Chapter 5

High Performance Technology in Algorithmic Cryptography

Arturo Lezama-León, José Juan Zarate-Corona,
Evangelina Lezama-León,
José Angel Montes-Olguín,
Juan Ángel Rosales-Alba and
Ma. de la Luz Carrillo-González

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75959

Abstract

Alan Turing's article, "Computation and intelligence", gives the preamble of the characteristics of guessing if it is a machine or another human being. Currently, the use of ubiquitous technologies, such as the use of firmware, allows direct access to analog data, however, we must find a way to secure the information. Analyzing cryptographic algorithms for the transfer of multimedia information. Raise the use of cryptarithmetic. Finite automata will be developed that will govern the logic of the cryptographic algorithms to be integrated into Firmware, performance tests and controls will be carried out to determine the best strategies for their performance and algorithmic complexity. Technologies are expressed that allow the creation of learning environments, such as neural networks, that support other processes as the recognition of patterns on images.

Keywords: cryptarithmetic, cryptographic algorithms, firmware, HPC

1. Introduction

In this research, it is revealed how algorithms are integrated into different representations of the data, information seen as signals, images, video and text.

1.1. Turing machines

Alan Turing's test, proposed in 1950, was designed to provide an operational and satisfactory definition of intelligence.

He suggested a test based on the inability to differentiate between indisputable intelligent entities and human beings.

The computer should have the following capabilities

- Natural language processing, which allows you to communicate in English.
- Representation of knowledge, to store what is known or felt.
- Automatic reasoning, to use stored information to answer questions and draw new conclusions.
- Machine learning, to adapt to new circumstances and to detect and extrapolate patterns.
- Computational vision, to perceive objects.
- Robotics, to manipulate and move objects.

These six disciplines cover most of the Artificial Intelligence (AI), in reference [1, 2].

1.2. Artificial intelligence and the cryptarithmetic

The Artificial Intelligence is the study of how to make computer do things which, at the moment, people do better, in Ref. [2].

1.2.1. cryptarithmetic

It considers high order constraints which can be represented as a collection dev binary options F <> T, in Ref. [3].

1.3. Automata design

An automaton is a graphic representation of a process, which simulates a sequential process, by means of a deterministic finite automaton, the use of a regular expression can be modeled, and this, in turn, can be evaluated by algorithmic complexity.

There is a counterpart which obeys different inputs at the beginning and consequently can represent several outputs, so we proceed by means of a mechanism to migrate them as a finite deterministic automaton, similarities with neural networks in terms of structure, but not functioning because they pursue different aspect.

Regarding its sequential form, it can be simulated by means of a flow diagram as a graphic form, however, in its parallel form, it must be used either an activity diagram or a Petri net, which can model the concurrent behavior, in reference [4].

Because the keys are usually registered by characters of the ASCII code, they can be validated by regular expressions and this in turn then recreating validation controls by deterministic finite automata.

http://dx.doi.org/10.5772/intechopen.75959

When a possible entry is described under this form, then we are in the presence of an entry control but not access.

For access, we search for a match of a stored key to managing access to the data, if the password is treated by a cryptographic system then the entry and access controls do not change their form, but the time of computation to corroborate its degree of efficiency.

By having access control list (ACL), the restrictions are carried out through the management of routing tables and entry rules.

The use of ACL increases the level of security in information systems.

The use of Firewalls allows having an accurate strategy as if it were a blog.

Cryptographic systems have been implemented to treat various types of data and signals such as multimedia so that not only text can be treated.

In this way its study is of interest because in applications oriented to the control and automation of signals in greenhouses, home automation, automation, automation and control, information security in closed or public environments, the integration of microcontrollers is intended which can supply to a large extent, restrictive measures which make their assurance slow.

In this research, it is revealed how algorithms are integrated into the different representations of the data, information seen as signals, images, video, and text.

The signals are presented in the form of a 1D dimension, two 2D dimensions, and three 3D dimensions. It is important to understand that as the degree of complexity is advanced, it increases as the subject deserves or intends for an even more exhaustive study.

This research does not intend to venture to deny or violate systems, but as a form of prevention, to continue with research studies, still need to specify the cryptanalysis for each system, only the studies discussed so far are presented.

1.4. Computer legislation and regulations

The use of technology in today's world is inevitable. Whether it is making reservations on our smartphones, or checking emails, or checking in for flights, usage of technology is present. Whilst its benefits cannot be questioned, unfortunately, the increase of our reliance on technology implies that we are at higher risk of attack and breaches – cyber-attacks. Responding to this current scenario, current trends of governments protecting their critical infrastructures is the implementation of cybersecurity standards to their critical sectors, in reference [5]. The Global Risk 2014 by World Economic Forum (WEF) shows the 'cyber-attacks' listed in the top 5 global risks, highlighting that the dependency on technology by economies and societies is inevitable, in reference [6].

The implementation of cybersecurity standards is by no means a silver bullet in critical infrastructure protection. However, its implementation can establish a set of controls that contribute and build better resiliency. The cybersecurity standards may support the capabilities of preparing, protecting, responding and recovering from cyber-attacks. Some of the common cybersecurity-related standards being implemented globally include the following (not exhaustive): ISO/IEC 27032:2012. Information technology – Security techniques

– Guidelines for cybersecurity. ISO/IEC 27001 Information technology – Security techniques – Information security management systems-Requirements. ISO 22301 Societal security – Business continuity management systems-Requirements. ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security. ISO/IEC 27035 Information technology – Security techniques – Information security incident management. ISO/IEC 27005 Information technology – Security techniques – Information security risk management. FIPS 140-1: Security Requirements for Cryptographic Modules. FIPS 186-3: Digital Signature Standard, in reference [5].

Countries take different approaches towards implementing cybersecurity standards in the efforts of protecting their critical infrastructures. Some countries implement cybersecurity standards through mandatory requirements, whilst others provide guidelines and frameworks, in reference [5].

The United Kingdom's priorities for action is to model the best practice on cyber security in the government systems which will set the standard for suppliers to government to raise the bar on cybersecurity requirement.

Due to this:

1. UK has enforced compliance to the Network Interoperability Consultative Committee (NICC) Minimum Security Standards (ND 1643) through the Communications Act 2003 to the Communications Sector,

2. UK has developed the cyber security and information assurance standards – Information Assurance Maturity Model (IAMM) incorporating the requirements from the Security Policy Framework (SPF),

3. SPF recognizes and has aligned its principles to the ISO/IEC 27001 and the Business Continuity Management (BCM) standards (BS 25999/ISO 22301), and.

4. The application of standards is promoted through the establishment of national-level certification schemes for the following standards such as the ISO/IEC 15408, ISO/IEC 27001, ISO/IEC 20000, BS 25999 and ISO 22301, in Ref. [5].

Australia's cybersecurity standards compliance implementation is supported by the country's Cybersecurity Strategy 2009 highlighting the need for a consistent and integrated framework of policies, procedures and standards to protect its government's systems, as well as the other interconnected systems. Australia's security measures are: (1) the development and enforcement of the Protective Security Policy Framework (PSPF) to the government agencies through a Directive by the Attorney-General Department (AGD), (2) Australian government has enforced the ISO/IEC 15408 for procurement of products with security functions in the Government Sector, and (3) standards implemented voluntarily and adopted by critical infrastructure organizations are the American National Standard Institute/International Society of Automation (ANSI/ISA)-99, Industrial Automation and Control Systems Security and ISO27799 Health Informatics – Information security management in health using ISO/IEC 27002.

United States of America (USA) has developed various national strategies on cyber security: (1) The Comprehensive National Cybersecurity Initiative (CNCI) will evolve to become the key

http://dx.doi.org/10.5772/intechopen.75959

element of a broader updated national USA cyber security strategy, (2) standards mandated to the Energy and Dams sectors are the Reliability Standards Critical Infrastructure Protection (CIP) 002-009 through the Code of Laws of the United States of America (U.S.C)Title 16 – Conservation, Section 824o – Electric Reliability (16 U.S.C 824o), (3) the standards mandated for the Government Sector is the Federal Information Processing Standards (FIPS) through Federal Information Security Management Act 2002 (FISMA), (4) other standards in the critical sectors are ISO 27799, ISO/IEC 27010 Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications as well as ISO/IEC 27011 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 for Telecommunications and ISO/ IECTR 27015 Information technology – Security techniques – Information security management guidelines for financial services for Financial Services, and (5) the government promotes the application of cyber security standards via establishment of national-level certification schemes for the following standards such as ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27006, ISO/IEC 20000, and ISO 22301, in reference [5].

The different approaches that countries take to cybersecurity standard compliance show that cybersecurity standards whether implemented mandatorily or voluntarily is a measure to enhance the protection of the critical infrastructure. Enforcing cybersecurity standards compliance may bring about a positive outcome to the overall cybersecurity management of a country, and not just the organizations implementing them, in reference [5].

1.5. Mexico rules and regulation

In Mexico, computer legislation is distributed in different rules and laws because the way in which it is pursued depends on the nature of the crime, then a list of some of the most common: show in **Table 1**.

1.6. E-government (eGov)

The year 2015 marked a milestone in efforts to eradicate poverty and promote prosperity for all people on a safe planet. With the adoption of the 2030 Agenda for Sustainable Development and other major international commitments. The 2030 Agenda is centered on a set of far-reaching and people-centered universal Sustainable Development Goals (SDGs). Reaching these goals in all countries and creating peaceful, just and inclusive societies will be extremely difficult in the absence of effective, accountable and inclusive institutions. Institutions need to be capable and equipped to adapt the Agenda to the national situation.

They need to be able to mobilize the society and the private sector in implementing the SDGs. Capacities and innovation will be required to promote policy integration, enhance public accountability, promote participation for more inclusive societies as well as ensure equitable and effective public services for all, particularly for the poorest and most vulnerable groups. Information and Communication Technology (ICT) and e-government are important tools to realize these objectives, in reference [8].

The 2030 Agenda itself recognized that "the spread of information and communications technology and global interconnectedness has great potential to accelerate human progress, to

1. E-commerce	Procurement Law, leases and public sector services (Ley de adquisiciones, arrendamientos y servicios del sector público)
	Commercial code (Código de comercio)
	Federal civil code (Código civil federal)
	Federal Law for Protection of the Consumer (Ley federal de protección al consumidor)
	Federal Law of Administrative Procedure (Ley Federal de Procedimiento Administrativo)
	Law of Investment Funds (Ley de Fondos de Inversión)
	Federation fiscal Code (Código Fiscal de la Federación)
	Social Security Law (Ley del Seguro Social)
2. Electronic signature	Advanced Electronic Signature Law (Ley de Firma Electrónica Avanzada)
	Law of the Tax Administration Service (Ley del Servicio de Administración Tributaria)
3. Personal data protection	Law of Investment Funds (Ley de Fondos de Inversión)
	Federal Law on Protection of Personal Data in Possession of Individuals (Ley Federal de Protección de Datos Personales en Posesión de los Particulares)
4. Right to the information	Article 6 Constitutional (Artículo 6° Constitucional)
	General Law of Transparency (Ley General de Transparencia)
	Access to public information (Acceso a la Información Pública)
	Federal Transparency Law (Ley Federal de Transparencia)
	Access to public information (Acceso a la Información Pública)
5. Violation of correspondence	Article 173 to 177 of the Federal Criminal Code (Artículo 173 al 177 del Código Penal Federal)
6. Revelation of secrets	Article 210 to 211 Bis of the Federal Penal Code (Artículo 210 al 211 Bis del Código Penal Federal)
7. Illicit access to computer systems and equipment	Articles from 211 bis 1 to 211 bis 7 of the Federal Criminal Code. (Artículos del 211 bis 1 al 211 bis 7 del Código Penal Federal).
8. Copyright	Articles from 424 to 429 of the Federal Penal Code (Artículos del 424 al 429 del Código Penal Federal).
9. Industrial property	Industrial property law (Ley de la propiedad industrial).
10. Stock market	Law of the marketc of values (Ley del mercado de valores).
11. Telecommunication	Federal Law on Telecommunications and Broadcasting (Ley Federal de Telecomunicaciones y Radiodifusión)
	Federal Criminal Code and Political Constitution of the United Mexican States (Código Penal Federal y Constitución Política de los Estados Unidos Mexicanos)

In Ref. [7].

Table 1. Mexico rules and regulation.

bridge the digital divide and to develop knowledge societies, as does scientific and technological innovation across areas as diverse as medicine and energy", in reference [8].

The General Assembly has recognized on several occasions the role of information and communications technology in promoting sustainable development and supporting public policies and service delivery. It has underscored that ICT have enabled breakthroughs "in Government and the provision of public services, education, healthcare and employment, as well as in business, agriculture and science, with greater numbers of people having access to services and data that might previously been out of reach or unaffordable". The General Assembly has also specifically affirmed the "potential of e-government in promoting transparency, accountability, efficiency and citizen engagement in public service delivery", in reference [8].

There are several definitions in circulation which differ as to the meaning or scope of the term "eGov". Next definitions illustrate different scope or stress in the understanding of what eGov is: (A) United Nations: the employment of the Internet and the world-wide-web for delivering government information and services to the citizens, (B) The World Wide Web Consortium says that is the use of the Web and other information technologies by governments to interact with the citizenry, between departments and divisions, and with other governments. (C) The Organization for Economic Co-operation and Development focuses on the use of new information and communication technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies has the potential to transform the structures and operation of government, in reference [9].

From the business perspective, eGov is a way of introducing new channels of interaction between government and consumers of its services, in order to make this interaction more convenient to the consumers and cheaper for the provider of the services, these business benefits, including the following

- Facilitating access to government data and processes to all types of consumers of these services, be it general public, business, government agencies or their employees, or other governments.
- Improving operational characteristics of government, including: (1) decreasing the cost to government of providing quality services to their consumers, (2) decreasing the load on the office workers by making at least some types of data or some of business processes directly available to service consumers.
- The reach of eGov services can be widened from initialized specialized groups to all consumers that have a need and a right for using the service without incurring substantial additional costs, in reference [9].

1.6.1. International and national standards in information security

The International Organization for Standardization (ISO) has the ISO/IEC 27000 family of standards, which aims to help in the management of asset security such as financial information, intellectual property and confidential information of employees or third parties.

Both ISO (the International Organization for Standardization) and IEC (International Electrotechnical Commission) make up the specialized system for global standardization, in Ref. [10].

The implementation of this system aims to preserve the confidentiality, integrity and availability of the information, through the application of a risk management process, which gives certainty to the interested parties that the risk has been adequately managed. They are considered best practices and are not considered mandatory as mentioned on their website, in Ref. [11].

In North America, there is NIST (National Institute of Standard Technology) of the United States Department of Commerce. This Institute handles issues of cybersecurity and privacy through the application of standards and best practices, including the ISO/IEC 27000 standards, in order to help organizations, manage the risk of cybersecurity within of a framework, in Ref. [12]. This framework includes physical, cybernetic and people security, applicable to organizations dependent on technology, such as industrial control systems, Information Technologies, cyber-physical systems, or connected devices, this includes the IoT (Internet of Things), in Ref. [13].

NIST has the National Cybersecurity Improvement Commission that is looking for:

- Awareness and protection at all levels of government, business and society to protect privacy,
- Guarantee public security and national economic security.
- Empower the Americans to have better control of their digital security.

Within NIST is the NC Coe (National Cybersecurity Center of Excellence), which are agreements with industry and institutions that participate in projects related to the topic of cybersecurity, in Ref. [14]. When information security is implemented, and the rules related to the country and form of government are respected, then its regulation must be followed to concretize the integration of the strategies involved. Such as applicable international norms and standards for their protection. Within the IT Audit is made aware of the use of controls for each aspect that involves the transfer of information, such as access control, entry control, communication control, etc.

A control is a procedure that verifies another procedure.

Therefore, control must be implemented that has not been violated, so its internal study is important.

The use of aspects such as high computing performance, infrastructure characteristics, is an important reason. Because there is no supercomputer, we opt for the design of a group of nodes that allows its gradual growth until it arrives as an operation to count on the performance of the supercomputers.

A network of computers has precisely the vision of the distributed and parallel system, however, care must be taken in the construction and operation thereof.

http://dx.doi.org/10.5772/intechopen.75959

2. High performance in technology

There is an international body that measures the capacity in supercomputing performance, within its schemes contemplated for most of its platforms the use of Linux, within the architecture is appreciated the use of MPP and the cluster, where you can appreciate the acceptable capabilities both work and performance. With this, it is possible to detect the speeds that are presented internationally. (e.g. **Table 2**, **Figure 1**).

The TOP500 project ranks and details the 500 most powerful don't distribute computer systems in the world, in reference [15].

The following graphs are presented in terms of performance and shared systems on an international scale, information retrieved from top500.org, in Ref. [15] (e.g. **Table 3**, **Figure 2**).

Mexico only occupies 0.2% of System share, it is for this reason that it is necessary to learn from the superpowers because it seems that the power of the supercomputing is wasted. (e.g. **Table 4**, **Figure 3**).

In which of the registered systems it can be noticed that Asia occupies the first place in the use of shared systems in High performance in computing.

2.1. High performance in computation

One of the first programs to verify the performance of the processes and programs was the task manager because it allows us to measure the performance by means of metrics to support the resources of a computer system such as our computer.

HPC stands for High-performance computing

By computation is processing, which has been attributed to thinking carefully about the hardware or a physical infrastructure, however, it should be distinguished in that the computation is also given by logic. It continued with the **Table 5**. Performance metric.

The use of cluster implies simultaneously using concurrent technology, in the concurrent model contains the following components

- Structure (static/dynamic)
- Granularity (nested/plane)
- Initialization (Thick/Fine Ending)
- Representation (parent/child or guardian/dependent)

Architecture	System share (%)
Cluster	87.4
MPP	12.6

Table 2. Architecture.

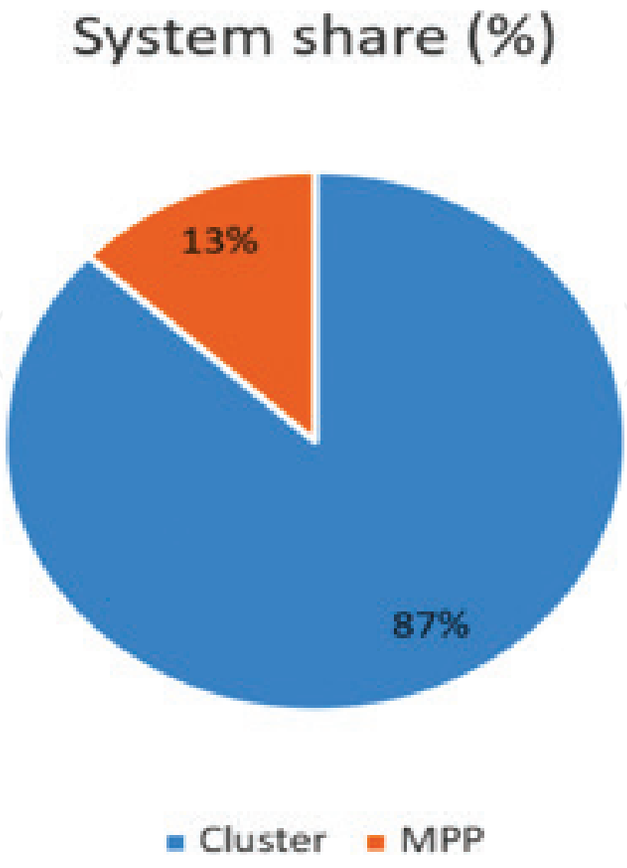

Figure 1. Architecture.

This systematic develop; consist in the use of the concurrent engineering by the design of components assembler. As show at the **Figure 4**.

By the moment these techniques have been studied at the final of Computer Sciences: the development of Systems in Real Time, the Recognition of Patterns, Semi-Intelligent Agents, the Computer Security as Cryptography and Crypto Analysis, the Information Systems based in knowledge, and Signs processing, are some cases for we appreciate this trouble, in reference [16].

Performance tests applied to cryptographic algorithms are abduction (statistics) and stress-based.

Continents	Performance
Other	0.70
Americas	30.20
Asia	48.70
Europe	20.40

Table 3. Continents.

http://dx.doi.org/10.5772/intechopen.75959

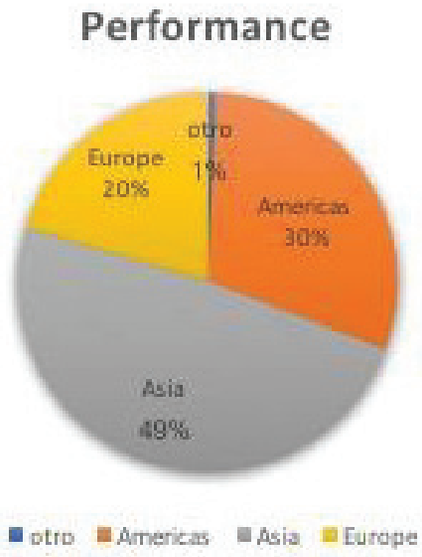

Figure 2. Performance.

Continents	System share (%)
Africa	0.2
Americas	29.8
Asia	50.4
Europe	18.6
Oceania	1

Table 4. Continents.

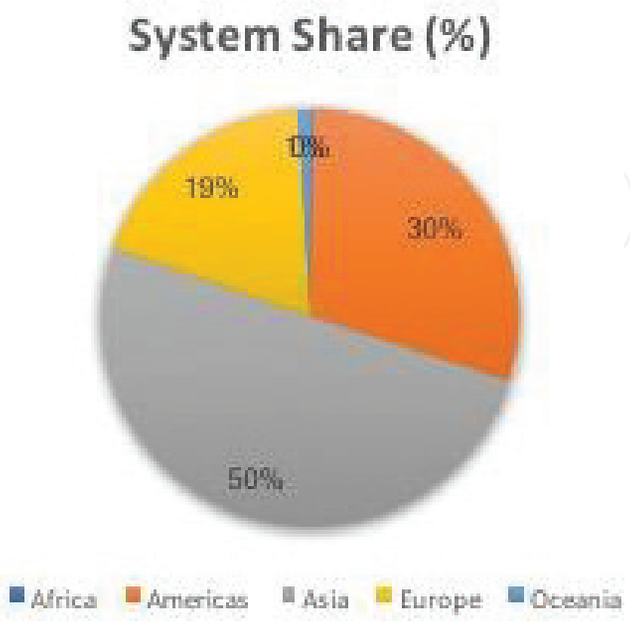

Figure 3. System share.

Metric	Load balance
	Runtime
	Communication volume
	Computing time
Metrics for multidimensional optimization	Cluster vs. Supercomputer
	Fiedler vector or spectral clustering
	Minimum normalized cut
	Connectors to eigenvectors
	Clustering by k means
	Restrictions in two dimensions
	Fourier modal analysis

Table 5. Performance metric.

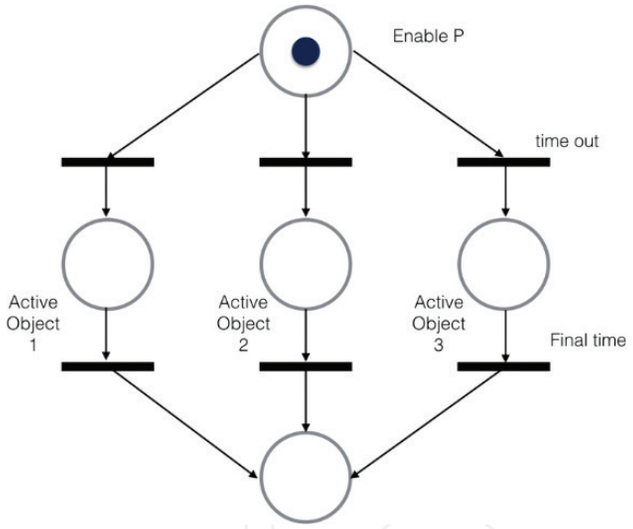

Figure 4. Petri net, model of concurrent active object.

3. Cryptographic algorithms

It can be implemented at any time, its operation involves calculating the key from the calculation of two keys that are presented with prime numbers.

The microchip company announced a microcontroller that has the ability to operate with most of the cryptographic algorithms, however, now it is worth thinking, what is it that is intended to ensure?

3.1. Cryptographic algorithms in IoT

Operating system being responsible for the management and control of all computer hardware resources, the security involves a multi-user and multi-programming environment where the

http://dx.doi.org/10.5772/intechopen.75959

primary goals include the prevention of any unauthorized access to data stored within the system, the safeguarding of users from undesirable results triggered by their own actions, the assurance that various user programs will not interfere with one another, and the ability of different users to have different rights and abilities to cooperate with each other. The issues which deal with him are critical and far reaching, for this reason, they are of vital importance for both its own and its applications' sakes, in reference [17].

Achieving security in operating systems depends on the security goals one has. These goals will typically include goals related to confidentiality, integrity, and availability. In any given system, the more detailed particulars of these security goals vary, which implies that different systems will have different security policies intended to help them meet their specific security goals, in reference [18].

Network security threats are also an operating system responsibility since a computer network is usually a rather large, single system which has been created from numerous individual computer systems. The data processing functions must now be distributed among a set of distinct systems thus decentralizing the control of data storage and processing. In addition, information which must be transmitted between the various computers within the network is subject to exposure. Forged user identification and unauthorized access to stored data by legitimate users are also problems which plague a multi-user, multi-resource environment. Consequently, these factors combine to complicate the problem of ensuring a high degree of security within the network and may present formidable pitfalls, in Ref. [17].

A good cryptographic system must have several characteristics: Small variations of plain texts: large variations of encrypted texts, the sizes of the flat texts must be comparable with the ciphers, the ciphered texts must be calculated efficiently from the planes, and the relationship between plain and ciphered texts should be unpredictable. A bad cryptographic system is characterized because: It appears a random relationship between planes and ciphers, but in reality, it is not, it is susceptible to elementary cryptanalysis, the calculation of ciphers is inefficient in time and space, and is vulnerable to its own manufacturers, in Ref. [19].

In the past, protection against the monitoring of communication lines was guaranteed by the use of physically secure lines. This technique, however, proved to be extremely expensive and, often times, impractical. Since that time, it has been discovered that data encryption may be used as a viable alternative to secure lines, in Ref. [17]. Cryptographic technology is, therefore, a relatively inexpensive and highly effective process by which sensitive data may be protected against disclosure, in reference [17].

Android includes cryptography to protect their information, many of the applications that are installed in a cell phone with an operating system have already cryptographic features to protect the information that the cell phone itself has. Each of the applications that have a cell phone, both those that have the factory and those that are installed after having purchased the cell phone, are handled in layers, where each of them uses services offered by the previous ones and offers the same to layers superiors All applications use the services, application interfaces and libraries of the previous layers. This structure facilitates the development of cryptographic applications in this operating system, but there is the disadvantage that the execution of cryptographic algorithms becomes more expensive as their complexity and strength increase, in Ref. [20]. Linux has a kernel crypto API that offers a rich set of cryptographic ciphers as well

as other data transformation mechanisms and methods to invoke these. The kernel crypto API serves the following entity types: (a) consumers requesting cryptographic services and (b) data transformation implementations (typically ciphers) that can be called by consumers using the kernel crypto API, in Ref. [21].

Apple Inc. has a variety of cryptographic technologies around of all their products.

App Transport Security (ATS) ATS establishes best-practice policies for secure network communications using Apple platforms, employing Transport Layer Security (TLS) version.

3.2. Forward secrecy and strong cryptography

Secure Transport API. Use Apple's secure transport API to employ current versions of the Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Datagram Transport Layer Security (DTLS) cryptographic protocols for network communications.

Supported Algorithms. With iOS 10 and macOS v10. 12, the RC4 cipher suite is now disabled by default. In addition, Apple recommends that you upgrade your servers to use certificates signed with the SHA-2 cryptographic function.

Cryptographic Signing. If distributing your Mac app outside of the Mac App Store, use cryptographic signing with Developer ID to certify that your app is genuine.

CryptoTokenKit for Smart Card Support. The CryptoTokenKit framework provides first-class access for working with smart cards and other cryptographic devices in macOS, in reference [22].

Microsoft shows in its web site the Cryptography API: Next Generation (CNG) that is the long-term replacement for the CryptoAPI. CNG is designed to be extensible at many levels and cryptography agnostic in behavior. Some of its features are listed next: Cryptographic Agility, Certification and Compliance, Suite B Support, Legacy Support, Kernel Mode Support, Auditing and Replaceable Random Number Generators, in reference [23].

According to the list dictated by top500.org, the best platforms in HPC are presented below (e.g. **Figure 5**).

3.3. Public key cryptography

The data that has been monitored by telepathic systems arises from information related to greenhouses, they are perhaps only data that support a part of a process in agronomy, however, they are important for their better interpretation.

JFLAP is software for experimenting with formal languages topics including nondeterministic finite automata, nondeterministic pushdown automata, multi-tape Turing machines, several types of grammars, parsing, and L-systems, by the University Duke, in Ref. [24] (e.g. **Figure 6**).

http://dx.doi.org/10.5772/intechopen.75959

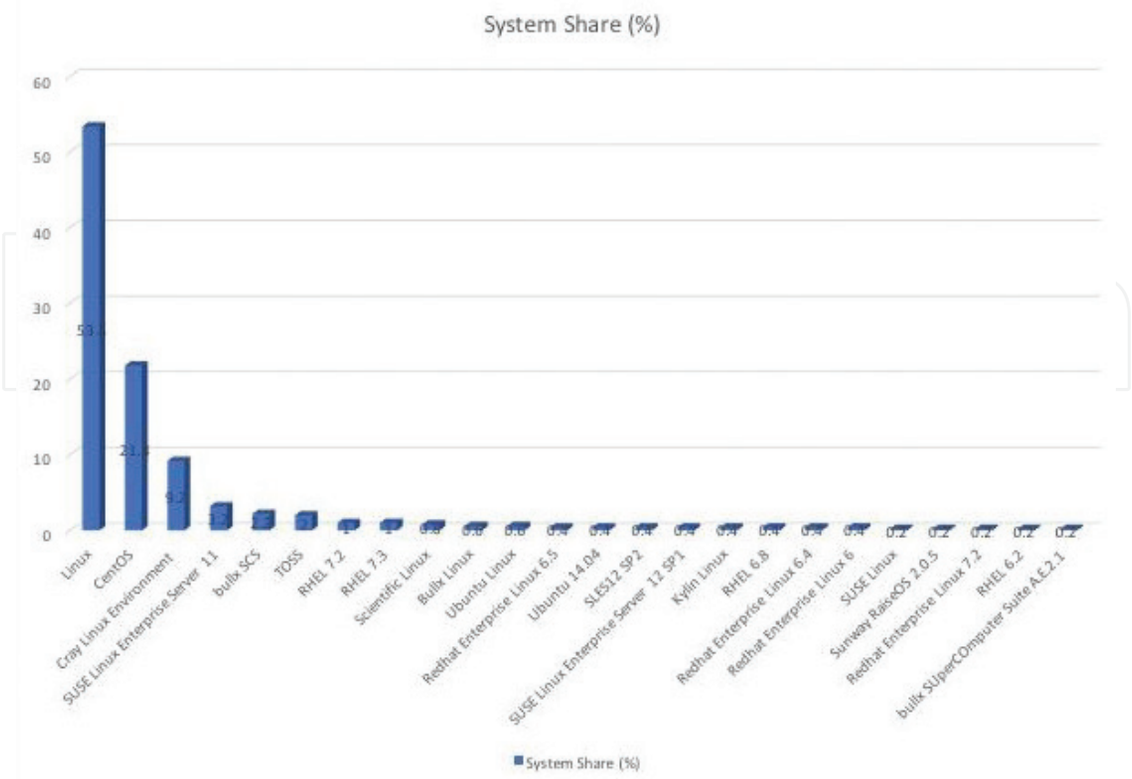

Figure 5. Histogram of platforms.

The type of applications that generally work with sophisticated equipment such as the supercomputer or cluster, is one that presents complexity in it is development, development, those that consume more massive storage capacity and require speeds appropriate to their way of being. While social networks currently involve more data consumption, it is important to recognize that so are the applications that generate scientific researchers by searching for new solutions to real-world problems or that are analogous to their area of expertise. The aim of the following scheme is precise to make known part of the advances that we as a research team have. We do not express all theories or investigations, it's just a

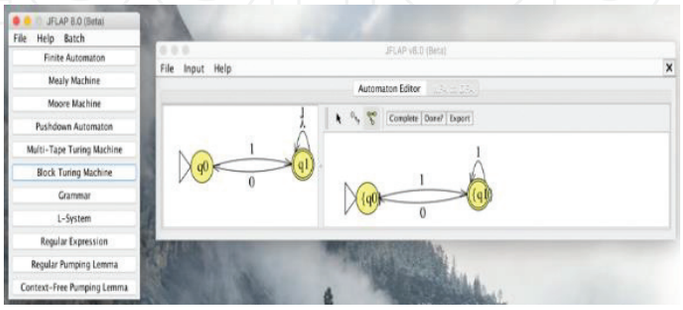

Figure 6. JFlap.

preamble of what these systems can be capable of doing in relation to what they are capable of doing. The use of state machines is important in the design of logical machines because they allow deducing the logic of their operation. That is to say, the following is the use of a simple machine that allows to deduce chains of 0 and 1, in such a way accept words of 0 and 1s, like prime numbers.

For the generation of keys, it is necessary to design an algorithm that allows the generation of random numbers, below is an algorithm that supports the generation of pseudorandom numbers, in reference [25].

Show in notation with Henon Map, this is a method chaotic map, and it is employed in dynamic systems to discrete process (e.g. **Figure 7**).

3.3.1. Encryption in one dimension (1D) flow

Used the RSA Algorithm to prove of text [26] (e.g. **Figure 8**).

3.3.2. Encryption in two dimension (2D) flow

The tent map, like various chaotic maps, as pseudorandom sequence generator, in Ref. [27] (e.g. **Figures 9** and **10**).

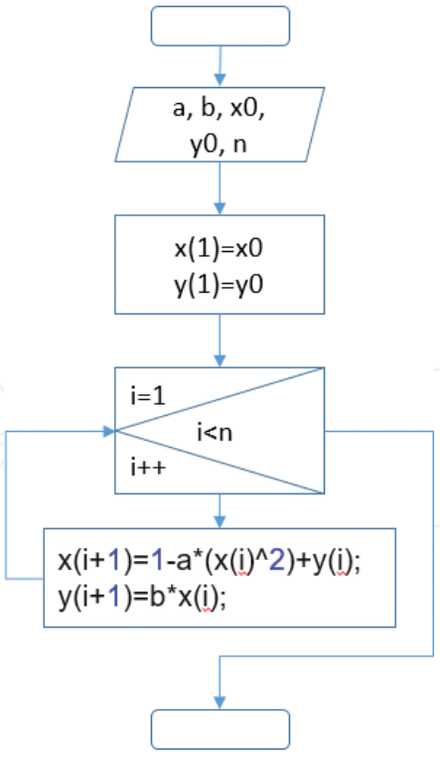

Figure 7. Pseudorandom by Henon map.

http://dx.doi.org/10.5772/intechopen.75959

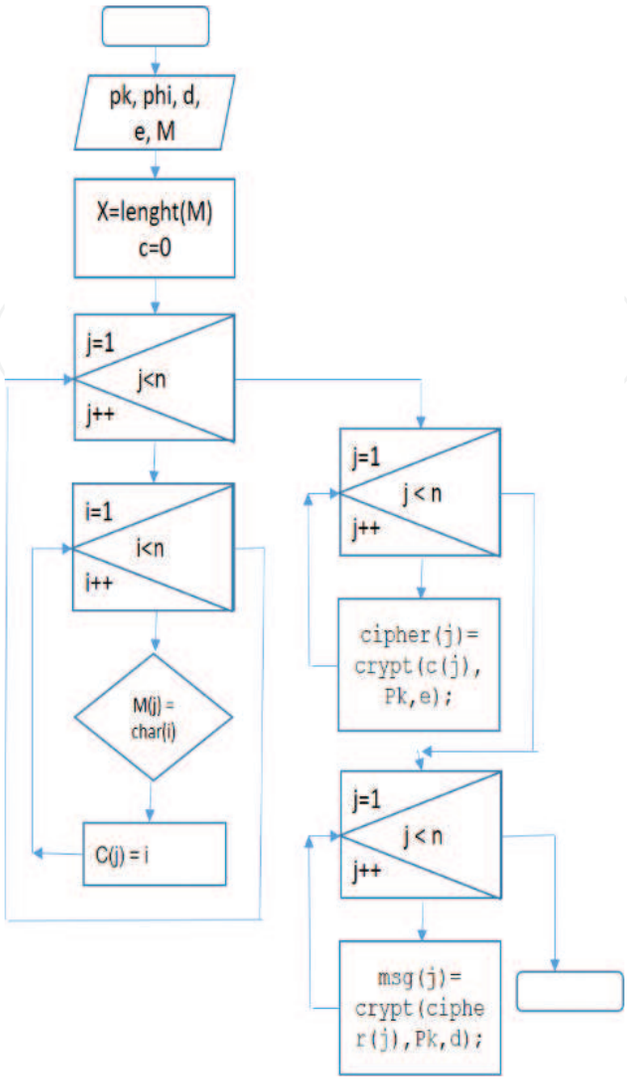

Figure 8. Algorithm by RSA.

These algorithms applied to images allow to know the range of operations necessary to work together, however, it is important to emphasize the moment in which the integration of the cryptographic algorithms must be perfected to the process involved.

3.3.3. Encryption in 3D flow

The reading of information generated by the stereo vision allow to get hard acquisition data, as the focal lens adjust. It proposes the tracking of systems at real time uses with the transformation Census. it is left for future work.

Real Time Stereo Vision with a modified Census transform and fast tracking in FPGA, in Ref. [28].

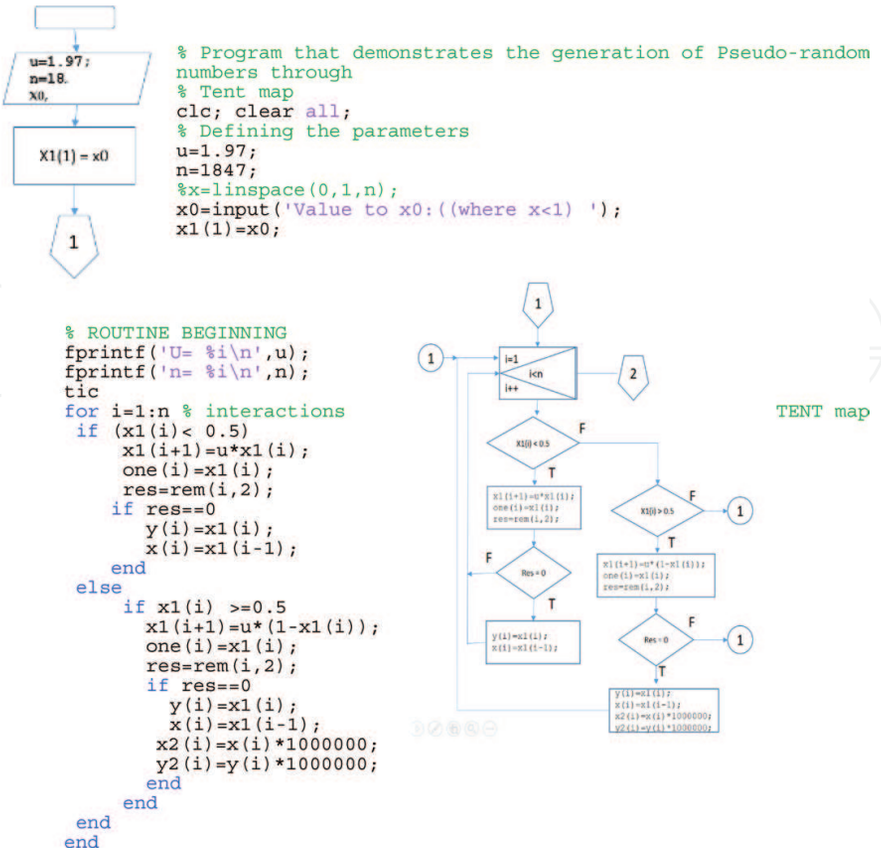

Figure 9. Algorithm by tent map.

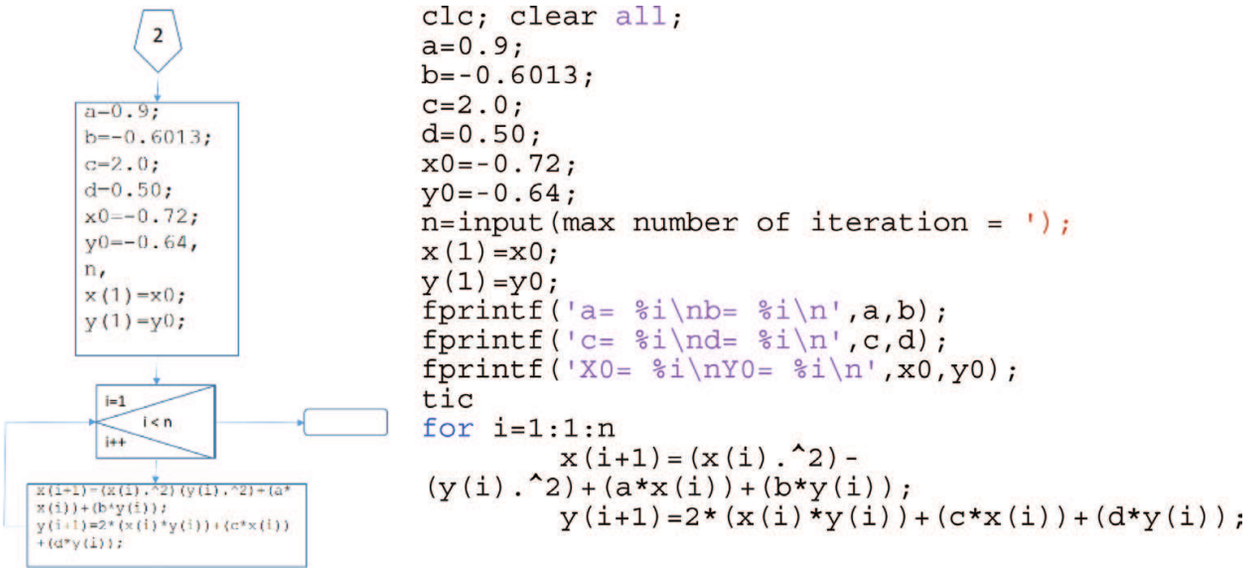

Figure 10. Algorithm by tent map.

http://dx.doi.org/10.5772/intechopen.75959

4. Conclusions

4.1. Operative systems and cryptography

Security is a priority since the operative systems are responsible to manage a multi-user and multi-programing environment. Complexity around these tasks involve goals for preventing unauthorized access, safeguarding users from undesirable results by their own actions, managing rights and abilities to cooperate, they also implies confidentiality, integrity and availability. Another thing to take on account is the network security which is responsible to protect the information that is exposed when it is transmitted between various computers. A solution for these problems have been tackled through hardware solutions however these solutions have proved to be expensive and, often times, impractical. Data encryption is a viable alternative solution to secure the information because cryptographic technology is, a relatively inexpensive and highly effective process to protect sensitive data against disclosure. By default, popular operative systems like Android, Linux, Mac OS and Microsoft Windows have cryptography technologies for enhancing their security systems in the way to protect sensible data, even some of the share their APIs with the objective to give tools for reducing risks related with data security.

4.2. Operative systems

Countries around the world like United Kingdom, Australia and United States of America are making respectable efforts directed specifically in the cyber security infrastructures. Most of them adopted international security standards of which stand out ISO/IEC 27032:2012, ISO/IEC 27001, ISO 22301, ISO/IEC 15408, ISO27799, ISO/IEC 27010 and they also have its own intern standards and specialized organizations as is the case of United Kingdom with the Network Interoperability Consultative Committee (NICC) and the Information Assurance Maturity Model (IAMM).

In the case of Mexico, the government has not adopted international standards yet and the legislation is distributed in different laws and norms because the way in which it is pursued depends on the nature of the crime. Regulations consider crimes like: separated into different laws like electronic commerce, electronic signature, personal data protection, right to the information, revelation of secrets, industrial property among others. This weakens people, companies and the government itself when they are the victims of an attack which has as a target the security of their data.

It is necessary to prepare the relevant technology for the cryptographic algorithms that work with Linux, in the Cluster infrastructure, to make the most of the benefits related to a complete information processing. While it is necessary to have logical security, you only need to work on the integration of technologies in schemes at the level nodes of the net, as is the case with the Internet of things (IoT) thus ensuring all kinds of information such as multimedia can be operated.

Author details

Arturo Lezama-León[1]*, José Juan Zarate-Corona[1], Evangelina Lezama-León[2], José Angel Montes-Olguín[3], Juan Ángel Rosales-Alba[3] and Ma. de la Luz Carrillo-González[3]

*Address all correspondence to: lezama@upp.edu.mx

1 Mathematics and Technology Sciences, Polytechnic University of Pachuca, Zempoala, Hidalgo, Mexico

2 Strategic Planning and Technology Management, Popular Autonomous University of the State of Puebla, Mexico

3 High Technological Institute Zacatecas Norte, Mexico

References

[1] Turing AM. Computing Machinery and Intelligence. Oxford Academic, Google Scholar Mind. 1 October 1950;**LIX**(236):433-460. DOI: 10.1093/mind/LIX.236.433. [Accessed: January 1, 2018]

[2] Russell S, Norvig P. Artificial Intelligence a Modern Approach. 2nd ed. Pearson Education Inc. Publishing as Prentice Hall; 2004. p. 1212. ISBN: 0-13-790395-2 [Accessed: January 2, 2018]

[3] Rich E, Knight K, Nair SB. Artificial Intelligence. 3rd ed. Mc Graw Hill. ISBN. 13: 978-0-07-0088770 [Accessed: January 3, 2018]

[4] Silva M. Las redes de Petri en la automática y la informática. AC; 1985. ISBN: 8472880451 [Accessed: January 4, 2018]

[5] KPMG International. Cyber Security Standards Compliance: A Vital Measure to Critical Infrastructure Protection. Printed in Malaysia. 2015 [Accessed: January 4, 2018]

[6] World Economic Forum. Insight Report Global Risks. 9th ed. 2014. ISBN 13: 92-95044-60-6. https://www.weforum.org/risks [Accessed: January 4, 2018]

[7] Torres & José. s.f. [Accessed: January 4, 2018]

[8] United Nations. 2016 [Accessed: January 4, 2018]

[9] California Department of Technology. 2014 [Accessed: January 4, 2018]

[10] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en [Accessed: January 4, 2018]

[11] https://www.iso.org/isoiec-27001-information-security.html [Accessed: January 4, 2018]

[12] https://www.nist.gov/cyberframework [Accessed: January 4, 2018]

[13] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf [Accessed: January 5, 2018]

[14] https://nccoe.nist.gov/ [Accessed: January 6, 2018]

[15] top500.org, published on November 2017 [Accessed: January 7, 2018]

[16] Fúster A, Hernández L, Martín A, Montoya F, Muñoz J. Criptografía, protección de datos y aplicaciones, 2013. ALFAOMEGA. ISBN 978-607-707-469-4 [Accessed: January 7, 2018]

[17] Painchaud M. Cryptography and its application to operating system security [thesis]. Rochester Institute of Technology; 1981 [Accessed: January 8, 2018]

[18] Arpaci-Dusseau RH, Arpaci-Dusseau AC. Operating systems: Three easy pieces. 2015. [Accessed: January 8, 2018]

[19] Morales Luna G. Criptografía: Seguridad en la información. CINVESTAV-IPN. 2006 [Accessed: January 9, 2018]

[20] Núñez R. El uso de la criptografía en el sistema operativo Android. 2016 [Accessed: January 9, 2018]

[21] The Linux Kernel. (s.f.). The Linux Kernel. Recuperado el 05 de January de 2017, de The Linux Kernel: https://www.kernel.org/doc/html/v4.12/crypto/intro.html#introduction. [Accessed: January 10, 2018]

[22] Apple Inc. Security. Recuperado el 18 de January de 2018, de Apple developer: https://developer.apple.com/security/. 2018 [Accessed: January 11, 2018]

[23] Microsoft. CNG Features. Recuperado el 18 de January de 2018, de Microsoft: https://msdn.microsoft.com/es-es/library/windows/desktop/bb204775(v=vs.85).aspx. 2018 [Accessed: January 12, 2018]

[24] Jopcroft JE, Motwani R, Ullman JD. Introduction to Automata Theory; Languages and Computation. 3rd ed. Published by Pearson Education, Inc. Publishing as Addison-Wesley. 2007. ISBN: 978-84-7829-088-8 [Accessed: January 12, 2018]

[25] Lezama-león A, Liceaga-Ortíz-de-la-Peña JM, Zarate-Corona JJ. IoT Equipment Security. Advances in Digital Technologies. In: Mizera-Pietraszko J et al. editors. IOS Press, 2017 © 2017 The authors and IOS Press. All rights reserved. DOI: 10.3233/978-1-61499-773-3-126. Vol. 295. Publishing by Frontiers in Artificial Intelligence and Applications (FAIA). ISBN: 1879-8314 [Accessed: January 13, 2018]

[26] González RC, Woods R, Eddins SL. Digital Image Processing Using Matlab. Pearson Education, Inc, Publishing as Prentice Hall; 2004. ISBN: 0-13-008519-7 [Accessed: January 14, 2018]

[27] Liceaga-Ortiz-De-La-Peña JM, Lezama-León A, Zarate-Corona JJ, Hernández-Terrazas RO. Politechnique University of Pachuca. The tent map, like various chaotic maps, as pseudorandom sequence generator. SIMCI 2013. Simposio Ibero Americano Multidisciplinario de Ciencias e Ingenierías [Accessed: January 14, 2018]

[28] Pérez JMX, León AL, de la Peña JMLO, Hernández Terrazas RO. Real Time Stereo Vision with a modified Census transform in FPGA. In: Proceedings of the IEEE International Conference on Electronics, Robotics and Automotive Mechanics Conference (CERMA), 2012. DOI: 10.119/CERMA.2012.23 [Accessed: January 15, 2018]

IntechOpen