Synthesis Lectures on
Engineering, Science, and Technology

SYNTHESIS
COLLECTION OF TECHNOLOGY

Rafael Martínez-Guerra
Juan Javier Montesinos-García
Juan Pablo Flores-Flores

Encryption and Decryption Algorithms for Plain Text and Images using Fractional Calculus

Springer

Synthesis Lectures on Engineering, Science, and Technology

The focus of this series is general topics, and applications about, and for, engineers and scientists on a wide array of applications, methods and advances. Most titles cover subjects such as professional development, education, and study skills, as well as basic introductory undergraduate material and other topics appropriate for a broader and less technical audience.

Rafael Martínez-Guerra •
Juan Javier Montesinos-García •
Juan Pablo Flores-Flores

Encryption and Decryption Algorithms for Plain Text and Images using Fractional Calculus

Springer

Rafael Martínez-Guerra
Automatic Control
Center for Research and Advanced Studies of the National Polytechnic Institute (CINVESTAV-IPN)
Mexico City, Mexico

Juan Pablo Flores-Flores
Automatic Control
Center for Research and Advanced Studies of the National Polytechnic Institute (CINVESTAV-IPN)
Mexico City, Mexico

Juan Javier Montesinos-García
Institute of Electronics and Mechatronics
Technological University of the Mixteca
Huajuapan de León, Mexico

ISSN 2690-0300 ISSN 2690-0327 (electronic)
Synthesis Lectures on Engineering, Science, and Technology
ISBN 978-3-031-20697-9 ISBN 978-3-031-20698-6 (eBook)
https://doi.org/10.1007/978-3-031-20698-6

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

In memory of my father,
Carlos Martínez Rosales.
To my wife and sons,
Marilen, Rafael, and Juan Carlos.
To my mother and brothers,
Virginia, Victor, Arturo, Carlos,
Javier, and Marisela.

Rafael Martínez-Guerra

To my mother Irma and my father Javier,
whose love and support allowed me
to reach all my goals.
To my aunt Rosario and Uncle Clemente,
their teachings, love and support were
instrumental in my formation up to today.
To my cousin Oscar, for all these years
of support and assertive counsel.
In loving memory of my grandmother Sofia,
aunt Margarita and cousin Daniel.

Juan Javier Montesinos-García

To my family,
Eladio, Candelaria, Edy, Abril,
Mario, Amaia, Akane and Najmeh.

Juan Pablo Flores-Flores

Preface

Many people know that it is possible to intercept and modify data if an application does not protect it when travels on an untrusted network, and the application then becomes a disaster when it comes to security. In this book, we offer an alternative to encrypt and decrypt messages using objects called integer and fractional-order estimators or observers, by means of security codes. We establish a class of observers capable of carrying out this work, by means of security codes where finally, since an observer is nothing more than a mathematical model represented through nonlinear differential equations that can be of integer or fractional type that serve as means to send messages either of the plain-text type or of the image type whose key or security code to encrypt or decrypt is nothing more than a set of initial conditions where it makes sense to speak of this means of transporting the message either plain-text or image for specific attacks for chaotic cryptosystems of the stream cipher type. In this book, we mention the type of observers to treat either the integer or fractional order type and their main characteristics. We discuss an important property of some systems such as Liouville systems that is very important for the encryption and decryption of messages in integer and fractional order nonlinear systems by using the synchronization property of chaotic systems where we address some logistic maps such as Mandelbrot sets including Julia and fractal sets taking advantage of their characteristics to encrypt or recover messages. We discuss some issues about stream and block ciphers and some state observers. Various types of observers are proposed for nonlinear systems of integer and fractional order from the simplest (Luenberger Observer) to the most sophisticated such as the Supertwisting Observer for message receivers as well as their vulnerability to attacks. Observers of the exponential polynomial type are proposed together with the property of the Liouville type. We also propose the usefulness of robust fractional systems of sliding modes with Liouville characteristics as means of transmission and reception of plain-text and image messages. Of all the alternatives for encryption and decryption of messages shown here, a vulnerability analysis to cryptographic attacks (cryptoanalysis) is made, this is a security analysis, an important topic on the subject of secure communications. The book is self-contained, that is to say, the necessary tools to address the issues such as fractional calculus are given in the same book and several

examples are presented. Moreover, this book includes exercises that are left to the reader. The book is directed to an audience such as professionals in the areas of mathematics, physics and engineering and researchers in general and related areas with a minimum of knowledge in higher mathematics. However, it also contains advanced research topics for people interested in encryption and decryption, observers, synchronization and secure communications areas. The book is organized as follows. In Chap. 1, a brief overview of the main topics covered is presented giving an introduction to the state of the art on encryption and decryption algorithms, synchronization of chaotic systems, security keys or codes, security analysis such as cryptographic attacks, linear and differential cryptanalysis, in addition to specific attacks for chaotic cryptosystems of type stream cipher. In Chap. 2, some definitions are given about the Lyapunov exponents, stability, and state observers; also fractals and synchronization are briefly introduced. Chapter 3 shows the stream and block ciphers and observers, binary representations as well as some conversions from binary to decimal and vice versa, representations of plain text and images in integer bits and ciphers with generalized synchronization. Chapter 4 deals with the study of Liouville systems and cryptography, and a supertwisting observer is addressed as a receiver as well as its vulnerability to cryptanalysis. Chapter 5 presents some basic concepts of state observers, the exponential polynomial observer is used as a receptor, and the receptors are based on properties related to Liouville systems. Chapter 6 shows some basic elements of fractional calculus and some observers. Chapter 7 deals with the implementation of systems with the property of Liouville and fractional order systems used for the encryption and decryption of plain-text and image messages. In Chap. 8, we present robust fractional order state observers as means of encryption and decryption, presenting a security analysis and situations that lead to decryption failures. Finally, in Chap. 9, a new topic is described in secure communications, and we present encryption and decryption algorithms by using state observers that are represented by means of fractional-order chaotic systems with the Atangana-Baleunu fractional derivative. Additionally, the reader will find throughout this material some exercises to strengthen the knowledge acquired.

Mexico City, Mexico

Rafael Martínez-Guerra
Juan Javier Montesinos-García
Juan Pablo Flores-Flores

Contents

Notations and Abbreviations

$\mathbb{N}$	The set of natural numbers
$\mathbb{Z}$	The set of integers numbers
$\mathbb{Q}$	The set of rational numbers
$\mathbb{R}$	The set of real numbers
$\mathbb{C}$	The set of complex numbers
$A, B, \ldots$	Capital letters represent arbitrary sets
$x, y, \ldots$	Lowercase letters represent elements of a set
$A \subset B$	A is subset of B
$x \in A$	x is element of A
$A \cup B$	The union of two sets
$A \cap B$	The intersection of two sets
A^c	Complement set of A
$A \setminus B$	Difference of sets A and B
$\oplus$	Bitwise XOR logical operation
$\emptyset$	Empty set
$\Longleftrightarrow$	Necessary and sufficient condition
$\forall$	For all
$\sim$	Equivalence relation
$a \equiv b \mod n$	a is congruent with b module n
$*$	Binary operation for groups
$\det(A)$	The determinant of a square matrix $A \in \mathbb{R}^{n \times n}$
$\mid A \mid$	The determinant of a square matrix $A \in \mathbb{R}^{n \times n}$
$\mathrm{Tr}(A)$	The trace of a matrix A
$A^\intercal$	The transpose of a matrix A
$\{\}$	Set
$(a_{ij})_{i,j}$	$m \times n$ matrix with entries $a_{ij},\ 1 \leq i \leq m, 1 \leq j \leq n$
$\mathrm{rank}(A)$	Rank of a matrix A
A^{-1}	Inverse of A
$\dot{y} = \frac{dy}{dt}$	First derivative of y with respect to t

$\square$	Designation of the end of a proof
$<$ ($>$)	Less (greater) than
$\leq$ ($\geq$)	Less (greater) than or equal to

List of Figures

Introduction

1

Abstract

In this chapter we give an overview of cryptography and cryptanalysis where basic concepts and definitions are given, also the relation of cryptography to chaotic systems synchronization is addressed.

1.1 Chaotic System Synchronization and Encryption Algorithms

Chaotic systems synchronization was introduced in [1]. There is proposed a methodology such that a chaotic system called slave, follows the state trajectories of a second chaotic system called master. This, by means of a coupling signal. Subsequently, numerous proposals have emerged to achieve the same goal, such as complete synchronization, generalized synchronization, impulsive synchronization, phase synchronization, delay synchronization, etc. As a result, multiple applications of chaotic systems synchronization have been found. One of the most important is secure communications [2–9], which is the main topic of this book.

Most encryption algorithms based on chaotic systems can be classified into one of the following kinds of encryption:

- **Chaotic masking**: It consists of adding the signal message on the output of a chaotic system.
- **Chaos shift keying (CSK)**: It consists of transmitting a message as variations of a given parameter of the chaotic system. It usually requires converting the message to its binary equivalent, therefore, in this scheme 1 corresponds to a specific parameter

R. Martínez-Guerra et al., *Encryption and Decryption Algorithms for Plain Text and Images using Fractional Calculus*, Synthesis Lectures on Engineering, Science, and Technology, https://doi.org/10.1007/978-3-031-20698-6_1

value and 0 to another. As a result, changes occur in the behavior of the chaotic system attractor.
- **Chaotic modulation**: Here, the message changes the value of some parameter of the chaotic system.

These are the best known methods that consist in encrypting messages with chaotic systems and then recovering them by means of a synchronization. A more extensive explanation of these encryption algorithms, based on chaotic systems is given below.

1.1.1 Encryption Through Chaotic Systems

There exist two basic types of chaotic cryptosystems: analog and digital. The former are mainly based on the synchronization of chaotic systems, the second ones, can be independent of synchronization and are completely digital. The implementation of an analog encryption algorithm requires the circuits responsible of generating chaos to be described in sufficient detail, such as the explicit form of the differential equation of the system and parameters that generate chaotic behavior. Meanwhile, for digital systems, precision, arithmetic (floating or fixed point), hardware configuration, among others, must be given.

In general, encryption algorithms are typically divided into two kinds: symmetric key and asymmetric key. The former uses the same key to encrypt and decrypt information, as a consequence these are extremely fast and useful to handle large volumes of data at high speed. This kind of algorithms are divided into two classes:

- **Stream cipher**: These generate a pseudo-random stream of symbols (keystream) by means of a public deterministic algorithm, which is governed by a secret key. Thus, the message is combined with the keystream, usually with a two-module sum or with a bitwise XOR. Among the most common stream ciphers we have: A5 / 1, A5 / 2, E0. RC4, SEAL, etc.
- **Block encryption**: These encrypt the original message by clustering its elements in blocks of two or more, so that each encrypted block is of the same size. These algorithms usually consist of an initial transformation, a cryptographic function iterated certain number of times and a final transformation. Then, the key is expanded using some algorithm so that enough key elements are obtained for each round of encryption. The most popular algorithms of this kind are: AES, DES, RC5, etc.

Symmetric key algorithms generally have keys between 128 and 256 bits. On the other hand, asymmetric key algorithms use two keys for the encryption and decryption process. Usually one of the keys is public and the other private. When encrypting, both keys are used and to decrypt only the private key is necessary. These algorithms are generally slow as require complex operations with large integers, so they are used to encrypt small data

packets such as digital signatures, secret key agreements, etc. The most common public key algorithm is RSA and its keys usually require between 1024 and 4096 bits [10].

The key is fundamental in any encryption algorithm. However, very few works in the literature, proportionate detailed information about the key. Therefore, in the following a simple introduction is given to understand the importance of these keys and how they should be obtained for chaotic cryptosystems.

1.2 Key or Security Code

A common element in all encryption algorithms is the key. The security code of an encryption algorithm must depend exclusively on the key [11].

No matter how strong and how well designed an algorithm is, if the key is not adequate, then the encryption will be easily violated [10]. As has been said, there is little information about how to choose or design the keys. Moreover, fundamental specifications such as the space of the key or the variables to be used as key are not presented. Therefore, here this will be one of the main aspects to be covered when proposing encryption algorithms.

The key space is defined as the set of values that can be used as keys. The size of the key space is given by the number of possible keys for the system. The keys from classical encryption algorithms are usually strings of random bits that are generated by some automatic process. In the chaotic encryption schemes, the properties of the key space elements are not the same, since not all keys are equally strong. For this, a bifurcation diagram can be useful to find intervals in which a key produces periodic orbits and thus avoid the use of weak keys (degenerate keys).

When many parameters are used simultaneously as a key, finding the most convenient intervals (without degenerate keys) might be difficult due to the dependence between the parameters. In such case, the positive Lyapunov exponents can be used to describe the key space. Thus, it must be obtained the largest Lyapunov exponent for the desired parameter combinations, then, if the obtained exponent is positive, the parameter combination can be used as a key.

The key space must be large enough to avoid brute force attacks. However, if the region that produces chaotic behavior is not large enough, it must be increased as much as possible to avoid equivalent keys. That is, to avoid a group of keys that can decrypt the same encrypted message due to its closeness. Thus, the region that produces chaotic behavior must be discretized so that the space between adjacent keys does not produce equivalent keys.

The keys should favor the presence of the so called avalanche property, that is, when a change occurs in the key the encrypted message will change radically and ideally it should change at least half of the values of the encrypted message. In some cases, the chaotic system parameters are set and only one of them is used as a key, which can be counterproductive since it is possible to use a bit-error-rate (BER) attack in which some system parameters are set and from these, an approximation of the one used as the key can

be obtained. Therefore, the partial knowledge of the key should never reveal information about the message or the unknown part of the key.

The security of an encrypted message is usually given by the priority when designing an encryption algorithm. When a new encryption algorithm is presented, it is common to provide a security analysis of it. Therefore, in the following will be presented an explanation on what an appropriate security analysis should contain for each type of cryptosystem.

1.3 Security Analysis

Security is the main interest of an encryption algorithm, so it must be evaluated at least by a basic security analysis. This is, it must at least withstand the most known and popular attacks to identify and correct defects before the system is published.

The algorithm will be resistant to the most common attacks if have two basic characteristics: confusion and diffusion. The first makes the relationship between the key and the encrypted message as complex as possible, making difficult to find redundancies or statistical patterns in the encrypted message. The second property consists of rearranging or scattering the bits in a message so that the influence of the message and the key are dispersed as best as possible within the encrypted message. To fulfill these requirements, the algorithm must satisfy the following [12]

1. Sensitivity with respect to the key, that is, changing a single character of the key produces completely different encrypted messages when the algorithm is applied to the same message.
2. Sensitivity with respect to the message, that is, altering one bit of the message should create totally different encrypted messages.
3. Absence of patterns in the encrypted text.

The first two characteristics generate confusion, while the last one is responsible for providing diffusion.

1.3.1 Cryptographic Attacks (Cryptanalysis)

During the security analysis, must be carried out attacks that assume that the cryptanalyst knows the exact design of the algorithm and how it works. This is, everything about the algorithm, except the key, is known. This must be done since the algorithm is sold to several users and therefore, it is reasonable to assume that it will easily be stolen, compromising all the details of its operation. Thus, the security of the algorithm must depend only on its key and not in the secrecy of its operation.

A cryptographic system can be described by the following elements:

1. P is the set of possible messages.
2. C is the set of possible encrypted messages.
3. K is the space of the key.
4. e_k is the encryption algorithm for each element $k \in K$.
5. d_k is the corresponding decryption algorithm for the element $k \in K$ mentioned in the previous point.

The operation of an algorithm can be summarized as follows: given a message $x \in P$, this can be encrypted with a key $k \in K$ by using the encryption rule $e(x, k) = y,\ y \in C$. Meanwhile, the encrypted message y is decrypted by using the corresponding decryption rule $d(y, k) = x$, such that $d(e(x, k), k) = x$.

There are several kinds of attacks to carry out the cryptanalysis of an algorithm. The most popular ones are listed below, starting with the most complicated:

1. **Ciphertext only (encrypted message)**: The attacker knows one or more encrypted messages $y_1, y_2, \ldots, y_n \in C$.
2. **Known plaintext (known message)**: The attacker knows one or more messages $x_1, x_2, \ldots, x_n \in P$ and its corresponding encrypted message $y_1, y_2, \ldots, y_n \in C$.
3. **Chosen plaintext (chosen message)**: The attacker has temporary access to the encryption device and can choose some messages $x_1, x_2, \ldots, x_n \in P$ as well as obtain the encrypted messages $y_1, y_2, \ldots, y_n \in C$ that are generated.
4. **Chosen ciphertext (chosen encrypted message)**: The attacker has temporary access to the encryption device and can choose some encrypted messages $y_1, y_2, \ldots, y_n \in C$ as well as obtain the messages $x_1, x_2, \ldots, x_n \in P$ that are generated.

The objective of each of these attacks is to obtain the key k or some equivalent key that was used to encrypt the messages. In particular, the attacks of known and chosen message are very effective in the cryptanalysis of algorithms based on chaotic systems [13–16]. There exist other attacks that are less common. However, these have characteristics of the already mentioned above. In the case of block encryption algorithms, the analysis on the susceptibility to differential and linear cryptanalysis should be included.

1.3.2 Differential Cryptanalysis

Differential cryptanalysis was introduced by Guojie et al. [17] and is a variant of the chosen message attacks, which tries to find the key of an iterative encryption algorithm. It consists of analyzing the differences caused in encrypted messages when performing determined changes in the messages that generated them. These differences are used to determine the most probable key among all the possible keys. At the same time, the number of tests that

would be done when implementing a brute force attack is reduced. Usually, the difference is chosen as the result of a bitwise XOR operation between the two unencrypted messages.

1.3.3 Linear Cryptanalysis

Linear cryptanalysis was introduced in [18] and is essentially a known message attack whose purpose is to generate a linear expression that approximates a certain block cipher. A linear expression for a given iteration will be an equation that is based on the module-two sum between the inputs and outputs of such iteration.

1.4 Specific Attacks for Stream Cipher-Type Chaotic Cryptosystems

There are several cryptanalysis forms for stream cipher encryption algorithms based on chaotic systems. These can be classified as follows:

1. Extraction of the signal from the message $s(t)$ of the transmitted signal $y(t)$.
2. Extraction of the signal that carries the data $c(t)$ and then remove it and retrieve the message $s(t)$.
3. Estimation of the transmitter's secret parameters to completely break the algorithm.
4. Brute force attacks.

Each of these analyses is explained in greater detail below.

1.4.1 Message Extraction

When using chaotic masking techniques, extracting the signal is possible if the message $s(t)$ is a periodic signal during a sufficient amount of time. Methods such as auto-correlation and cross-correlation analysis, spectral power analysis, filtering techniques, and generalized synchronization are usually used.

Power spectral analysis and filtering take advantage of the chaotic signals limitations, which are used to mask the message. The power spectrum of the message must be completely covered with the power spectrum of the chaotic signal that was used to mask it. However, several encryption algorithms fail at this, since the commonly used chaotic oscillators, such as Rössler, Lorenz, Chua, Duffing, etc., have a much lower density power than common messages. Therefore, these cannot support this type of filter-based attacks.

The generalized synchronization attack was introduced in [19]. This assumes that the attractor used is known, but the oscillator parameters are ignored. Its purpose is to

reconstruct the signals used to hide the message and then access the signal that contains the message.

1.4.2 Parametric Estimation

Several chaos-based encryption schemes are not sensitive enough to variations in transmitter and receiver parameters, allowing similar parameters to be used for message retrieval.

Different methods can be used for this, for example, it is possible to solve the differential equations based on the signals that they emit. Also, the parameters can be estimated from a generalized synchronization scheme. In addition, some adaptive control techniques can be useful to find equivalent keys.

1.4.3 Brute Force Attacks

A brute force attack consists on testing all the possible keys. The effectiveness of this attack will depend on the size of the key space and the attacker's processing capacity. It is commonly considered that any space with less than 2^{100} elements it is not safe, although this number increases when the processing power is improved [10].

References

1. Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical Review Letters A*, *64*, 821–824.
2. Kocarev, L., Halle, K. S., Eckert, K., Chua, L. O., & Parlitz, U. (1992). Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Chaos*, *2*(03), 709–713.
3. Liao, T. L., & Huang, N. S. (1999). An observer-based approach for chaotic synchronization with applications to secure communications. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *46*(9), 1144–1150.
4. Cuomo, K. M., Oppenheim, A. V., & Strogatz, S. H. (1993). Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, *40*(10), 626–633.
5. Smaoui, N., Karouma, A., & Zribi, M. (2011). Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systems. *Communications in Nonlinear Science and Numerical Simulation*, *16*(8), 3279–3293.
6. Wang, S., Kuang, J., Li, J., Luo, Y., Lu, H., & Hu, G. (2002). Chaos-based secure communications in a large community. *Physical Review E*, *66*(6), 065202.
7. Li, Z., & Xu, D. (2004). A secure communication scheme using projective chaos synchronization. *Chaos, Solitons & Fractals*, *22*(2), 477–481.
8. Nana, B., Woafo, P., & Domngang, S. (2009). Chaotic synchronization with experimental application to secure communications. *Communications in Nonlinear Science and Numerical Simulation*, *14*(5), 2266–2276.

9. Li, C., Liao, X., & Wong, K. W. (2004). Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communication. *Physica D: Nonlinear Phenomena*, *194*(3–4), 187–202.
10. Schneier, B. (2007). *Applied cryptography: Protocols, algorithms, and source code in C*. John Wiley & Sons.
11. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.
12. Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, *16*(08), 2129–2151.
13. Biham, E., & Shamir, A. (2012). *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media.
14. Alvarez, G., Montoya, F., Romera, M., & Pastor, G. (2000). Cryptanalysis of a chaotic encryption system. *Physics Letters A*, *276*(1–4), 191–196.
15. Stojanovski, T., Kocarev, L., & Parlitz, U. (1996). A simple method to reveal the parameters of the Lorenz system. *International Journal of Bifurcation and Chaos*, *6*(12b), 2645–2652.
16. Li, C., Li, S., Zhang, D., & Chen, G. (2005, May). Chosen-plaintext cryptanalysis of a clipped-neural-network-based chaotic cipher. In *International Symposium on Neural Networks* (pp. 630–636). Berlin, Heidelberg: Springer.
17. Guojie, H., Zhengjin, F., & Ruiling, M. (2003). Chosen ciphertext attack on chaos communication based on chaotic synchronization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *50*(2), 275–279.
18. Matsui, M. (1993, May). Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 386–397). Berlin, Heidelberg: Springer.
19. Yang, T., Yang, L. B., & Yang, C. M. (1998). Breaking chaotic switching using generalized synchronization: Examples. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *45*(10), 1062–1067.