these generators is an important problem. The TRNG (physical) class, which is an alternative to DRNG structures, has an advantage of low

(may impossible) predictability; however, high cost and bad statistical properties are serious problems for researchers and designers.

The keys to be used in the process of encrypting sensitive information are required to have both good statistical properties and an unpredictable structure. Therefore, a hybrid generator architecture is proposed in this study. The unpredictable requirements of the proposed generator architecture are met by chaotic systems and PUF structures. In order to improve the statistical properties, the initial conditions and control parameters of chaotic systems were improved with optimization algorithms, while hash functions were applied to PUF outputs. The most widely accepted NIST randomness tests [78] were applied to analyze the success of the proposed approach. Here, 100,000,000 bit was generated as the PUF output. This output was divided into 100 pieces with a length of 1,000,000, because 1,000,000 bits are required to run NIST tests. A total of 84 of these 100 tests were successfully achieved. The remaining 16 pieces passed 14 tests and failed only one test. The analysis results of five randomly selected tests are given in Table 4.3. A comparison of the real random number generator used as the PUF structure with other TRNG structures is given in Table 4.4. The distribution of random values obtained after the seed values produced for the PUF hardware used in this study were processed through certain complex processes is given in Figure 4.9. The manufacturer's web page states that "the driver allows application of a multiplier, which defines how many bits will be put out of the hashing function for each incoming bit of entropy. This enables generating over 50 megabytes of pure random numbers without measurable degradation of entropy." Reference [33] can be examined for more details.

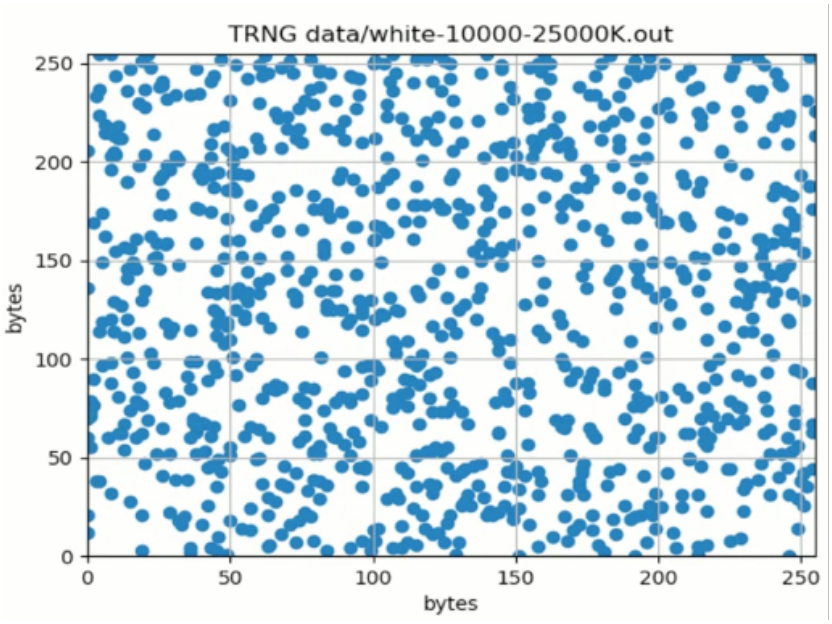


**Figure 4.9.** Distribution of random values after applying various postprocessing techniques to Crowd Supply Infinite Noise TRNG core values.

**Table 4.3.** NIST test results for PUF outputs.

| NIST Test Name | Sample Sequence 1 | Sample Sequence 2 | Sample Sequence 3 |
|---|---|---|---|
| Monobit test | P = 0.79641 | P = 0.94579 | P = 0.68034 |
| Frequency within block test | P = 0.7009 | P = 0.63344 | P = 0.79594 |
| Runs test | P = 0.74286 | P = 0.75504 | P = 0.94088 |
| Longest run ones in a block test | P = 0.011128 | P = 0.19989 | P = 0.48956 |
| Binary matrix rank test | P = 1 | P = 1 | P = 1 |
| DFT test | P = 0.80431 | P = 0.17442 | P = 0.08449 |
| Nonoverlapping template matching | P = 0.46496 | P = 0.18217 | P = 0.68789 |
| Overlapping template matching | P = 0.5839 | P = 0.5839 | P = 0.5839 |
| Maurer's universal test | P = 0.56922 | P = 0.56656 | P = 0.57023 |
| Linear complexity test | P = 1 | P = 1 | P = 1 |
| Serial test | P = 0.91661 | P = 0.95029 | P = 0.91625 |
| Approximate entropy test | P = 0.88844 | P = 0.6324 | P = 0.93674 |
| Cumulative sums test | P = 1 | P = 1 | P = 1 |
| Random excursion test | P = 0.83024 | P = 0.46499 | P = 0.97178 |
| Random excursion variant test | P = 0.45337 | P = 0.90175 | P = 0.51685 |

**Table 4.4.** Comparisons for TRNG Structures.

| Criteria/Generator | OneRNG | ChaosKey | Linux CSPRNG | Used PUF (Infinite Noise TRNG) |
|---|---|---|---|---|
| Open hardware | Yes | Yes | N/A | Yes |
| Open software | Yes | Yes | Yes | Yes |
| Operating principle | RF & Avalanche noise | Reverse biased p-n junction | User-input and timing | Modular entropy multiplication |
| Live health monitor | No | No | No | Yes |
| Requires firmware | Yes | Yes | N/A | No |
| Output rate | 350 kbit/s | 10 Mbit/s | Only very few bit/s | >300 kbit/s |
| Pocket-friendly | Yes | Yes | No | Yes |
| Price | 40 USD | 40 USD | free | 35 USD |

Chaotic systems constitute the other leg of the hybrid generator. The pseudo code of the chaotic generator is given in Table 4.5. Optimization algorithms were used to determine the initial conditions of the chaotic system. Statistical properties were guaranteed, as the objective function of the optimization algorithm was chosen as NIST tests. NIST tests for the 1,000,000 bit value generated for the 0.187791210204038, 0.468326113906509, and 0.766654720925613 initial values of the logistic map are given in Table 4.6. Four control parameters of logistic maps were chosen. Since a hash function is applied to the output of the generated values, a countermeasure

was established against numerical deterioration and/or known/chosen plaintext attacks. Obtaining the key as a result of applying XOR to the outputs produced from chaotic systems and PUF structures is considered as the last step positively affecting security. References [26, 28] can be examined for more details.

**Table 4.5.** Pseudo code for chaotic bit generator for logistic map.

```
Input: Value, ControlParam
Output: sequence
1.  begin
2.      sequence [1:1000000]
3.      for i = 1 to 1000000
4.      begin
5.          xValue = ControlParam * xValue * (1 − xValue)
6.          if(xValue < 0.5)
7.              sequence[i] = 0
8.          else
9.              sequence[i] = 1
10.         end if
11.     end for
12. return sequence
13. end
```

**Table 4.6.** NIST test results for outputs of chaotic systems.

| **NIST Test Name** | **Chaotic Sequence 1** | **Chaotic Sequence 2** | **Chaotic Sequence 3** |
|---|---|---|---|
| Monobit test | P = 0.1197 | P = 0.2644 | P = 0.0536 |
| Frequency within block test | P = 0.5171 | P = 0.6282 | P = 0.1408 |
| Runs test | P = 0.4205 | P = 0.7090 | P = 0.4828 |
| Longest run ones in a block test | P = 0.5725 | P = 0.9077 | P = 0.5391 |
| Binary matrix rank test | P = 0.7053 | P = 0.9603 | P = 0.1408 |
| DFT test | P = 0.3985 | P = 0.0862 | P = 0.0986 |
| Nonoverlapping template matching | P = 0.7900 | P = 0.1831 | P = 0.5539 |
| Overlapping template matching | P = 0.2946 | P = 0.8186 | P = 0.2737 |
| Maurer's universal test | P = 0.8511 | P = 0.3253 | P = 0.0455 |
| Linear complexity test | P = 0.8635 | P = 0.0251 | P = 0.4263 |
| Serial test | P = 0.6410 | P = 0.0747 | P = 0.3272 |
| Approximate entropy test | P = 0.4704 | P = 0.4867 | P = 0.6237 |
| Cumulative sums test | P = 0.1537 | P = 0.3002 | P = 0.0535 |
| Random excursion test | P = 0.6779 | P = 0.7999 | P = 0.6208 |
| Random excursion variant test | P = 0.1245 | P = 0.3353 | P = 0.0462 |

# 5. CONCLUSIONS

The aim of this thesis was to realize a new cryptographic key generator algorithm and its practical application. As a practical application, the aim was to develop an image encryption algorithm that can eliminate security concerns. Analysis results showed that all goals were successfully achieved. This shows that the original aspects of the proposed architecture can be considered as cryptographical components in various security applications in the future.

- The proposed key generator module successfully meets all the requirements (R1, R2, R3 and R4) needed for cryptographical applications.
- The developed key generator module has a high bit output rate (1:1).
- It was shown that the most suitable initial conditions and control parameters that meet the statistical randomness requirements for chaotic systems can be determined with the help of optimization algorithms.
- A user-friendly image encryption algorithm was designed.
- It was shown that the correlation problem in digital images can be overcome by using the space-filling curve transformation method.
- The cryptanalysis of the image encryption algorithm was proven using not only statistical measurements, but also a provable security approach. This approach addressed security concerns via proof with mathematical techniques.
- The proposed encryption architecture is based on a key generator fed from two different entropy sources and cryptographic primitives such as the SHA3 mod function and XOR operator, whose security has been proven as a result of long-term cryptanalysis studies. These design choices specifically address critical security threats such as known-plaintext [79] and chosen-ciphertext [13] attacks.

Despite these advantages, it is thought that there are aspects of the proposed approach in future studies that need improvement. These aspects, which can be discussed as the limits of the proposed method, are listed below [80].

- Hardware was used as a PUF structure in the study. The dependency of this hardware can be a problem. This hardware dependency can be reduced by using alternative PUF resources in the future.
- The computing realization of chaotic systems is a critical issue, especially considering the problem of digital deterioration. In order to avoid this problem, the calculation sensitivity

of the machine in the proposed study should be such that it does not cause this problem. This dependency can be considered as a disadvantage.

- Optimization algorithms are used to determine the initial conditions. It has been evaluated that the computational complexity of optimization algorithms can be interpreted as a disadvantage, although the process of determining the initial conditions with optimization algorithms can be operated offline.
- The cryptology science is a challenge between attacker and designer. Technological advances always keep the possibility of attack alive. Although the security of the proposed method has been proven from different angles, there is a need for a continuous cryptanalysis studies against vulnerabilities that may occur in the future.

# REFERENCES


[1] She, R.; Liu, S.; Wan, S.; Xiong, K.; Fan, P. Importance of Small Probability Events in Big Data: Information Measures, Applications, and Challenges. IEEE Access 2019, 7, 100363–100382, doi:10.1109/access.2019.2926518.

[2] Yu, J.-Y.; Lee, E.; Oh, S.-R.; Seo, Y.-D.; Kim, Y.-G. A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security. IEEE Access 2020, 8, 45304–45324, doi:10.1109/access.2020.2977778.

[3] Son, J.; Choi, J.; Yoon, H. New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants. IEEE Access 2019, 7, 78379–78390, doi:10.1109/access.2019.2922335.

[4] Aljohani, M.; Ahmad, I.; Basheri, M.; Alassafi, M.O. Performance Analysis of Cryptographic Pseudorandom Number Generators. IEEE Access 2019, 7, 39794–39805, doi:10.1109/access.2019.2907079.

[5] Ahmad, M.; Al-Solami, E.; Alghamdi, A.M.; Yousaf, M.A. Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures. IEEE Access 2020, 8, 110397–110411, doi:10.1109/access.2020.3001868.

[6] Zahid, A.H.; Al-Solami, E.; Ahmad, M. A Novel Modular Approach Based Substitution-Box Design for Image Encryption. IEEE Access 2020, 8, 150326–150340, doi:10.1109/access.2020.3016401.

[7] Özkaynak, F. Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dyn. 2018, 92, 305–313, doi:10.1007/s11071-018-4056-x.

[8] Zhang, G.; Ding, W.; Li, L. Image Encryption Algorithm Based on Tent Delay-Sine Cascade with Logistic Map. Symmetry 2020, 12, 355, doi:10.3390/sym12030355.

[9] Kang, Y.; Huang, L.; He, Y.; Xiong, X.; Cai, S.; Zhang, H. On a Symmetric Image Encryption Algorithm Based on the Peculiarity of Plaintext DNA Coding. Symmetry 2020, 12, 1393, doi:10.3390/sym12091393.

[10] Thoai, V.P.; Kahkeshi, M.S.; Van Huynh, V.; Ouannas, A.; Pham, V.-T. A Nonlinear Five-Term System: Symmetry, Chaos, and Prediction. Symmetry 2020, 12, 865, doi:10.3390/sym12050865.

[11] Li, Z.; Peng, C.; Tan, W.; Li, L. A Novel Chaos-Based Color Image Encryption Scheme Using Bit-Level Permutation. Symmetry 2020, 12, 1497, doi:10.3390/sym12091497.

[12] Zhang, R.; Yu, L.; Jiang, D.; Ding, W.; Song, J.; He, K.; Ding, Q. A Novel Plaintext-Related Color Image Encryption Scheme Based on Cellular Neural Network and Chen's Chaotic System. Symmetry 2021, 13, 393, doi:10.3390/sym13030393.

[13] Muhammad, Z.M.Z.; Ozkaynak, F. Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique. IEEE Access 2019, 7, 99945–99953, doi:10.1109/access.2019.2930606.

[14] Datcu, O.; Macovei, C.; Hobincu, R. Chaos Based Cryptographic Pseudo-Random Number Generator Template with Dynamic State Change. Appl. Sci. 2020, 10, 451, doi:10.3390/app10020451.

[15] Hua, Z.; Zhou, B.; Zhou, Y. Sine Chaotification Model for Enhancing Chaos and Its Hardware Implementation. IEEE Trans. Ind. Electron. 2019, 66, 1273–1284, doi:10.1109/tie.2018.2833049.

[16] Yang, C.-H.; Chien, Y.-S. FPGA Implementation and Design of a Hybrid Chaos-AES Color Image Encryption Algorithm. Symmetry 2020, 12, 189, doi:10.3390/sym12020189.

[17] Natiq, H.; Ariffin, M.; Asbullah, M.; Mahad, Z.; Najah, M. Enhancing Chaos Complexity of a Plasma Model through Power Input with Desirable Random Features. Entropy 2020, 23, 48, doi:10.3390/e23010048.

[18] Ozkaynak, F. A Novel Random Number Generator Based on Fractional Order Chaotic Chua System. Elektron. Elektrotechnika 2020, 26, 52–57, doi:10.5755/j01.eie.26.1.25310.
[19] Li, C.; Zhang, J.; Sang, L.; Gong, L.; Wang, L.; Wang, A.; Wang, Y. Deep Learning-Based Security Verification for a Random Number Generator Using White Chaos. Entropy 2020, 22, 1134, doi:10.3390/e22101134.
[20] Moysis, L.; Tutueva, A.; Volos, C.; Butusov, D.; Munoz-Pacheco, J.M.; Nistazakis, H. A Two-Parameter Modified Logistic Map and Its Application to Random Bit Generation. Symmetry 2020, 12, 829, doi:10.3390/sym12050829.
[21] Stoller, S.; Campbell, K. Demonstration of Three True Random Number Generator Circuits Using Memristor Created Entropy and Commercial Off-the-Shelf Components. Entropy 2021, 23, 371, doi:10.3390/e23030371.
[22] Demidova, L.A.; Gorchakov, A.V. A Study of Chaotic Maps Producing Symmetric Distributions in the Fish School Search Optimization Algorithm with Exponential Step Decay. Symmetry 2020, 12, 784, doi:10.3390/sym12050784.
[23] Chai, X.; Fu, X.; Gan, Z.; Zhang, Y.; Lu, Y.; Chen, Y. An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. Neural Comput. Appl. 2018, 32, 4961–4988, doi:10.1007/s00521-018-3913-3.
[24] Tsafack, N.; Kengne, J.; Abd-El-Atty, B.; Iliyasu, A.M.; Hirota, K.; El-Latif, A.A.A. Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Inf. Sci. 2020, 515, 191–217, doi:10.1016/j.ins.2019.10.070.
[25] Ramasamy, P.; Ranganathan, V.; Kadry, S.; Damaševičius, R.; Blažauskas, T. An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map. Entropy 2019, 21, 656, doi:10.3390/e21070656.
[26] Tanyildizi, E.; Ozkaynak, F. A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps. IEEE Access 2019, 7, 117829–117838, doi:10.1109/access.2019.2936447.
[27] Jiang, Y.; Lau, F.C.M.; Wang, S.; Tse, C.K. Parameter identification of chaotic systems by a novel dual particle swarm optimization. Int. J. Bifurc. Chaos 2016, 26, 1650024.
[28] Acikkapi, M.S.; Ozkaynak, F. A Method to Determine the Most Suitable Initial Conditions of Chaotic Map in Statistical Randomness Applications. IEEE Access 2021, 9, 1482–1494, doi:10.1109/access.2020.3046470.
[29] Strogatz, S.H. Nonlinear Dynamics and Chaos with Applications to Physics; Taylor & Francis: New York, NY, USA, 2014.
[30] Sprott, J. Elegant Chaos Algebraically Simple Chaotic Flows; World Scientific: Singapore, 2010.
[31] Schindler, W. Random Number Generators for Cryptographic Applications. In Cryptographic Engineering; Metzler, J.B., Ed.; Springer: Berlin/Heidelberg, Germany, 2009.
[32] Özkaynak, F. Cryptographically secure random number generator with chaotic additional input. Nonlinear Dyn. 2014, 78, 2015–2020, doi:10.1007/s11071-014-1591-y.
[33] Crowdsupply. Infinite Noise TRNG. Available online: https://www.crowdsupply.com/13-37/infinite-noise-trng (accessed on 07 May 2021).
[34] Kong, J.; Koushanfar, F. Processor-Based Strong Physical Unclonable Functions with Aging-Based Response Tuning. IEEE Trans. Emerg. Top. Comput. 2013, 2, 16–29, doi:10.1109/tetc.2013.2289385.
[35] Shamsoshoara, A.; Korenda, A.; Afghah, F.; Zeadally, S. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. Comput. Networks 2020, 183, 107593, doi:10.1016/j.comnet.2020.107593.

[36] Guajardo J.; Gu, Q.; Paillier, P.; Lange, T.; Teske, E.; Hankerson, D.; Menezes, A.; Zhang, D.; Yue, F.; Zuo, W.; et al. Physical Unclonable Functions (PUFs). In Encyclopedia of Cryptography and Security; Springer: Boston, MA, USA, 2011; pp. 929–934.

[37] Dworkin, M.J. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. In SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015.

[38] Liu, L.; Lei, Y.; Wang, D. A Fast Chaotic Image Encryption Scheme with Simultaneous Permutation-Diffusion Operation. IEEE Access 2020, 8, 27361–27374, doi:10.1109/access.2020.2971759.

[39] Jolfaei, A.; Wu, X.-W.; Muthukkumarasamy, V. On the Security of Permutation-Only Image Encryption Schemes. IEEE Trans. Inf. Forensics Secur. 2015, 11, 235–246, doi:10.1109/tifs.2015.2489178.

[40] Alshammari, B.M.; Guesmi, R.; Guesmi, T.; AlSaif, H.; AlZamil, A. Implementing a Symmetric Lightweight Cryptosystem in Highly Constrained IoT Devices by Using a Chaotic S-Box. Symmetry 2021, 13, 129, doi:10.3390/sym13010129.

[41] Askar, S.; Al-Khedhairi, A.; Elsonbaty, A.; Elsadany, A. Chaotic Discrete Fractional-Order Food Chain Model and Hybrid Image Encryption Scheme Application. Symmetry 2021, 13, 161, doi:10.3390/sym13020161.

[42] Lin, C.-H.; Hu, G.-H.; Chan, C.-Y.; Yan, J.-J. Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm. Appl. Sci. 2021, 11, 1329, doi:10.3390/app11031329.

[43] Guo, H.; Zhang, X.; Zhao, X.; Yu, H.; Zhang, L. Quadratic Function Chaotic System and its Application on Digital Image Encryption. IEEE Access 2020, 8, 55540–55549.

[44] Elkamchouchi, D.H.; Mohamed, H.G.; Moussa, K.H. A Bijective Image Encryption System Based on Hybrid Chaotic Map Diffusion and DNA Confusion. Entropy 2020, 22, 180, doi:10.3390/e22020180.

[45] Zhang, D.; Chen, L.; Li, T. Hyper-Chaotic Color Image Encryption Based on Transformed Zigzag Diffusion and RNA Operation. Entropy 2021, 23, 361, doi:10.3390/e23030361.

[46] Khan, J.S.; Boulila, W.; Ahmad, J.; Rubaiee, S.; Rehman, A.U.; Alroobaea, R.; Buchanan, W.J. DNA and Plaintext Dependent Chaotic Visual Selective Image Encryption. IEEE Access 2020, 8, 159732–159744, doi:10.1109/access.2020.3020917.

[47] Wan, Y.; Gu, S.; Du, B. A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding. Entropy 2020, 22, 171, doi:10.3390/e22020171.

[48] Iqbal, N.; Hanif, M.; Abbas, S.; Khan, M.A.; Al Motiri, S.H.; Al Ghamdi, M.A. DNA Strands Level Scrambling Based Color Image Encryption Scheme. IEEE Access 2020, 8, 178167–178182, doi:10.1109/access.2020.3025241.

[49] Diaz, E.A.H.; Meana, H.M.P.; Garcia, V.M.S. Encryption of RGB Images by Means of a Novel Cryptosystem using Elliptic Curves and Chaos. IEEE Lat. Am. Trans. 2020, 18, 1407–1415, doi:10.1109/tla.2020.9111676.

[50] Luo, Y.; Ouyang, X.; Liu, J.; Cao, L. An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems. IEEE Access 2019, 7, 38507–38522, doi:10.1109/access.2019.2906052.

[51] Yousif, S.F.; Abboud, A.J.; Radhi, H.Y. Robust Image Encryption with Scanning Technology, the El-Gamal Algorithm and Chaos Theory. IEEE Access 2020, 8, 155184–155209, doi:10.1109/access.2020.3019216.

[52] Song, Y.; Zhu, Z.; Zhang, W.; Yu, H.; Zhao, Y. Efficient and Secure Image Encryption Algorithm Using a Novel Key-Substitution Architecture. IEEE Access 2019, 7, 84386–84400, doi:10.1109/access.2019.2923018.

[53] Li, H.; Deng, L.; Gu, Z. A Robust Image Encryption Algorithm Based on a 32-bit Chaotic System. IEEE Access 2020, 8, 30127–30151, doi:10.1109/access.2020.2972296.

[54] Rehman, A.U.; Firdous, A.; Iqbal, S.; Abbas, Z.; Shahid, M.M.A.; Wang, H.; Ullah, F. A Color Image Encryption Algorithm Based on One Time Key, Chaos Theory, and Concept of Rotor Machine. IEEE Access 2020, 8, 172275–172295, doi:10.1109/access.2020.3024994.

[55] Shah, T.; Haq, T.U.; Farooq, G. Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation. IEEE Access 2020, 8, 52609–52621, doi:10.1109/access.2020.2978083.

[56] Muhammad, Z.M.Z.; Ozkaynak, F. An Image Encryption Algorithm Based on Chaotic Selection of Robust Cryptographic Primitives. IEEE Access 2020, 8, 56581–56589, doi:10.1109/access.2020.2982827.

[57] Boussif, M.; Aloui, N.; Cherif, A. Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher. IET Image Process. 2020, 14, 1209–1216, doi:10.1049/iet-ipr.2019.0042.

[58] Liu, X.; Xiao, D.; Huang, W.; Liu, C. Quantum Block Image Encryption Based on Arnold Transform and Sine Chaotification Model. IEEE Access 2019, 7, 57188–57199, doi:10.1109/access.2019.2914184.

[59] Zhou, S. A Quantum Image Encryption Method Based on DNACNot. IEEE Access 2020, 8, 178336–178344, doi:10.1109/access.2020.3027964.

[60] Faragallah, O.S.; Afifi, A.; El-Shafai, W.; El-Sayed, H.S.; Naeem, E.A.; AlZain, M.A.; Al-Amri, J.F.; Soh, B.; El-Samie, F.E.A. Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications. IEEE Access 2020, 8, 42491–42503, doi:10.1109/access.2020.2974226.

[61] Yang, F.; Mou, J.; Sun, K.; Cao, Y.; Jin, J. Color Image Compression-Encryption Algorithm Based on Fractional-Order Memristor Chaotic Circuit. IEEE Access 2019, 7, 58751–58763, doi:10.1109/access.2019.2914722.

[62] Neto, J.R.D.O.; Lima, J.B.; Panario, D. The Design of a Novel Multiple-Parameter Fractional Number-Theoretic Transform and Its Application to Image Encryption. IEEE Trans. Circuits Syst. Video Technol. 2020, 30, 2489–2502, doi:10.1109/tcsvt.2019.2925522.

[63] Ibrahim, S.; Alhumyani, H.; Masud, M.; Alshamrani, S.S.; Cheikhrouhou, O.; Muhammad, G.; Hossain, M.S.; Abbas, A.M. Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps. IEEE Access 2020, 8, 160433–160449, doi:10.1109/access.2020.3020746.

[64] Li, T.; Du, B.; Liang, X. Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz. IEEE Access 2020, 8, 13792–13805, doi:10.1109/access.2020.2966264.

[65] Ali, T.S.; Ali, R. A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map. IEEE Access 2020, 8, 71974–71992, doi:10.1109/access.2020.2987615.

[66] Wu, Y.; Noonan, J.; Again, S. Npcr and Uaci Randomness Tests for Image Encryption. JSAT 2011, 31–38.

[67] Bellare, M. Practice-Oriented Provable-Security. In Proceedings of the International Workshop on Information Security, Kuala Lumpur, Malaysia, 6–7 November 1999; pp. 1–15.

[68] Goldwasser, S.; Bellare, M. Lecture Notes on Cryptography Summer Course ‘Cryptography and Computer Security’; Massachusetts Institute of Technology: Cambridge, MA, USA, 1999.

[69] Feng, W.; He, Y.-G. Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling. IEEE Photon J. 2018, 10, 1–15, doi:10.1109/jphot.2018.2880590.

[70] Li, C.; Lin, D.; Lu, J. Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits. IEEE MultiMedia 2017, 24, 64–71, doi:10.1109/mmul.2017.3051512.

[71] Ozkaynak, F. Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals. In Proceedings of the 2017 International Conference on Computer Science and Engineering (UBMK), London, UK, 5–7 July 2017.

[72] Feng, W.; He, Y.; Li, H.; Li, C. Cryptanalysis and Improvement of the Image Encryption Scheme Based on 2D Logistic-Adjusted-Sine Map. IEEE Access 2019, 7, 12584–12597, doi:10.1109/access.2019.2893760.

[73] Li, C.; Zhang, Y.; Xie, E.Y. When an attacker meets a cipher-image in 2018: A year in review. J. Inf. Secur. Appl. 2019, 48, doi:10.1016/j.jisa.2019.102361.

[74] Burhan, Y.; Artuger, F.; Ozkaynak, F. A Novel Hybrid Image Encryption Algorithm Based on Data Compression and Chaotic Key Planning Algorithms. In Proceedings of the 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 10–12 June 2019; pp. 1–5.

[75] Wernam, B.; Steven, M. Frank Miller: Inventor of the One-Time Pad. Cryptologia 2021, 35, 203–222.

[76] Paar, C.; Pelzl, J. Understanding Cryptography: A Textbook for Students and Practitioners; Springer: Berlin/Heidelberg, Germany, 2010.

[77] Stipčević, M.; Koç, K. True Random Number Generators. In Open Problems in Mathematics and Computational Science; Metzler, J.B., Ed.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 275–315.

[78] Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications; Defense Technical Information Center: Fort Belvoir, VA, USA, 2010.

[79] Wei, W.; Woźniak, M.; Damaševičius, R.; Fan, X.; Li, Y. Algorithm Research of Known-plaintext Attack on Double Random Phase Mask Based on WSNs. J. Internet Technol. 2019, 20, 39–48.

[80] Muhammad, A. S., Özkaynak, F. SIEA: Secure Image Encryption Algorithm Based on Chaotic Systems Optimization Algorithms and PUFs, Symmetry 2021.

# CURRICULUM VITAE

**Aina'u SHEHU MUHAMMED**

[redacted]

Intelligence.