International Journal of Computational Intelligence Systems
Vol. **13(1)**, 2020, *pp.* 604–623
DOI: https://doi.org/10.2991/ijcis.d.200430.001; ISSN: 1875-6891; eISSN: 1875-6883
https://www.atlantis-press.com/journals/ijcis/

Research Article

Using Fuzzy Logic Algorithms and Growing Hierarchical Self-Organizing Maps to Define Efficient Security Inspection Strategies in a Container Terminal

Leonela Morales[1], Luis Onieva[1,], Ventura Pérez[2], Pablo Cortés[1,*,]

[1]*Grupo Ingeniería de Organización, Escuela Técnica Superior de Ingeniería, Universidad de Sevilla, Camino de los Descubrimientos s/n, 41092, Sevilla (Spain)*
[2]*Dpto. Ingeniería Química y Ambiental, Escuela Técnica Superior de Ingeniería, Universidad de Sevilla, Camino de los Descubrimientos s/n, 41092, Sevilla (Spain)*

ARTICLE INFO

Article History
Received 27 Aug 2019
Accepted 04 Feb 2020

Keywords
Container terminal
Port: Security inspection
Fuzzy logic
Growing hierarchical self-organizing map

ABSTRACT

Maritime transport is one of the oldest methods of moving various types of goods, and it continues to have an important role in our modern society. More than 20 million containers are transported across the oceans daily. However, this form of transportation is constantly threatened by illegal operations, such as the smuggling of goods or people and merchandise theft. Port security departments must be prepared to face the different threats and challenges that accompany the use of innovative techniques and devices to achieve efficient inspection strategies. Two inspection strategies are presented in this study. The first strategy is based on fuzzy logic (FL), and the second strategy is based on the growing hierarchical self-organizing map (GHSOM) approach. The weight variation and security index (SI) of a container and the readings from certain technologies, such as radio-frequency identification (RFID) and X-ray scanning, are considered as the input data. To minimize the inspection time and considering the costs associated with the security inspections of containers, the results of both inspection strategies are compared and analyzed. The findings indicate there is potential for improving the effectiveness of security inspections by employing both techniques, and the specific relevance in the case of GHSOMs is discussed.

1. INTRODUCTION

Container transport has an important role in global supply chains and has become increasingly important around the world by contributing to economic development. However, considerable security vulnerabilities have emerged [1].

A container terminal is a complicated system with several interrelated components and different interconnected operations, such as security inspections, which should be harmoniously executed to avoid delays in the corresponding inspection times.

Security inspections can add costs, delays and uncertainties during the transport process. The disruptions in the supply chain caused by delays in the inspection area of a container terminal can be disastrous and have cascading consequences [1]. In addition, container transport can be used for illegal operations, such as the smuggling of goods and people, and can be employed by terrorist organizations to transport weapons of mass destruction or biohazards [2].

Port authorities are increasingly making demands regarding the data required for containers as they provide information about their content, country of originand shipping company. The daily analysis of container data can be a difficult process; thus, the following scientific question should be answered: *Is it possible to reduce the number of containers assigned to manual inspection in ports and simultaneously improve the systems for the detection of containers that transport illegal material via new technologies without increasing the cost or time spent on inspection?*

As a hypothesis based on this question, we propose that the use of artificial intelligence techniques, which have not yet been incorporated into the security inspection systems of container port terminals, can improve the process efficiency and possibly reduce or at least maintain the corresponding time and cost. Thus, the goal of this investigation is to demonstrate the possibility of increasing the detection of illegal containers (containers with illegal material or containers whose merchandise has been stolen) without increasing the cost or time of the inspection processes. The fusion of information and computational algorithms will enable the automatic identification of threats and the presentation of the relevant data to an operator to provide decision support regarding the classification of containers.

Methodologies that are based on artificial intelligence (fuzzy logic (FL) and the growing hierarchical self-organizing map (GHSOM)) and the extensive information associated with containers and their processes, including information from the technological devices that are currently used in their surveillance, are employed to develop tools for decision-making that automate the process and minimize manual inspections without reducing their reliability.

*Corresponding author. Email: pca@us.es

In addition, the use of the container weight as an additional decision variable in the early stages of the container inspection process is a novel proposal that arises from the new regulations that have been promoted by the International Maritime Organization (IMO) since 2016 as part of the new implemented measures for the verification of the gross mass of full containers in the Safety of Life at Sea (SOLAS) convention. These measures have been put in place due to the numerous container ship accidents caused by the excessive weight of containers. Consequently, this information could be appropriately integrated into the inspection strategy in the near future.

In this way, two new inspection strategies are developed based on FL and GHSOM methods. In our case, these strategies employ the container information along with the innovative use of the weight readings (which are currently not incorporated into security procedures) and container security indices (SIs) as well as radio-frequency identification (RFID) and nonintrusive technologies.

There is some scientific literature that deals with RFID technology [3], the SI of containers and nonintrusive inspection techniques for containers (e.g. see the English and Zuver [4]). However, the integration of these elements in one approach has not been addressed. In addition, the consideration of the FL and GHSOM approaches is novel in the scientific literature regarding their application to container inspection at ports.

The structure of the paper is as follows: A literature review of the related studies is presented in Section 2. Section 3 presents a general inspection strategy, and Section 4 details the FL and GHSOM methods. The procedures for generating the experimental data are explained in Section 5, and the results of both models are presented in Section 6. In Section 7, the discussion and final conclusions are provided.

2. LITERATURE REVIEW

The process by which security inspections are performed in container terminals is important because this process affects both the maritime supply chain and the associated costs. In this section, a scientific literature review of the inspection processes in container port terminals and the FL and GHSOM approaches is presented.

2.1. Container Inspection in Port Terminals

Among the different operations performed in a container terminal, the security inspection is one of the most important operations. The delays in the inspection area of a container terminal are primarily attributed to the manual inspection of containers. As these manual inspections require several hours per container, the manual inspection of all the containers is not viable in terms of the general efficiency of container terminal operations. Classifying the containers using a certain inspection strategy helps to reduce the number of containers that will be manually inspected, thereby reducing the time of the operations in the container terminal. By investigating different algorithms, methods and approaches, as well as the implementation of FL, we were able to improve the classification of containers and minimize the inspection times and costs.

Bakshi *et al.* [5] analyzed the impact of two important inspection initiatives: the Container Security Initiative (CSI) and the Security Freight Initiative (SFI). Boros *et al.* [6] developed a linear decision tree model to obtain the optimum sequences of inspection strategies. Boros *et al.* [7] considered a combination of decision trees and inspection systems by enumerating efficient inspection policies. Longo [8] designed operationally effective practices and policies to improve the flow of containers both toward the inspection zone and within the normal operations of a container terminal. Lee *et al.* [9] presented a genetic algorithm for optimizing the percentage of containers that are examined and the sequence of the container movements, which minimizes time-delay costs. Harris *et al.* [10] performed simulations to determine the necessary inspection resources for minimizing the interruption caused by an increase in security inspections in a container terminal.

Elsayed *et al.* [11] presented several optimization approaches to simultaneously determine the optimal levels of the sensor threshold and the sequence of the inspection. Young *et al.* [12] presented a study that corresponds to an extension of the study by Elsayed *et al.* [11], in which, unlike the latter, they present a multiobjective optimization approach for determining the optimal management of sensors and their threshold levels, considering the total costs. van Weele and Ramirez-Marquez [13] presented an optimization technique for developing an inspection strategy that establishes an inspection rate of suspect containers that minimizes the inspection costs. Riahi *et al.* [14] employed a dataset to establish the values of the reliability percentages, both for the country of origin and the shippers and container terminals; they obtain the SIs of the containers.

Ramirez-Marquez [15] presented an inspection strategy that introduces different types of reliability and cost measures. An evolutionary optimization approach that is known as a probabilistic solution discovery algorithm is applied to generate an optimal inspection strategy.

Concho and Ramirez-Marquez [16] developed a holistic evolutionary algorithm for identifying the optimal threshold values for every sensor and the optimal configuration for the inspection strategy. Ma *et al.* [17] employed the maximum likelihood (ML) estimation method to identify the efficiency factors for inspection, which improves the quarantine and clearance processes of the containers in a port. Wang *et al.* [18] developed a stylized queueing model with novel features related to the security checkpoints to analyze policy initiatives. Wang *et al.* [19] discussed an inspection investment planning problem for the international container terminal at the Dalian Port using a simulation method. They proposed a framework that combines an arena-based simulation model that considers various types of container ships and flexible container truck scheduling and routing.

Table 1 presents a summary of the investigations regarding the optimization methods for improving the security of a container terminal.

2.2. Fuzzy Logic

FL allows us to deal with nonaccurate information by considering the data as fuzzy sets. The fuzzy sets combine different rules to define the actions. Thus, control systems based on FL are able to

Table 1 Approaches for improving the security of a container terminal.

Reference	Modeling (Algorithms)	Experimental Data Size	Main Contribution
[5]	Simulation models	Two container terminals	Effect of inspections on the flow of containers
[6]	Algorithms Mathematical models	Container inspections in container terminals	Minimize the inspection costs and inspection error rate
[5]	Decision trees Dynamic programming algorithms	Port inspections represented by decision trees	Establish some effective properties for inspection systems, which minimize the cost
[16]	Holistic evolutionary algorithm General decision tree model	Container inspection strategy	Minimize the total cost of inspection while maintaining a user-specified detection rate for "suspicious" containers
[11]	Port-of-entry problem	Small number of inspection stations	Optimal sensor threshold levels
[10]	Process model Triangular distribution Simulations Sensitivity analysis	Alabama Container Terminal	Minimize the interruptions from the increased security inspections of containers in a terminal
[9]	Genetic algorithm	Operations of a container terminal	Optimize the inspection process and the sequence of the movements of containers in the yard; minimize the total costs
[8]	Simulation models Design of experimental techniques Variance analysis	Container terminal	Integration of the security procedures in the normal operations of the container terminal
[17]	Factor conception model Structural equation model	Inspection and quarantine clearance efficiency in Shanghai, China	Provide a theoretical basis for the analysis of the internal economic effectiveness
[15]	(n + 1)-echelon decision tree General decision tree model	Container inspections in container terminals	Minimizes the total cost of inspection while maintaining a user-specified detection rate for "suspicious" containers
[14]	Bayesian network (BN) Analytic hierarchy process (AHP)	Case study	Evaluate the security score of a container
[20]	Genetic algorithms Decision tree	Modeling of security inspections with four types of sensors	Inspection rates for suspicious containers
[18]	Queueing model with novel features	Security-check waiting lines for screening cargo containers	Provide a modeling framework to understand the economic trade-offs embedded in the container-inspection decisions
[19]	Arena-based simulation model Visual Basic for Applications Simulation experiments	International container terminal at Dalian Port	Address an inspection investment planning problem for the international container terminal at Dalian Port using a simulation method
[12]	Port-of-entry problem Multiobjective optimization Analysis of variance (ANOVA)	They considered two suspect containers per 10,000 containers	Determine the optimal levels of sensor layouts and thresholds

combine the input variables by applying groups of rules that lead to one or more output values [21].

Systems based on FL can be applied to nonlinear or partially defined problems as neural networks. However, in contrast to neural networks, FL allows for the easy implementation of expert knowledge by formalizing the sometimes ambiguous knowledge of experts. In addition, FL allows for the design of inexpensive and quick control and decision systems.

The application of an FL algorithm can be described by the following three steps:

- Fuzzification, where the input values are converted to fuzzy values
- Inference, which is a process based on the logic rules
- Defuzzification, where the fuzzy variables are reconverted, and a decision is made

FL has been used as a tool for processing large amounts of information, in which the data can have an associated degree of partial set membership. FL methods are the main actors in some investigations of system control; in other studies, FL methods aid in decision-making.

In Starczewski [27], an efficient fuzzy logic system (FLS) that is based on triangular type-2 fuzzy sets is designed. This FLS provides a new method for reducing computational complexity in t-norm operations that is extended to triangular type-2 fuzzy sets. Motepe

et al. [26] presented an FL method and experimental investigation. This study was associated with real measurements of the South African power system network. Magudeeswaran and Ravichandran [25] presented an FL-based histogram equalization (FHE) method to enhance image contrast to highlight the details of a hidden image or increase the image contrast with a new dynamic range.

Liang *et al.* [24] used fuzzy set theory to construct an optimum output quantity decision model to obtain the maximum profit of a duopoly market. Huerta *et al.* [22] presented an FL-based preprocessing approach that consists of two main steps. First, the approach employs fuzzy inference rules to transform the gene expression levels of a given dataset into fuzzy values. Second, the approach applies a similarity relation to the fuzzy values to define the fuzzy equivalence groups. Each group contains similar genes, which assists with the selection of an essential subset of genes for the classification and analysis of microarray data. Hsueh [23] used the Delphi method and FL theory to develop a quantification assessment model that is based on the qualitative analysis used to evaluate the results and influences of participation in environmental protection education and green community development by residents of the Taiwan community.

Table 2 presents a summary of the investigations regarding the FL method.

2.3. The SOM and GHSOM

Self-organizing maps (SOMs) were developed by Teuvo Kohonen in the 1990s (see Kohonen [28] for a good introduction to SOMs) as a continuation of the competitive networks proposed by Von Der Malsburg. SOM networks have been successfully applied to a large variety of problems, such as pattern classification, size reduction, process monitoring and data mining, among others [21].

A SOM obtains the statistical characteristics of the input data which is then applied to a wide data classification field [29]. However, the effectiveness of traditional SOM models is limited by the following issues:

- Problems related to their statistical topology and their inability to represent the hierarchical relationships in the input data [30–35].
- The size and dimensionality of the SOM model, which is corrected prior to the training process and determined by trial and error [30–33,35,1].

The GHSOM approach seeks to overcome these problems [30–32,36,34,33,37].

The GHSOM has an adaptive architecture without supervision that focuses on clustering data. When the distribution of the data increases in a hierarchical manner, the approach allows for its hierarchical decomposition and exploration of the data clusters in a horizontal manner [38]. This self-organizing model (GHSOM) has a hierarchical architecture that is divided into layers; each layer is composed of different SOMs, and the size of each SOM is automatically determined during the unsupervised learning process [34]. The main advantage of a GHSOM compared with a traditional SOM is that the trial and error are removed from the training process. An ideal topology is formed in an unsupervised manner based on the training data [33].

Palomo *et al.* [34] presented a new approach for analyzing and visualizing network forensics data (network forensics is an area of research that collects information regarding crimes that involve digital evidence) based on GHSOMs. Ippoliti and Zhou [33] proposed an adaptive GHSOM approach (AGHSOM) for network anomaly detection. Chattopadhyay *et al.* [31] proposed a GHSOM that improves the cell formation problem (CFP) of a cellular manufacturing system. Chan and Pampalk [30] developed a GHSOM Toolbox for MATLAB, which has an advantage in visualization due to its capability of presenting classes and subclasses of similar data. By combining the GHSOM with mutual information, Zhang *et al.* [37] proposed a new intrusion detection method for detecting unknown network attacks.

Table 3 provides a summary of investigations on the SOM and GHSOM approaches.

Table 2 Approaches for fuzzy logic method.

Reference	Modeling (Algorithms)	Experimental Data Size	Main Contribution
[22]	Fuzzy logic	Analysis of microarray data	Gene selection
[23]	Fuzzy logic	Community residents' participation in environmental protection education	Assess the results and influences of community residents' participation in environmental protection education on green community development
[24]	Fuzzy decision environment	Duopoly market	Construct an optimum output quantity decision model that aims to maximize the profit of a duopoly market
[25]	FL-based histogram equalization	Images	Unveil the hidden image details or increase the image contrast with a new dynamic range
[26]	FL	South African power systems network	Determine a distribution power systems' loading measurement accuracy
[27]	FLS based on triangular type-2 fuzzy sets	t-norm operations	Provide a new method for computational complexity reduction in t-norm operations extended to triangular type-2 fuzzy sets

FL, fuzzy logic; FLS, fuzzy logic system.

In Section 2.1, the different investigations within the optimization field for improving the security inspections in port terminals were analyzed. Although different models, simulations and optimization designs have been employed to achieve an optimal inspection strategy, the inspection strategies based on FL or SOM and GHSOM approaches have not been designed considering the container weights as input data, which is our research contribution. Both strategies are compared and analyzed to obtain the most efficient inspection strategy when classifying the containers as follows: suspicious containers will be manually inspected; probably suspicious containers will be inspected by X-ray scanning; and not suspicious containers will be released to continue their path through the container terminal.

3. THE INSPECTION STRATEGY

The following values were employed for this investigation: the weight variation (ΔW) among the containers; the values provided by the RFID technology that indicate if the container could have been opened; the SI values from Riahi *et al.* [14], which are shown in Table 4; and the values obtained from the simulation of X-ray scanning at the control points. These variables are combined to design an efficient algorithm that is able to overcome the limitations of considering each variable in an independent and individualized way and provide a very satisfactory classification of containers (suspicious and nonsuspicious).

Safety management regulation is an important complement to market forces to establish a sufficient safety level in high-risk industries [39], which explains why the IMO implemented measures for the verification of the gross mass of full containers in the SOLAS convention [40] due to the numerous container ship accidents caused by the excessive weight of containers. The new regulation, which has been in effect since July 1, 2016, seeks to avoid accidents caused by an improper weight distribution by requiring the verification of the container weights. This information is reflected in the documentation. These regulations enable the use of the container

Table 3 Approaches for SOM and GHSOM.

Reference	Modeling (Algorithms)	Experimental Data Size	Main Contribution
[30]	GHSOM Toolbox for MATLAB	Determine the size of the SOM Presenting classes and subclasses of similar data	Development of the GHSOM Toolbox for MATLAB
[31]	SOM approach GHSOM	CFP of cellular manufacturing system	Development of optimum machine-part cell formation algorithms
[32]	GHSOM	Set of data	Grow in terms of map size and a three-dimensional tree-structure to represent the hierarchical structure in a data collection during an unsupervised training process
[36]	Growing hierarchical tree SOM (GHTSOM)	Set of Internet meaning data	Allow the network to adapt the topology of each layer of the hierarchy to the characteristics of the training set
[33]	AGHSOM	Set of online data	Network anomaly detection
[34]	GHSOM	Network forensics	Improve the visualization of network traffic data
[37]	GHSOM method	Set of data	Clustering of input data

SOM, self-organizing maps; GHSOM, growing hierarchical self-organizing map; CFP, cell formation problem.

Table 4 Security percentages of the countries of origin and carriers/ports.

Reliability value of the country of origin	Reliability value an ocean carrier and a landing port										
	100%	97%	94%	91%	88%	85%	84%	83%	82%	81%	80%
100%	**0.8466**	**0.8326**	**0.8186**	**0.8047**	**0.7907**	**0.7767**	**0.7721**	**0.7674**	**0.7628**	**0.7581**	**0.7535**
98%	**0.8387**	**0.8248**	**0.811**	**0.7971**	**0.7833**	**0.7694**	**0.7648**	**0.7602**	**0.7556**	**0.7510**	0.7463
96%	**0.8307**	**0.8170**	**0.8032**	**0.7895**	**0.7758**	**0.7620**	**0.7574**	**0.7529**	0.7486	0.7437	0.7391
94%	**0.8227**	**0.8091**	**0.7955**	**0.7818**	**0.7682**	**0.7546**	**0.7501**	0.7455	0.741	0.7365	0.7319
92%	**0.8147**	**0.8012**	**0.7877**	**0.7742**	**0.7607**	0.7472	0.7427	0.7382	0.7337	0.7292	0.7247
90%	**0.8067**	**0.7933**	**0.780**	**0.7666**	**0.7532**	0.7398	0.7353	0.7309	0.7264	0.722	0.7175
88%	**0.7987**	**0.7855**	**0.7722**	**0.7589**	0.7457	0.7324	0.7280	0.7236	0.7191	0.7147	0.7103
86%	**0.7907**	**0.7776**	**0.7644**	**0.7513**	0.7381	0.725	0.7206	0.7162	0.7118	0.7075	0.7031
84%	**0.7827**	**0.7697**	**0.7567**	0.7436	0.7306	0.7178	0.7132	0.7089	0.7046	0.7002	0.6959
82%	**0.7748**	**0.7618**	0.7489	0.736	0.7231	0.7102	0.7059	0.7016	0.6973	0.6930	0.6887
80%	**0.7667**	**0.7539**	0.7411	0.7284	0.7156	0.7028	0.6985	0.6942	0.69	0.6857	0.6815
78%	**0.7587**	0.7461	0.7334	0.7207	0.708	0.6954	0.6911	0.6869	0.6827	0.6785	0.6742
76%	**0.7507**	0.7382	0.7256	0.7131	0.7005	0.6880	0.6838	0.6796	0.6754	0.6712	0.667

weight as input data for our investigation; this variable has not been included in inspection strategies for decision-making.

The RFID technologies are very reliable but cannot guarantee 100% security, which indicates that an inspection strategy based on RFID technologies would not provide optimal results when classifying containers as suspicious or not suspicious. In addition to these technologies, the container weights and other technologies and indicators will be considered in this study.

- The RFID technologies have the following limitations [41]:
- The collisions that occur when trying to simultaneously read several tags cause data loss.
- The RFID tags can be damaged during container transport.
- The weather conditions can affect the RFID tag and cause the transmission of inaccurate readings regarding the opened or closed condition of the container.

The containers that are considered to be suspicious can be subjected to X-ray scanning as in the image discrimination system proposed by [42], where the theory of using two X-ray energies (E_1 and E_2) was developed to analyze objects and extract their atomic information. This system enables the load of a container to be classified according to the image attenuation range and will therefore provide a final classification of the containers; suspicious containers will require a manual inspection, while the not suspicious containers will be cleared from the container terminal.

Dual-energy imaging comprises a technique that scans objects with dual X-ray energy layers, E_1 and E_2. In our case, the attenuation coefficients of $E_1 = 10$ MeV and $E_2 = 6$ MeV are employed (MeV – Megaelectron-volt), which are the values provided by the National Institute of Standards and Technology (NIST, U.S.)

3.1. The General Inspection Strategy

Inside a container terminal, all the containers undergo an initial inspection, the results of which are used to classify them as "suspicious" or "not suspicious." Based on this classification, a container will be subjected to additional controls that will enable its entrance or clearance or determine whether it has to be manually inspected.

The use decision trees for inspection strategies was first suggested by Boros *et al.* [6], later in a more general way the process was represented as a decision tree by Van Weele and Ramirez-Marquez [20], where the results of each inspection determine the path of the container through the tree.

The decision tree models presented in this document consider different factors in the inspection process to improve the strategy, such as the weight and security score of a container and the RFID readings. The decision trees for each optimization method are shown in Figures 1 and 2.

Both trees are similar for the inspection and classification of a container. As shown in Figure 1, the largest difference between the two strategies is that the RFID reading from the container is analyzed in node 1 to indicate if the container has been opened during transit. If the container was opened, it is classified as a suspicious container

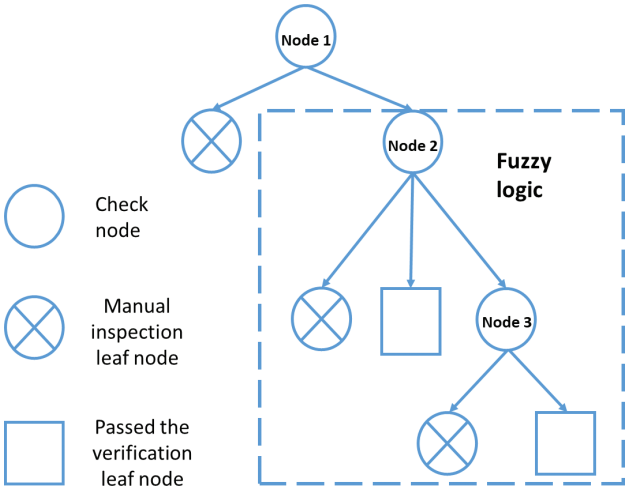

Figure 1 | Decision tree for the FL-based inspection strategy.

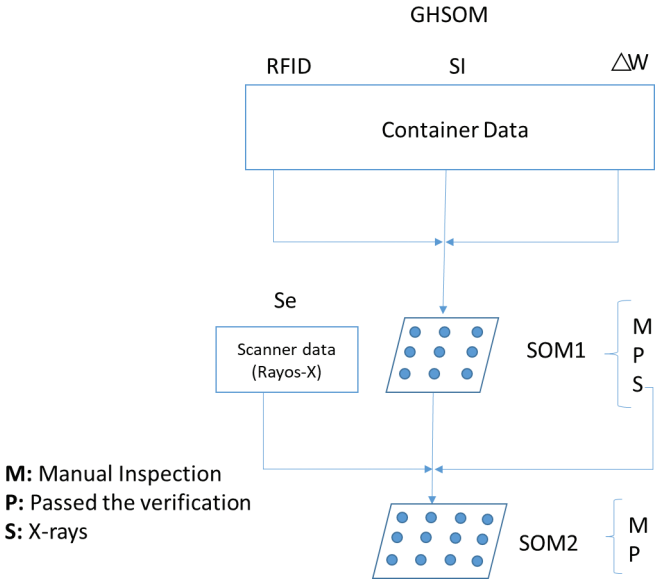

Figure 2 | Decision tree of the GHSOM-based inspection strategy.

and will directly undergo manual inspection; otherwise, it will be classified as probably suspicious and will pass to node 2, where the classification of the container can be obtained by analyzing the container input data, such as the weight variation (ΔW) and the *SI*) values, by applying FL. In this manner, the containers will be classified as suspicious, not suspicious and probably suspicious and will pass to node 3 where the weight variation, SI data and X-ray results (Se) will be reanalyzed by FL.

This separation of the variables in the decision tree is attributed to the fuzzy nature of the three measures (weight variation, SI and X-ray results), which contrasts the use of the binary RFID variable.

To generate the first GHSOM or SOM 1 level, the input data, which consists of the weight variation, SI values and the RFID readings, as shown in Figure 2, are simultaneously analyzed in the first step. Thus, first, the containers are classified into three sets: M, for the containers that are suspicious that will directly proceed to manual inspection; P, for containers that are not suspicious, which will leave the inspection area; and S, for the containers that will be

subjected to X-ray scanning, since there is not sufficient information to determine if they are suspicious. The SOM is employed for data clustering and visualization, which enables the classification of the variables regardless of whether they are fuzzy or not.

4. DECISION SUPPORT METHODOLOGIES FOR SECURITY INSPECTION BASED ON ARTIFICIAL INTELLIGENCE

In this section, we detail the proposed methodology for security inspection strategies based on the FL and GSHOM approaches.

4.1. The FL Model

The proposed inspection strategy FL-based process is explained next.

As indicated, *FL* is an artificial intelligence technique that facilitates or enables working with information that is inaccurate and poorly defined. *FL* is used as a calculation tool for truth criteria; it is based on a scale of values from the falsest value to the truest value and provides a quantitative result that ensures the selection of an alternative that is closest to the truth and considers the attributes that it satisfies as a basis to attain a certain goal [43]. In this manner, *FL* is a robust method that does not require a substantial amount of information.

We will use FL to sharpen the inspection strategy results. The input data, weight variation (ΔW) and security score (SI) are considered in nodes 2 and 3, where a new data input will be added for the X-ray (Se) information to obtain a final classification that minimizes the inspection times and the manual inspections.

4.1.1. The data and variables of the *FL* model

In the model of Figure 1, node 1 is a classic logic decision. If a container has been opened, it will be manually inspected. If a container has not been opened, it will proceed to node 2, where it will be classified again due to the fuzzy algorithm. The variables to be analyzed by the algorithm in nodes 2 and 3 of the decision tree are defined in the following section.

The structure followed during the decision processes starts with the statement of the input and output variables. Then, the membership functions for each input are explained, and the fuzzy linguistic variables are detailed by means of the structure rules (IF x AND y THEN z) creating the rule matrix. Finally, to solve the problem we make use of the Root-Sum-Square (RSS) method.

The calculations for all the fuzzy variables were performed using the MATLAB Fuzzy Toolbox. This toolbox allows the creation and editing of fuzzy inferences with graphical tools or command line functions; they can also be generated with the adaptive cluster techniques in the toolbox.

4.1.2. Decision process in node 2

Two fuzzy variables are defined: the weight and security score of the container:

ΔW: the weight variation

SI: the container security index

where the output will be

P: If the container is not suspicious

Sc: If the container is probably suspicious

M: If the container is suspicious

- ***System states***

Input 1: the weight variation

The weight variation input variable, ΔW, is constructed for each container, C_j, by using two weight values: W_{0j} and W_{1j}, where W_{0j} is the weight value of a container at the origin (first measurement of the container weight), and W_{1j} is the weight value at the destination port (last measurement of the container weight). This variable evaluates if the weight of container C_j has changed during the trip from the origin to the destination. This fact can alert against the theft of goods in case of a reduction of the original container weight, that is $W_{1j} \leq W_{0j} - \tau$; or alert against suspicious (and possibly illegal) introduction of goods in the container during the trip when $W_{1j} \geq W_{0j} - \tau$, being τ a tolerance threshold. Consequently, we define the following three cases:

$$-R \text{ if container } C_j \text{ weighs less } \left(W_{1j} \leq W_{0j} - \tau\right) \quad (1)$$

$$Z \text{ if the weight of container } C_j \text{ did not vary } \left(\left|W_{0j} - W_{1j}\right| < \tau\right) \quad (2)$$

$$+R \text{ if container } C_j \text{ weighs more } \left(W_{1j} \geq W_{0j} + \tau\right) \quad (3)$$

where τ is the boundary of the weight sensor threshold. For the case study, τ is set to 250 kilograms, as suggested in the OIMLR 60 regulation of the International Organization of Legal Metrology as an appropriate threshold given the size of the containers.

A variation between the values above the threshold suggests that the container should be considered as suspicious. This could be due to an increase in the weight (that could be associated with adding some illegal goods for smuggling) or a decrease in the weight (that could be associated with the theft of goods from the container).

Input 2: container SI

The container *SI* will be

$$S \text{ If the security score of container } C_j \text{ is high, then it is safe} \quad (4)$$

$$Z \text{ If the security score of container } C_j \text{ is intermediate} \quad (5)$$

$$R \text{ If the security score of container } C_j \text{ is low, then it is risky} \quad (6)$$

Figure 3 shows the membership function according to the weight variation and SI values and the defuzzification function for determining the output of node 2.

Table 5 presents the matrix of rules that determines the membership.

Structure rules and the rule matrix

$$R1: \text{ If } W = -R \text{ and } SI = S \text{ then output} = M$$

$$R2: \text{ If } W = Z \text{ and } SI = S \text{ then output} = P$$

$$R3: \ If\ W = +R\ and\ SI = S\ then\ output = M$$

$$R4: \ If\ W = -R\ and\ SI = Z\ then\ output = M$$

$$R5: \ If\ W = Z\ and\ SI = Z\ then\ output = Sc$$

$$R6: \ If\ W = +R\ and\ SI = Z\ then\ output = M$$

$$R7: \ If\ W = -R\ and\ SI = R\ then\ output = M$$

$$R8: \ If\ W = Z\ and\ SI = R\ then\ output = Sc$$

$$R9: \ If\ W = +R\ and\ SI = R\ then\ output = M$$

The RSS method is applied to solve the system. This approach combines the effects of all the rules, scales the functions according to their dimensions and calculates the fuzzy centroid of the composed area.

Using the RSS approach, the values of the probably suspicious containers (Sc) can be obtained using Equation (7); the values of the not suspicious containers (P) can be obtained using Equation (8); and the values of the suspicious containers (M) can be obtained using Equation (10). These equations are incorporated into the defuzzification function for the final decision (Figure 3c).

$$RSS_{Sc} = \sqrt{\sum_{i=1} nR_i^2} \qquad if\ R_i = SC \tag{7}$$

$$RSS_P = \sqrt{\sum_{i=1}^{n} R_i^2} \qquad if\ R_i = P \tag{8}$$

$$RSS_M = \sqrt{\sum_{i=1}^{N} R_i^2} \qquad if\ R_i = M \tag{9}$$

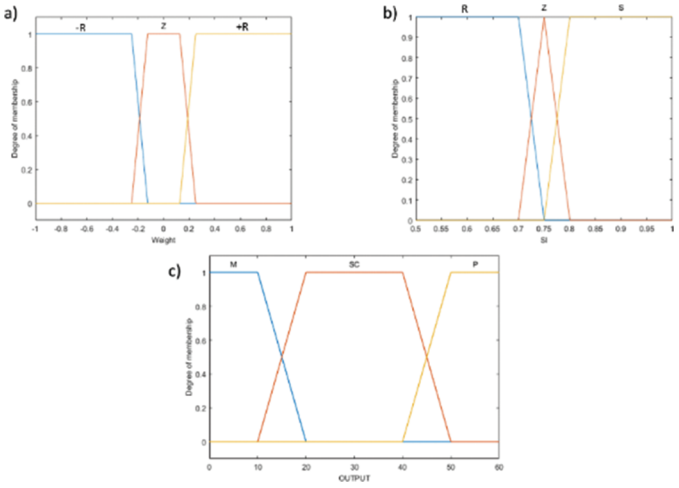

Figure 3 | a) Membership function for the weight variation, W; b) Membership function for the SI of a container; c) Output of node 2.

Table 5 | Rule matrix for Node 2.

		W		
		$-R$	Z	$+R$
SI	S	R1=M	R2=P	R3=M
	Z	R4=M	R5=Sc	R6=M
	R	R7=M	R8=Sc	R9=M

4.1.3. Decision process in node 3

After passing through node 2, all the containers that are classified as probably suspicious will be inspected by a nonintrusive X-ray scan in node 3, where they will be classified again using the *FL* model, considering their weight, security score and X-ray result. The containers will be classified into suspicious or nonsuspicious.

For node 3, input 1 and input 2 (the weight variation and SI of a container, respectively) will be the same as in node 2. The container will be scanned by X-ray and a new input is defined for the X-ray analysis data and the output of node 3.

where

Se: X-ray scanning result

The output will be as follows:

P: For the containers that pass the inspections

M: For the containers that will undergo a manual inspection

- ***System states***

Input 3: X-ray scanning result

The X-ray scanning result will be

$$S \text{ If container } C_j \text{ is considered safe} \tag{10}$$

$$Z \text{ If container } C_j \text{ is considered intermediate} \tag{11}$$

$$R \text{ If container } C_j \text{ is considered risky} \tag{12}$$

Figure 4 represents the membership functions according to the values of the weight variation, SI and the X-ray scanning result. Figure 5 shows the defuzzification function for determining the output of node 3.

Table 6 presents the matrix of rules that determine the membership.

4.1.4. Structure rules and the rule matrix

$$R11: \ If\ Se = R\ and\ W = -R\ and\ SI = S\ then\ output = M$$

$$R12: \ If\ Se = R\ and\ W = Z\ and\ SI = S\ then\ output = M$$

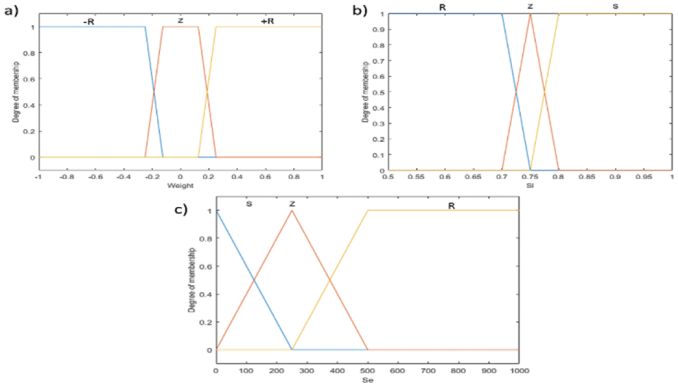

Figure 4 | a) Membership function for the weight variation ΔW; b) Membership function for the SI of a container; c) Membership function for Se.

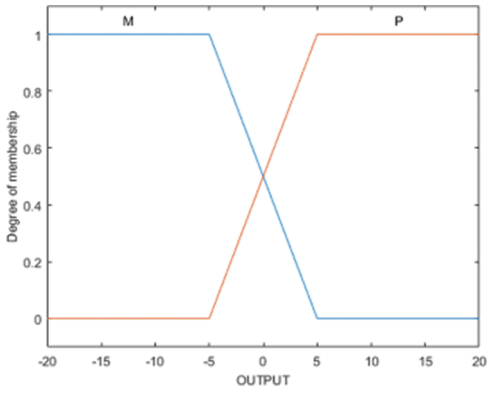

Figure 5 | Output of node 3.

Table 6 | Structure of rules for node 3.

	W			
SI	Se=R	$-R$	Z	$+R$
	S	R11=M	R12=M	R13=M
	Z	R14=M	R15=M	R16=M
	R	R17=M	R18=M	R19=M

	W			
SI	Se=Z	$-R$	Z	$+R$
	S	R21=M	R22=P	R23=M
	Z	R24=M	R25=P	R26=M
	R	R27=M	R28=P	R29=M

	W			
SI	Se=S	$-R$	Z	$+R$
	S	R31=M	R32=P	R33=M
	Z	R34=M	R35=P	R36=M
	R	R37=M	R38=P	R39=M

$R13: If\ Se = R\ and\ W = +R\ and\ SI = S\ then\ output = M$

$R14: If\ Se = R\ and\ W = -R\ and\ SI = Z\ then\ output = M$

$R15: If\ Se = R\ and\ W = Z\ and\ SI = Z\ then\ output = M$

$R16: If\ Se = R\ and\ W = +R\ and\ SI = Z\ then\ output = M$

$R17: If\ Se = R\ and\ W = -R\ and\ SI = R\ then\ output = M$

$R18: If\ Se = R\ and\ W = Z\ and\ SI = R\ then\ output = M$

$R19: If\ Se = R\ and\ W = +R\ and\ SI = R\ then\ output = M$

$R21: If\ Se = Z\ and\ W = -R\ and\ SI = S\ then\ output = M$

$R22: If\ Se = Z\ and\ W = Z\ and\ SI = S\ then\ output = P$

$R23: If\ Se = Z\ and\ W = +R\ and\ SI = S\ then\ output = M$

$R24: If\ Se = Z\ and\ W = -R\ and\ SI = Z\ then\ output = M$

$R25: If\ Se = Z\ and\ W = Z\ and\ SI = Z\ then\ output = P$

$R26: If\ Se = Z\ and\ W = +R\ and\ SI = Z\ then\ output = M$

$R27: If\ Se = Z\ and\ W = -R\ and\ SI = R\ then\ output = M$

$R28: If\ Se = Z\ and\ W = Z\ and\ SI = R\ then\ output = P$

$R29: If\ Se = Z\ and\ W = +R\ and\ SI = R\ then\ output = M$

$R31: If\ Se = S\ and\ W = -R\ and\ SI = S\ then\ output = M$

$R32: If\ Se = S\ and\ W = Z\ and\ SI = S\ then\ output = P$

$R33: If\ Se = S\ and\ W = +R\ and\ SI = S\ then\ output = M$

$R34: If\ Se = S\ and\ W = -R\ and\ SI = Z\ then\ output = M$

$R35: If\ Se = S\ and\ W = Z\ and\ SI = Z\ then\ output = P$

$R36: If\ Se = S\ and\ W = +R\ and\ SI = Z\ then\ output = M$

$R37: If\ Se = S\ and\ W = -R\ and\ SI = R\ then\ output = M$

$R38: If\ Se = S\ and\ W = Z\ and\ SI = R\ then\ output = P$

$R39: If\ Se = S\ and\ W = +R\ and\ SI = R\ then\ output = M$

The RSS method is applied to solve the system and obtain the values of the suspicions containers (M) in Equation (13) and not suspicious containers (P) in Equation (14), which are incorporated into the defuzzification function for the final decision (Figure 5):

$$RSS_M = \sqrt{\sum_{i=1,j=1}^{n} R_{ji}^2} \qquad if\ R_{ij} = M \tag{13}$$

$$RSS_P = \sqrt{\sum_{i=1,j=1}^{n} R_{ji}^2} \qquad if\ R_{ij} = P \tag{14}$$

4.2. The GHSOM Model

As previously explained, the GHSOM rules are networks formed by several SOM networks whose size is automatically determined during the unsupervised learning process [34]. In this section, their operation and implementation are described, beginning with the SOM network training process.

4.2.1. SOM network training

A SOM is an unsupervised neural network model that can be used for data clustering and visualization applications [44]. An SOM can project high-dimension patterns onto a low-dimension topology map. The SOM maps consist of a one-dimensional (1D) or two-dimensional (2D) node grid. These nodes are also referred to as neurons. The weight vector of each neuron has the same dimension as the input vector.

These neural networks classify the unsupervised input data, and their architecture consists of two layers: the first layer, which is also called the competition layer, consists of the learning nodes, which contain information about the resulting representation, and the input nodes, which represent the original vectors during the training process. All the elements of the first layer are connected to all the elements of the second layer.

Figure 6 shows the basic structure of an SOM network, where W_{ij} represents the weights assigned to each node of the competition layer, and x_n represents the input nodes.

The classic SOM network learning algorithm can be formulated as follows (for an in-depth analysis of the algorithm, refer to [45]):

The synaptic weights, W_{ijk}, are initialised as small absolute values or, in our case, default values. An input neuron vector, $x_n\,(x_1,\ x_2,\ \ldots x_n)$, is randomly chosen. The winner neuron is determined by calculating the Euclidean distance between the previously chosen input neuron vector, X, and the synaptic weight vector

$$d^2\left(W_{ij}, X\right) = \sum_k \left(W_{ijk} - x_k\right)^2 \tag{15}$$

Equation (15) determines the Euclidean distance between the synaptic weight vector and the input, where W_{ijk} represents the synaptic weights, and x_k is the input. Then, the winner neuron, g, is chosen as the neuron with the shortest distance to the input neuron vector, X.

The synaptic weights of the winner neuron and its neighboring neurons are actualized according to the weight actualization rules.

$$W_{ijk}\,(t+1) = W_{ijk}\,(t) + \propto (t)\, h\left(\left(i-g\right),\ t\right)\left(x_k\,(t) - W_{ijk}(t)\right) \tag{16}$$

where $\propto\ (t)$ represents the learning rate and $h\left(\left(i-g\right),\ t\right)$ represents the neighborhood function.

The learning rate determines the neuron weight variation; it is a time-decreasing function that is actualized with a linear function and its values fall between 0 and 1.

$$\propto (t) = \propto_0 + \left(\propto_f + \propto_0\right)\frac{t}{t_\propto} \tag{17}$$

where $\propto_0$ is the initial learning rate, $\propto_f$ is the final learning rate, and $t_\propto$ is the maximum number of iterations.

The neighborhood function is used to determine which neurons, i, are neighbors of the winner neuron, g, for each iteration t.

$$|i-g| = \sqrt{(i-g1)^2 + (i-g2)^2} \tag{18}$$

The neighborhood function, h, decreases with time and depends on a parameter called the neighborhood radius (t), which represents the size of the current neighborhood.

The simplest representation for the neighborhood function is step-like:

$$h\left(|i-g|, t\right) = \begin{cases} 0, & si\ |i-g| > R(t) \\ 1, & si\ |i-g| \le R(t) \end{cases} \tag{19}$$

A neuron is in the neighborhood of the winner neuron if the Euclidean distance is smaller than $R(t)$.

The algorithm is repeated from step 2) to the required number of iterations, t, or until $t \ge t_\propto$.

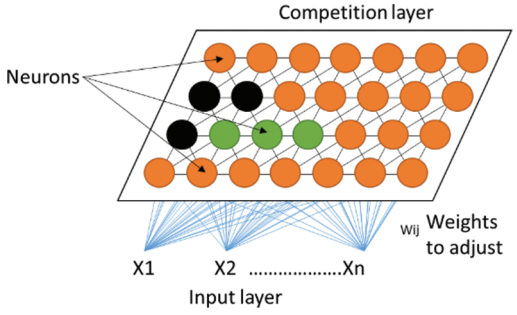

Figure 6 Basic structure of an SOM network.

4.2.2. GHSOM network training

In this section, we explain the procedures for training the SOM 1 and 2 networks, in which neuron identification was performed to obtain the classification results of the container. Figure 7 shows the algorithm designed to determine the size of the networks.

After the network has been trained and its neurons have been identified, the network is tested and evaluated, and the container data are introduced.

We used the MATLAB GHSOM Toolbox to train our network; this toolbox increases the functionality of the SOM Toolbox [30]. The use of the basic functions of the SOM Toolbox to create the GSHOM networks provides a more robust and standardized network than the SOM Toolbox. Once the network is trained, the decision algorithm identifies the hexagons to then use to evaluate the network results. If the classification error rate of the containers is less than 0.5% (which indicates that at least 50 containers have been misclassified), then the network is considered to be satisfactory; otherwise, the size of the network will be increased and retrained.

For the SOM 1 network, the algorithm determined an optimal size of 10 × 10. The algorithm determined an optimal size of 20×20 for the SOM 2 network.

SOM 1

This phase is the first step of the inspection strategy where the network classifies the input data, which consist of the weight variation, ΔW, *RFID* and *SI*. The result of the decision algorithm that determines the network size is shown in Figure 7, and the trained

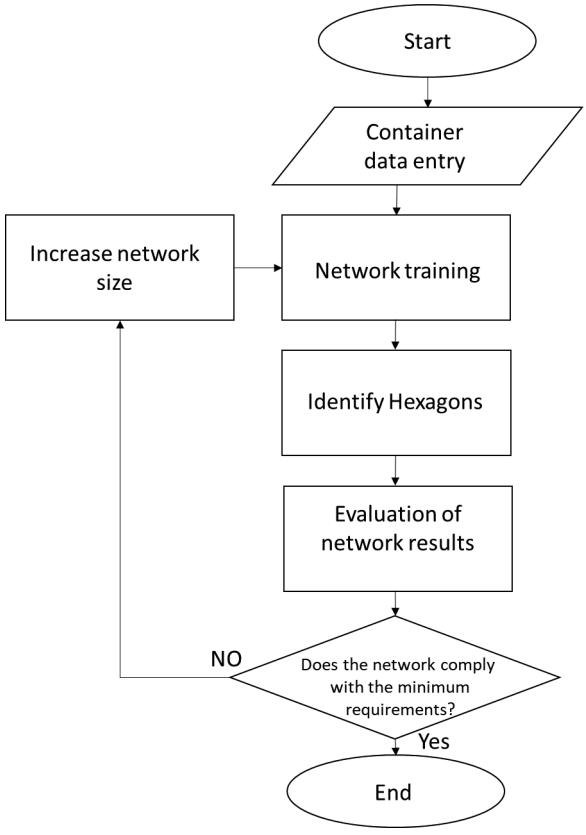

Figure 7 Decision algorithm for the SOM network size.

SOM 1 network is depicted in Figure 8. This figure shows the final configuration of the trained network that satisfies the error parameter conditions.

In Figure 8, the blue hexagons represent the neurons, the red lines connect the neighboring neurons, and the other colors represent the distances between the neurons; the darker colors represent longer distances, and the lighter colors represent shorter distances.

After properly training the neurons to achieve a container classification error rate of less than 0.5% (fewer than 50 misclassified containers), the containers that are assigned to each neuron of the SOM 1 network are identified, that is, the neurons that will classify the containers as suspicious, probably suspicions or not suspicious, depending on their information, are identified.

Figure 3a and 3b show the membership functions for the ΔW and the *SI* variables, respectively. For the hexagon classification, we use the same previously defined membership functions since they provide the boundaries for each of these variables due to their fuzzy nature and because we ensure that both inspection strategies employ the same information. These boundaries define the risky, safe and no-information or zero zones of each variable. For the RFID variable, a membership function is not needed, since it is a binary variable has a value of 0 if the container was opened and 1 otherwise. Using this information, the type of containers that are assigned to each neuron can be identified.

The neuron classification in the SOM 1 network, the training of which was depicted in Figure 8, is visualized in Figure 9. The containers associated with neurons classified as *M* will be manually inspected; the containers associated with neurons classified as *P* will leave the inspection zone since they are considered not suspicious; and the containers associated with neurons classified as *S* will proceed to the following verification level of the GHSOM (SOM 2), where they will undergo an X-ray scan.

In the following level of the GHSOM consisting of SOM 2, the ΔW, *SI* and *RFID* input variables for the containers that had been classified as probably suspicious (*S*) and the variable *Se*, which provides information about the X-ray inspection of the container, will be analyzed again.

SOM 2

With the variables ΔW, *SI* and *RFID*, the state of all containers, suspicious or not suspicious, cannot be defined. As a result, a new network (SOM 2) is trained. The input data are the output data of the SOM 1 network, namely, the containers classified as probably suspicious. The ΔW, *SI*, *RFID* variables are employed by the SOM 2 network as well as the X-ray scanning result obtained from the containers (*Se*).

Figure 10 shows the results of the decision algorithm that defines the size of the network (see the flow chart in Figure 7) for SOM 2, which defines a 20 × 20 network size. Again, this configuration is

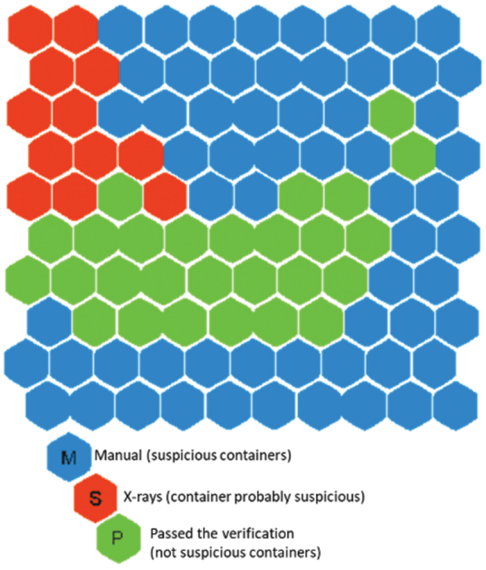

Figure 9 Distribution of the SOM 1 final classification.

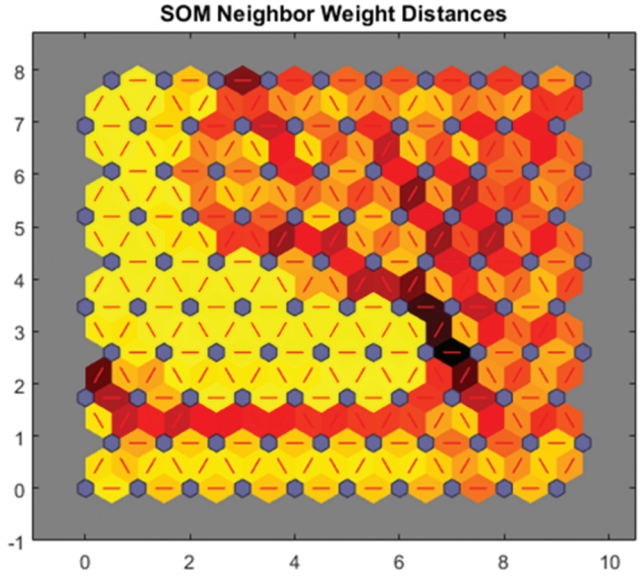

Figure 8 Trained SOM 1 network with the weights and distances of the neighboring neurons.

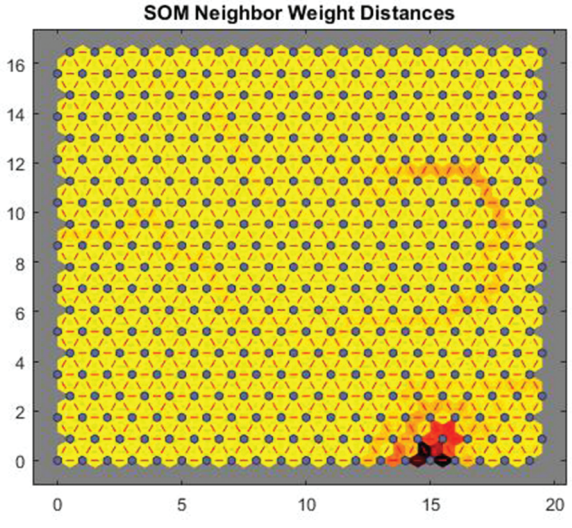

Figure 10 Trained SOM 2 network with the weights and distances of the neighboring neurons.

the final configuration that meets the error requirements stated in the algorithm to define the network size.

In Figure 10, the blue hexagons represent the neurons; the red lines connect the neighboring neurons, the different colors represent the distances between the neurons the darker colors represent longer distances; and the lighter colors represent shorter distances. Unlike in SOM 1, the distances between the neurons are very small due to the size of the network and the variable values.

The type of neuron that will classify the containers as suspicions or not suspicious, depending on the variables ΔW, *SI*, *RFID* and *Se*, is identified.

As previously explained, to identify which type of containers are assigned to each neuron, the membership functions were employed for the ΔW and *SI* variables. For the new SOM 2 network, the membership functions for *Se* are shown in Figure 3a and 3b and Figure 4c, respectively.

Figure 11 shows the neuron positions for the container classification obtained by the algorithm, given the network size that was shown in Figure 10. The containers located in neurons classified as *M* will be manually inspected, and the containers located in neurons classified as *P* will leave the inspection zone.

5. ANALYSIS OF THE RESULTS

The results of each inspection strategy are analyzed in this section. Each strategy uses the same data for the 10,000 containers as input (see Annex 1 for the details related to the data generation for the experimentation). The efficiency of each strategy based on artificial intelligence is observed for the classification of containers. The ability to minimize the cost and times of the inspection zone in a container terminal and the ability to minimize the number of illegal containers that are not detected in the inspection zone are observed, as we presented in the initial scientific equation. The novel introduction of the weight variation variable, ΔW, is very useful and discriminative for the classification of the container input data since both methods can be employed to make decisions for the classification of each container.

5.1. The Base Case

The same data for 10,000 containers were used for each inspection strategy. The results of the inspection strategies, the strategy based on FL and the strategy based on GHSOM networks, are presented in the following section.

5.1.1. The FL approach

In node 1, the RFID tags of the 10,000 containers are analyzed, of which 732 containers were found to have been illegally opened and were classified as suspicious and manually inspected. Of the 732 suspicious containers, 263 containers contained some smuggled merchandise, and 469 containers had part of their merchandise stolen.

A total of 9,268 containers were classified as likely suspicious and were used as the input data of node 2. Using the *FL* algorithm, an analysis of the *W* and *SI* variables of each of the 9,268 containers was performed.

The *FL* approach classified 478 containers as suspicious; these containers contained some type of illegal merchandise. Simultaneously, 5,792 containers were classified as not suspicious and continued their path through the terminal. However, two of these

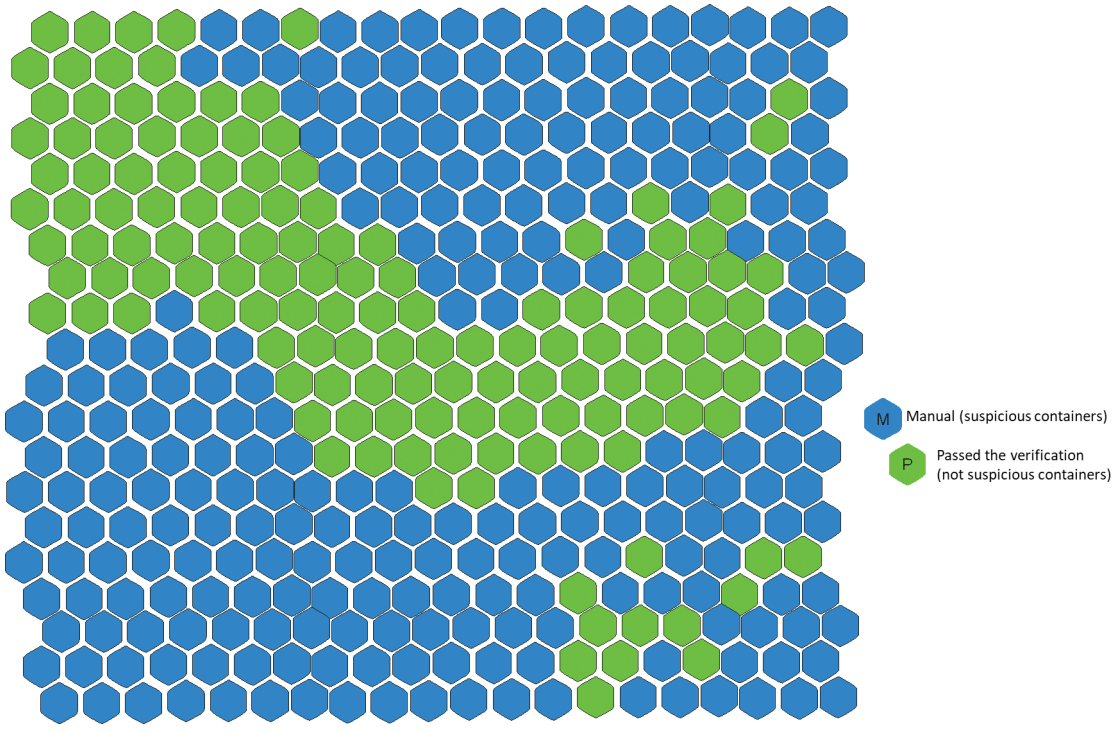

Figure 11 | Distribution of the SOM 2 final classification.

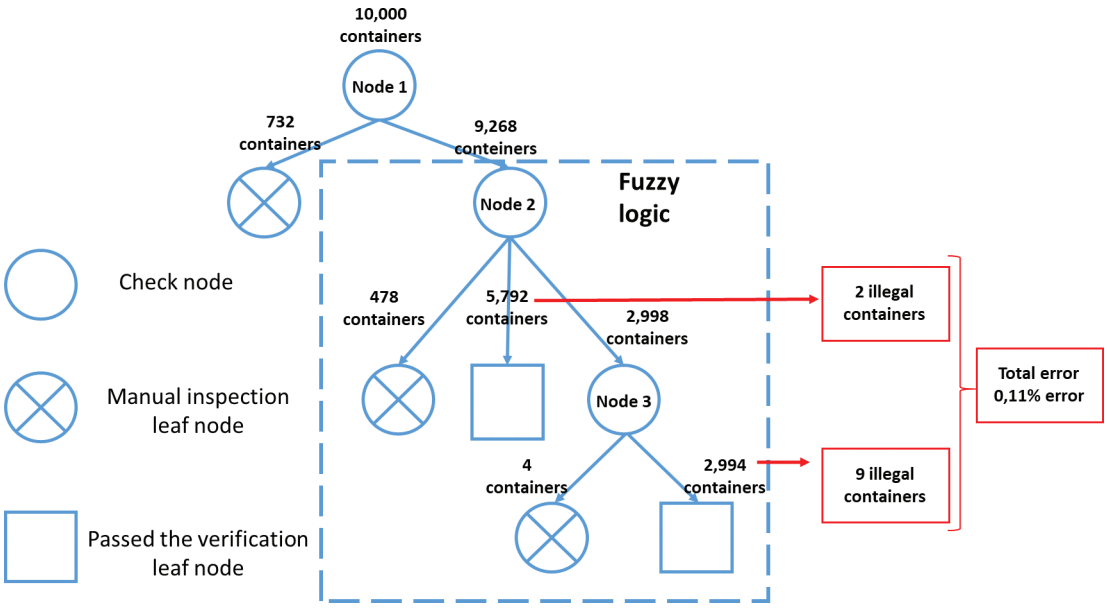

Figure 12 Decision tree summary of the container classification.

containers carried smuggled merchandise. The remaining 2,998 containers continued to be analyzed in node 3.

In node 3, 2,998 containers were analyzed and passed through an X-ray inspection. With the ΔW and SI data of each container, 4 containers were classified as suspicious and had to be manually inspected; they contained illegal merchandise. A total of 2,994 containers were classified as not suspicious and continued their path through the container terminal. From these containers, 9 containers carried some type of illegal merchandise that could not be detected by the inspection strategy. To calculate the error rate, we employ the following equation:

$$Err\% = \frac{ICo\ x\ 100}{TC} \tag{20}$$

where ICo is the number of illegal containers that left the inspection zone as not suspicious, in both nodes 2 and 3; and TC is the total number of containers that entered the system. In our case,

$$Err\% = \frac{(9+2)x100}{10,000} = 0.11\%$$

Thus, the error rate is 0.11%. A summary of the inspection strategy results is shown in Figure 12. This output error rate, for both nodes 2 and 3, is attributed to the notion that the values used to classify the containers were very small and were almost undetectable by the X-ray scan, weight variation or the SIs. This finding is observed in Figures 13 and 14, where the weight variation is given in tons [T].

Specifically, the classification error rate of the inspection strategy was attributed to the very small values of different variables. As shown in Figure 13, two containers had high SI values and were illegal but were classified as not suspicious when a small weight variation existed between the two containers. As shown in Figure 14, these 9 containers were classified as not suspicious when they were illegal because their weight variation was very small and their SI values were very high or the values of the X-ray simulation were low;

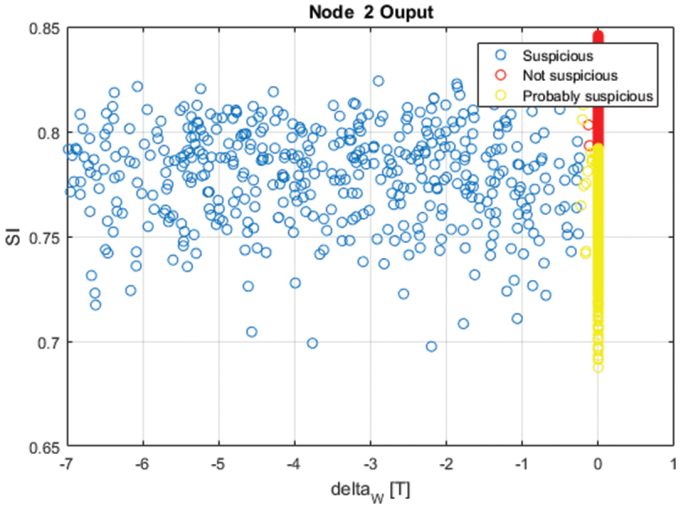

Figure 13 Classification analysis of the node 2 output.

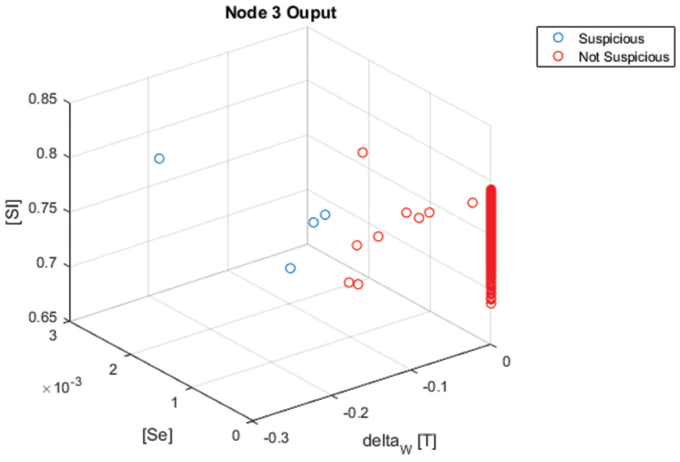

Figure 14 Classification analysis of the node 3 output.

that is, if two of the container variables had values similar to those that are considered as safe, the system considered these containers not suspicious.

The inspection strategy based on FL consists of three steps: (i) the first node detects containers that were forced open as determined by the RFID data, (ii) the second node makes use of the ΔW and *SI* variables to further analyze those containers with a positive RFID result to determine whether the smuggling or theft of goods was possibly carried out at the origin or the electronic seal was replaced and falsified (at node 2, only those containers with all the variables at the maximum level of security are classified as safe), and finally, (iii) at the third node, a nonintrusive technology (X-ray) is used to classify the last risky containers.

5.1.2. The GHSOM approach

In SOM 1, the ΔW, *SI* and *RFID* variables of the same 10,000 containers of the previous case were analyzed, of which 1,216 containers were classified as suspicious, 3,837 containers were classified as not suspicious, and 4,947 containers continued to be analyzed in SOM 2. Of the 1,216 suspicious containers, 747 containers carried illegal merchandise and 469 containers had removed or stolen merchandise. Of the 3,837 containers that were classified as not suspicious, none contained any illegal merchandise.

In SOM 2, 4,947 containers were analyzed and subjected to an X-ray scan. With the ΔW, *SI* and *RFID* data of each container, one container was classified as suspicious and had to be manually inspected; it contained illegal merchandise. A total of 4,946 containers were classified as not suspicious and continued their path through the container terminal. Of these containers, 8 containers contained some type of illegal merchandise that could not be detected by the inspection strategy. These 8 containers represent the error rate of the inspection strategy, which is 0.08%.

A summary of the inspection strategy results is shown in Figure 15. This error rate in the SOM 2 output is attributed to the fact that the illegal merchandise in the container was not easily detected by the X-ray scanning model, which hindered the analysis of the weight variation and *SI* value.

Figure 15 shows the complete inspection strategy and the results. Note that there are no errors in the classification obtained by SOM 1 for the suspicions containers and not suspicions containers. The classification obtained by SOM 2 has an error rate of 0.08%, as the amount of illegal merchandise was not detectable by the X-ray scans in this case.

Figure 16 shows the SOM 1 output; the data are grouped into two data clouds defined by the *RFID* variable. The network is capable of detecting and correctly classifying all the containers with $RFID = 0$, which are containers that were illegally opened. All the containers with a significant ΔW are classified as suspicious, and the containers with a small ΔW value and a *SI* value near zero (refer to Figure 3b) are classified as probably suspicious. The containers whose parameters are in the safe zone are classified as not suspicious.

The SOM 2 output is given in Figure 17. A second analysis of the parameters was necessary to detect another suspicious container from the 8 remaining containers in this inspection strategy point. The combination of the Δ*W* and *Se* variables was necessary to detect this container, since all the variables were within the zero threshold; that is, they do not provide sufficient information to identify the type of the container.

6. SUMMARY OF THE RESULTS

In this final summary, we follow a specific table design that allows us to easily visualize the performance of each approach. Each row represents the instances of the predetermined class, and each column represents the instances of the predicted class (or vice versa)

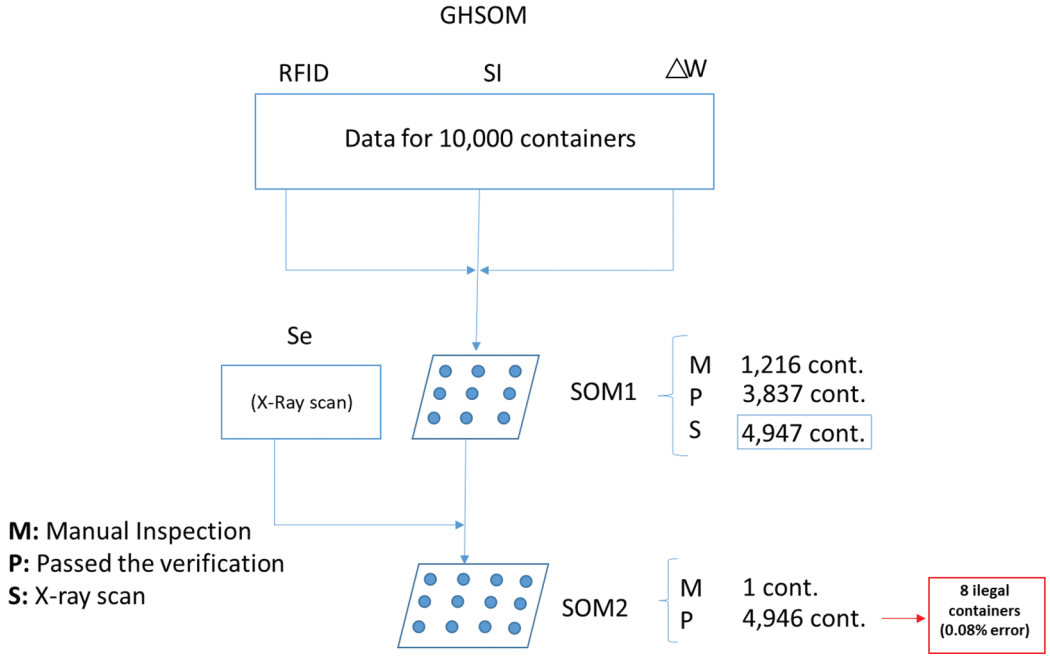

Figure 15 Summary of the classification of the containers.

[46]. Given a classifier and an instance, there are four possible results as Table 7 shows.

If the instance is positive and it is classified as positive, then it is a true positive (a). However, if it is classified as negative, it is a false negative (b). If the instance is negative and it is classified as negative, then it is a true negative (d). However, if it is classified as positive, it is a false positive (c). Given a classifier and a set of instances, a confusion matrix can be easily constructed (see [47]).

The rate of true positives and negatives, as well as false positives and negatives, can be calculated using the following metrics (21–24).

The true positive rate of the classification is given by

$$TPrate = \frac{a}{a+b} \tag{21}$$

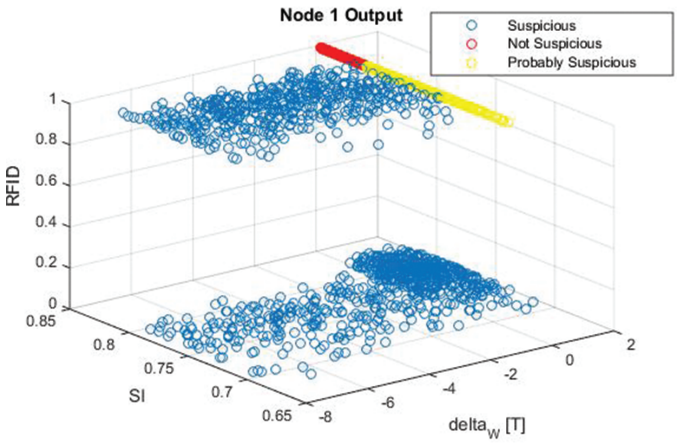

Figure 16 | Classification analysis of the SOM 1 output.

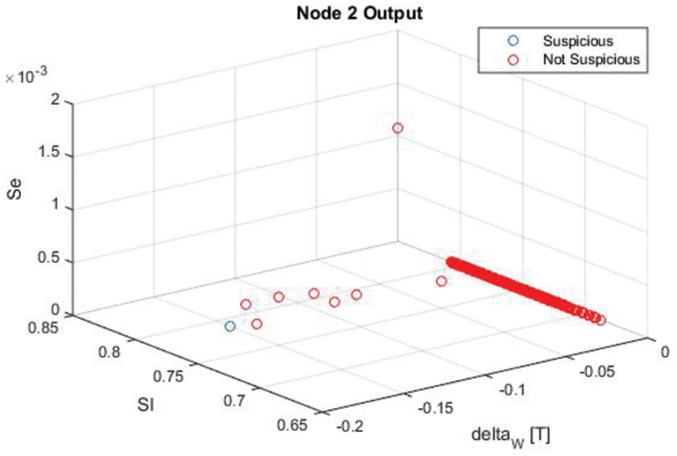

Figure 17 | Classification analysis of the SOM 2 output.

Table 7 | Confusion matrix.

		Predicted Values	
		Positive	**Negative**
Real values	Positive	a	b
	Negative	c	d

The false positive rate of the classification is given by

$$FPrate = \frac{b}{a+b} \tag{22}$$

The true negative rate of the classification is given by

$$TNrate = \frac{d}{c+d} \tag{23}$$

The false negative rate of the classification is given by

$$FNrate = \frac{c}{c+d} \tag{24}$$

Next, the confusion matrix of the proposed algorithms allows us to analyze the performance of the FL and GHSOM approaches (see Tables 8 and 9).

- **Fuzzy Logic**
  The algorithm shows a good capability to appropriately classify the different containers of our case study. All the legal containers were correctly classified in 100% of the cases and did not require any manual inspection with its corresponding cost and time. In the case of the illegal containers, the algorithm showed a very low rate of confusion. Only 11 containers representing 0.89% of the instances were classified as false positives and passed the verification without a manual inspection. Of the illegal containers, 99.1% were appropriately identified for manual inspection. Therefore, the algorithm presents a low failure rate.
- **GHSOM**
  Regarding the GHSOM approach, the algorithm shows a very high degree of appropriate classification. First, all the legal containers were correctly classified in 100% of the cases and did not require manual inspection with its corresponding cost and time. Regarding the false negative containers, only 8 containers (0.65%) were inadequately classified and were not subjected to manual inspection. On the other hand, 1,217 illegal containers were appropriately subjected to manual inspection.

  The comparison of the approaches shows that both of the algorithms are very good classifiers that perfectly classify the legal containers. Both approaches show a very good level of classification for illegal containers with a very low error rate. In this line, the GSHOM approach showed a slightly better performance.

Table 8 | Confusion matrix for the fuzzy logic approach.

	P (Passed the Verification)	**M (Manual)**
L (legal)	8,775 (100%)	0 (0%)
I (illegal)	11 (0.89%)	1,214 (99.1%)

Table 9 | Confusion matrix for the GHSOM approach.

	P (Passed the Verification)	**M (Manual)**
L (legal)	8,775 (100%)	0 (0%)
I (illegal)	8 (0.65%)	1,217 (99.34%)

GHSOM, growing hierarchical self-organizing map.

7. CONCLUSIONS

This study has demonstrated how efficient security inspections can be achieved by increasing the security of container transport and minimizing the time and cost spent by applying two artificial intelligence methodologies, which are based on FL and the GHSOM. The container input data, such as the RFID readings, X-ray scanning results and container security data, were analyzed. A novel contribution of the new IMO regulations was the inclusion of the container weight variation to achieve a better adjusted classification of the containers and reduce the number of suspicious containers that are not detected in the inspection area.

Additionally, the weight sensors in the container terminal work with threshold values between 40 and 20 tons. The sensors recommended in the OIMLR 60 regulation (from the International Organization of Legal Metrology) suggest an accuracy of approximately ± 250 kg for the sensor working range. It is clear that the weight variation offers significant help in the inspection strategy, but it cannot be used by itself to identify low levels of smuggling. Thus, a combined inspection strategy is proposed, which includes the RFID data, SI and results from a nonintrusive inspection together with the weight variation in an integrated way.

Unlike the data provided by the RFID readings (a binary output variable), the remaining variables were fuzzy (ΔW, *SI* and X-ray variables). Based on the proposed methodologies, inspection strategies can be employed to rapidly classify the containers with a high reliability percentage.

In both algorithms, the use of the weight variation among containers prevents the inspection of all containers and maintains a low error rate or while reducing the inspection time in the system. For the FL algorithm, 7,002 containers do not pass through the X-ray inspection, which prevents 350 hours of inspection. Using the GHSOM algorithm, 5,053 containers do not pass through the X-ray inspection, which prevents 252 hours of inspection. The hours of inspection are calculated considering the inspection time of approximately 20 containers/hour given by [48].

To compare the capabilities of each algorithm, the same data are employed as inputs and adjustment information in both algorithms. Thus, the information received a priori does not affect the results.

First, the FL algorithm achieves very competent global results, with an error rate of only 0.89%. This error rate is low, and only a small amount of smuggling cannot be detected in this strategy (size smaller than 0.00375 m^3), which was the margin established in the X-ray simulation as detectable.

Second, the GHSOM neural network algorithm offers even more promising results, with an error rate of only 0.65% for illegal containers. This capability is attributed to the large classification capacity of these types of algorithms, which indicates that this approach is the better option for minimizing the time and costs in the inspection area of a container terminal and decreasing the error rate.

We conclude that the GHSOM and fuzzy algorithms are very similar to each other in terms of their ability to detect and group the study objects into many different categories. Both of the strategies demonstrated very strong capability for the correct classification of containers, and they achieved similar results in terms of the classification accuracy. The false negative rate was slightly better in the case of the GSHOM, but the difference between the two approaches was very low. However, we recommend the adoption of the GHSOM approach specially when dealing with complex problems due to its better ability to classify the data in very different groups

The improvement in the classification capacity of the GHSOM-based algorithm over that of the FL-based algorithm is due to its intrinsic nature. The fuzzy algorithm uses four variables: ΔW, Se and SI, where each variable is divided into three zones, and the RFID variable that is divided into two zones. In node 3, the algorithm is capable of classifying a container into 27 different groups (three variables divided into three zones). Using the same variables, the GHSOM-based algorithm classified them into the same zones but does not have this limit. In this particular case, the algorithm classifies the containers into 400 different groups (SOM 2 has a size of 20×20).

To appropriately analyze a comparison between both approaches, wider alternative experimentation sets should be constructed. This is now one of our future lines of research: the definition of a wide set of experimentation data that closely represents a real situation and considers possible combinations of actions (and also combinations of illegal actions). In this line, a deeper analysis of the intrinsic vulnerabilities of the ΔW and *SI* variables should be considered, with particular attention to the *SI* variable.

Finally, a detailed study of the cost and time savings at the container terminal attributable to the proposed strategy versus a general (or random) manual inspection strategy would help to identify the advantages of the proposed approaches. Such a study should be conducted using a discrete event simulation approach and should include the saved inspection time, its associated cost savings estimate and an estimate of the consequences of incorrect classifications. This is also a challenging future research direction.

Annex 1. Data generation for experimentation

This annex describes the procedure followed to generate the data for the 10,000 containers that are used for the experimentation.

The data was generated by using the MATLAB "random" function. This function generates random numbers using a probability density function (*PDF*). We used a normal distribution to calculate the probability density function (*PDF*) as stated in Equation (25):

$$y = f\left(x|\mu,\sigma\right) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \quad \mu = 0;\ \sigma = \frac{1}{3} \tag{25}$$

The reliability percentages for the country of origin of the containers (*RCO*) and the reliability percentages of the carriers and port (*RT*) were randomly generated using the "random" function and Equation (25). The generated numbers were then transformed to obtain positive values in an increasing histogram with the following limits:

$$0.76 \leq RCO \leq 1;\ \ 0.8 \leq RT \leq 1$$

The limits are defined according to Table 4 [14] so that that every *RCO* value under 76% and every *RT* value under 80% is considered a risky container. Figure 18 depicts the obtained histograms for *RT* and *RCO*.

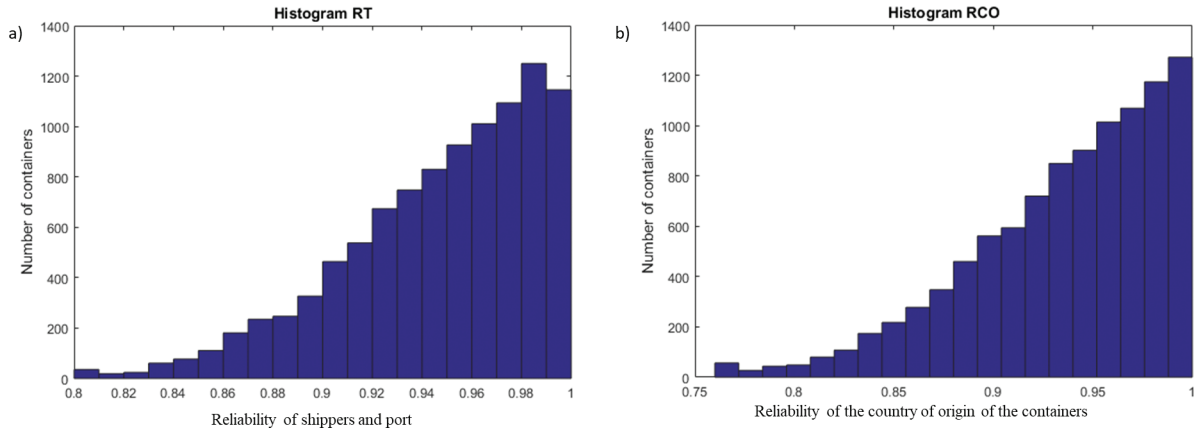

Figure 18 | Histogram for *RT* and *RCO*.

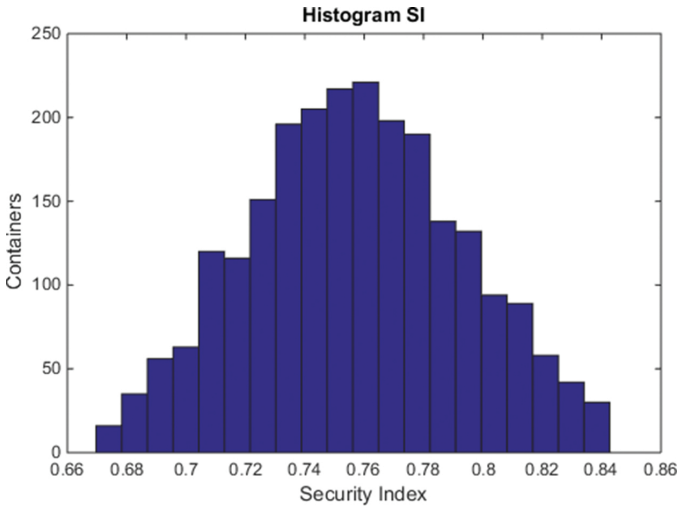

Figure 19 | Histogram of the container security scores, SI.

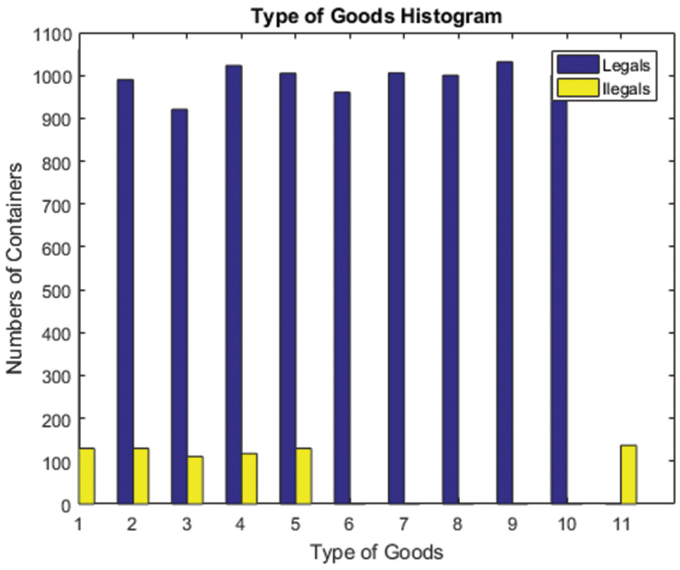

Figure 20 | Distribution of the types of legal goods and illegal goods transported.

The container *SI*) was obtained from Table 4. The exact *SI* value was obtained by interpolating the *RCO* and *RT* values of each container. The results are depicted in Figure 19, and the SI values are between 0.65 and 0.85. This set of values defines the a priori risky and non-risky containers.

In our case study, the *RFID* variable represents the reading obtained from the electronic seals on the containers. The ancillary variable, *r*, is generated using the "random" function and a *PDF* distribution (Equation 25). The generated numbers are then transformed to obtain an increasing histogram of positive values whose limits are:

$$0 \leq r \leq 1$$

Then, the ancillary variable, *r*, is compared to *RT*. If $r < RT$ then $RFID = 1$ (not forced open container). If $r > RT$ then $RFID = 0$ (forced open container). Higher values of *RT* imply a lower probability that it is a container that has been forced open.

I is a binary variable that indicates whether a container contains illegal goods. To construct the set, we define another ancillary variable, r_i, that is generated using the "random" function and a PDF distribution (Equation 25). The generated numbers are then transformed to obtain an increasing histogram of positive values whose limits are:

$$0 \leq r_i \leq 1$$

Then, the ancillary variable, r_i, is compared to *RCO*. If $r_i < RCO$ then $I = 1$ (container contains illegal goods). If $r_i > RCO$ then $I = 0$ (container does not contain illegal goods). High values of *RCO* imply a high probability that the container contains illegal goods.

The following variables are defined: W_0 gives the container weight at the origin, I_W gives the weight of the illegal goods, and W_S gives the weight of stolen freight. These variables were generated using the MATLAB "rand" function for uniformly distributed random numbers. In our case study, we assume a maximum container load of $W_{max} = 30$ *tons* [49], then:

$$W_{max} = w_0 + I_w = 30\ Tons. \tag{26}$$

where the W_0 is uniformly distributed between $0 \leq W_0 \leq 22.5\,tons$ and I_w is uniformly distributed between $0 \leq I_w \leq 7.5\,tons$. Therefore, the maximum weight of a container is 22.5 Tons (at the origin) plus 7.5 tons (if it contains illegal goods).

Then, W_s is uniformly distributed between $-2\,Tons \leq W_s \leq 0$ to define weight of stolen goods in the containers of our case study.

The relationship between the *RFID* and I values helps simulate the behavior of the weight readings of the weight sensors, W_1, as follows:

$$W_1 = W_0 + I_W \qquad \forall\, RFID = 0,\ I = 0 \tag{27}$$

$$W_1 = W_0 + W_s \qquad \forall\, RFID = 0,\ I = 1 \tag{28}$$

$$W_1 = W_0 + I_W \qquad \forall\, RFID = 1,\ I = 0 \tag{29}$$

$$W_1 \cong W_0 \qquad \forall\, RFID = 1,\ I = 1 \tag{30}$$

It can be appreciated that in our research, the smuggling and stolen freight events do not occur at the same time. That is, a container could not have been stolen from and contain illegal goods at the same time.

The illegal and legal goods were obtained by generating two ancillary variables using the MATLAB "rand" function with limits between 0 and 1 to obtain uniformly distributed numbers.

G is the set of legal goods, which are liquors, fuels, tobacco, medications, weapons, raw materials, textiles, food, manufactured goods and vehicles. To define set G, the ancillary variable range is divided into 10 equal parts.

IT is the set of illegal goods. The range of the ancillary variable is divided into 6 equal parts. The value indices vary from 1 to 5 for liquors, fuels, tobacco, medications, weapons and 11 for illegal drugs.

Figure 20 shows all the different types of (legal and illegal) goods. Each index in the graphic represents the type of goods. The legal goods are represented by blue: 1 (liquors), 2 (fuels), 3 (tobacco), 4 (medications), 5 (weapons), 6 (raw material), 7 (textiles), 8 (foods) and 9 (manufactured products). The illegal goods are represented by yellow: 1 (liquors), 2 (fuels), 3 (tobacco), 4 (medications), 5 (weapons) and 11 (illegal drugs). Additionally, Table 10 defines the types of goods considered for our case study.

The data generation algorithm assumes that each container only transports one type of goods, and in the case that the container contains illegal goods, it is only one type of illegal goods.

In our case study, we selected X-ray technology as the nonintrusive inspection method among the current existing technological alternatives. X-ray imaging is one of the main nonintrusive technologies for container inspection, and it provides convincing details of the content of large objects such as containers [50], to determine the behaviors of both the X-ray scanner results and the operator. The proposed simulation emulates the behavior of an operator at the moment that an X-ray scan is performed, that is, the operator will see and analyze the data on the container contents, for example, the volume, shape, weight and type of material that it transports. This

Table 10 The types of goods used in the case study.

Goods Transported	Classification of Goods	Classification of Goods According to Type
1 liquors	Legal or illegal	Vodka, whiskey, beer, rum, etc.
2 fuels	Legal or illegal	Oil, gasoline, diesel, kerosene, etc.
3 tobacco	Legal or illegal	Cigarettes, cigars, etc.
4 medications	Legal or illegal	Prescription medicines, legal drugs, natural medicines, etc.
5 weapons	Legal or illegal	Firearms, ammunition, bladed weapons, etc.
6 raw material	Legal	Vegetable, animal, mineral, liquid or fossil.
7 textiles	Legal	Different types of cloth, clothes, etc.
8 foods	Legal	Vegetables and animals.
9 manufactured products	Legal	Consumer goods, capital goods and materials and supplies.
11 illegal drugs	Illegal	Cocaine, ecstasy, amphetamines, etc.

simulation uses the S_e (X-ray) variable, which depends on several factors:

$$S_e = F_v F_f F_w F_m \tag{31}$$

where F_v is the volume factor, F_f is the shape factor, F_w is the weight factor, and F_m is the materials factor.

The volume factor is given by the following equation:

$$F_v = \frac{V_I}{V_R} \tag{32}$$

where V_R is the reference volume, and V_I is defined as

$$V_I = \frac{M}{\rho_I} \tag{33}$$

where M is the mass of illegal merchandise and ρ_I is the density; the density values were obtained from [51].

The shape factor is determined by comparing the shape of the transported goods G and the shape of illegal merchandise I, where it will equal 1 if the shape of G is similar or equal to that of I and 0 otherwise.

The following is the weight factor given by

$$F_w = \frac{I_W}{W_G} \tag{34}$$

where W_G is the weight of the transported goods, and as previously mentioned, I_W is the weight of illegal merchandise.

The material factor is expressed by the following equation:

$$Fm = \frac{FaG_{(6MeV)} FaG_{(10MeV)}}{FaI_{T_{(6MeV)}} FaI_{T_{(10MeV)}}} \tag{35}$$

where FaG and FaI_T are the attenuation coefficients for each type of goods and illegal merchandise, respectively, obtained from [51] in relation to the level of the X-ray energy, considering that

$$\text{if } G = I_T, \text{ then } F_m = 1 \tag{36}$$

Two X-ray energy levels were applied (6 MeV and 10 MeV). Using this property, we can classify the contents of a container based on the image provided by the ratio of the different levels of attenuation [42].

CONFLICT OF INTEREST

The authors declare that they have no competing interests.

AUTHORS' CONTRIBUTIONS

The study was conceived and designed by Pablo Cortés and Leonela Morales. Luis Onieva and Ventura Pérez revised the different versions of the research and suggested improvements.The director of the research and final responsible for the revisions was Pablo Cortés. All authors read and approved the manuscript.

ACKNOWLEDGMENTS

The authors wish to acknowledge the financial support of project "Estrategias de diseño microelectronico para IOT en escenarios hostiles" (Ref. TEC2016-80396-C2-2-R) funded by the Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad for the completion of this work.

REFERENCES

[1] X. Zhao, H. Yan, J. Zhang, A critical review of container security operations, Maritime Policy Manage. 44 (2017), 170–186.
[2] T.J. Leonard, P. Gallo, S. Véronneau, Security challenges in United States sea ports: an overview, J. Transport. Secur. 8 (2015), 41–49.
[3] S.-L. Chao, P.-S. Lin, Critical factors affecting the adoption of container security service: the shippers' perspective, Int. J. Prod. Econ. 122 (2009), 67–77.
[4] K. English, C. Zuver, Network centric sensor fusion for shipping container security, 2006. https://patents.google.com/patent/US20070200701.
[5] N. Bakshi, S.E. Flynn, N. Gans, Estimating the operational impact of container inspections at international ports, Manag. Sci. 57 (2011), 1–20.
[6] E. Boros, E. Elsayed, P. Kantor, F. Roberts, M. Xie, Optimization problems for port-of-entry detection systems, Stud. Comput. Intell. 135 (2008), 319–335. http://www.scopus.com/inward/record.url?eid=2-s2.0-45949088542&partnerID=40&md5=c2cbb0744b2a638de4cf6fb7c34ac23e.
[7] E. Boros, N. Goldberg, P.B. Kantor, J. Word, Optimal sequential inspection policies, Ann. Oper. Res. 187 (2011), 89–119. http://www.scopus.com/inward/record.url?eid=2-s2.0-79960282619&partnerID=40&md5=7a1d4f6c1aa564208cdca8e300d6d800.
[8] F. Longo, Design and integration of the containers inspection activities in the container terminal operations, Int. J. Prod. Econ. 125 (2010), 272–283. http://www.scopus.com/inward/record.url?eid=2-s2.0-77950627799&partnerID=40&md5=a6f08e0a87fdee9af6bf44ea902b094e.
[9] D.-H. Lee, L. Song, H.Q. Wang, An optimization approach to security operations toward sustainable seaport, Int. J. Sustain. Transport. 2 (2008), 115–133.
[10] G.A. Harris, B.J. Schroer, M.D. Anderson, D.P.F. Moëller, Resources to minimize disruption caused by increased security inspection of containers at an intermodal terminal: application of simulation, Trans. Res. Record. (2009), 109–116. http://www.scopus.com/inward/record.url?eid=2-s2.0-76149094150&partnerID=40&md5=58db2ba6e387ea36297bcb1cd8dae608.
[11] E.A. Elsayed, C.M. Young, M. Xie, H. Zhang, Y. Zhu, Port-of-entry inspection: sensor deployment policy optimization, IEEE Trans. Automat. Sci. Eng. 6 (2009), 265–276.
[12] C.M. Young, M. Li, Y. Zhu, M. Xie, E.A. Elsayed, T. Asamov, Multiobjective optimization of a port-of-entry inspection policy, IEEE Trans. Automat. Sci. Eng. 7 (2010), 392–400. http://www.scopus.com/inward/record.url?eid=2-s2.0-77950861263&partnerID=40&md5=ff991adfe3e33d1660052cb62d6bca9b.
[13] S.F. van Weele, J.E. Ramirez-Marquez, Optimization of container inspection strategy via a genetic algorithm, Ann. Oper. Res. 187 (2011), 229–247.
[14] R. Riahi, K. Li, I. Robertson, I. Jenkinson, S. Bonsall, J. Wang, A proposed decision-making model for evaluating a container's security score, Proc. Inst. Mech. Eng. Part M J. Eng. Maritime Environ. 228 (2014), 81–104. http://www.scopus.com/inward/record.url?eid=2-s2.0-84900874104&partnerID=40&md5=2cb4bc1e11e36383298913734fe0d42c.
[15] J.E. Ramirez-Marquez, Port-of-entry safety via the reliability optimization of container inspection strategy through an evolutionary approach, Reliab. Eng. Syst. Safety. 93 (2008), 1698–1709. http://www.scopus.com/inward/record.url?eid=2-s2.0-44549088740&partnerID=40&md5=80ad7d6bf6b0928dc2523166a2dc2c71.
[16] A.L. Concho, J.E. Ramirez-Marquez, An evolutionary algorithm for port-of-entry security optimization considering sensor thresholds, Reliab. Eng. Syst. Safety. 95 (2010), 255–266. http://www.scopus.com/inward/record.url?eid=2-s2.0-73649122395&partnerID=40&md5=2377189cfd730bbde12e9c18737cc71e.
[17] Z.-X. Ma, Y. Ding, G.L. Lin, C.-Y. Hou, Identification of efficiency factors for inspection and quarantine clearance using an improved structural equation model, J. Indus. Prod. Eng. 31 (2014), 261–273.
[18] C.-H. Wang, M.-E. Wu, C.-M. Chen, Inspection risk and delay for screening cargo containers at security checkpoints, in Proceedings - 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2015), Adelaide, Australia, 2016.
[19] W. Wang, Y. Zhou, X. Song, G. Tang, Z. Fang, Operational impact estimation of container inspections at Dalian Port: the application of simulation, Simulation. 93 (2017), 135–148.
[20] S.F. Van Weele, J.E. Ramirez-Marquez, Optimization of container inspection strategy via a genetic algorithm, Ann. Oper. Res. 187 (2010), 229–247.
[21] B.M. Brío, A.S. Molina, Redes neuronales y sistemas borrosos, in: Textos Universitarios, Ra-Ma,2006.
[22] E.B. Huerta, B. Duval, J.-K. Hao, Fuzzy logic for elimination of redundant information of microarray data, Genom. Proteom. Bioinf. 6 (2008), 61–73.
[23] S.-L. Hsueh, A fuzzy logic enhanced environmental protection education model for policies decision support in green community development, Sci. World J. 2013 (2013), 1–8.
[24] G.-S. Liang, L.-Y. Lin, C.-F. Liu, The optimum output quantity of a duopoly market under a fuzzy decision environment, Comput. Math. Appl. 56 (2008), 1176–1187.

[25] V. Magudeeswaran, C.G. Ravichandran, Fuzzy logic-based histogram equalization for image contrast enhancement, Math. Probl. Eng. 2013 (2013), 1–10.
[26] S. Motepe, B. Twala, Q.-G. Wang, R. Stopforth, Determining distribution power system loading measurements accuracy using fuzzy logic, Procedia Manuf. 7 (2017), 435–439.
[27] J.T. Starczewski, Efficient triangular type-2 fuzzy logic systems, Int. J. Approx. Reason. 50 (2009), 799–811.
[28] T. Kohonen, Self-Organizing Maps, Springer Series in Information Sciences, New York, NY, USA, 2001.
[29] V. Chaudhary, R.S. Bhatia, A.K. Ahlawat, A novel Self-Organizing Map (SOM) learning algorithm with nearest and farthest neurons, Alex. Eng. J. 53 (2014), 827–831.
[30] A. Chan, E. Pampalk, Growing hierarchical self organising map (GHSOM) toolbox: visualisations and enhancements, in Proceedings of the 9th International Conference on Neural Information Processing (ICONIP '02), IEEE, Singapore, 2002, vol. 5, pp. 2537–2541.
[31] M. Chattopadhyay, P.K. Dan, S. Mazumdar, Comparison of visualization of optimal clustering using self-organizing map and growing hierarchical self-organizing map in cellular manufacturing system, Appl. Soft Comput. 22 (2014), 528–543.
[32] M. Dittenbach, A. Rauber, D. Merkl, Uncovering hierarchical structure in data using the growing hierarchical self-organizing map, Neurocomputing. 48 (2002), 199–216.
[33] D. Ippoliti, X. Zhou, A-GHSOM: an adaptive growing hierarchical self organizing map for network anomaly detection, J. Parallel Distrib. Comput. 72 (2012), 1576–1590.
[34] E.J. Palomo, J. North, D. Elizondo, R.M. Luque, T. Watson, Application of growing hierarchical SOM for visualisation of network forensics traffic data, Neural Netw. 32 (2012), 275–284.
[35] J.-Y. Shih, Y.-J. Chang, W.-H. Chen, Using GHSOM to construct legal maps for Taiwan's securities and futures markets, Expert Syst. Appl. 34 (2008), 850–858.
[36] A. Forti, G.L. Foresti, Growing hierarchical tree SOM: an unsupervised neural network with dynamic topology, Neural Netw. 19 (2006), 1568–1580.
[37] Y. Zhang, W. Bu, C. Su, L. Wang, H. Xu, Intrusion detection method based on improved growing hierarchical self-organizing map, Trans. Tianjin Univ. 22 (2016), 334–338.
[38] D.D. Patil, P. Gupta, Growing Hierarchical Self-Organizing Map (GHSOM) for mining gene expression data general terms GHSOM and SOM algorithms keywords Self-organizing Map (SOM), Growing Hierarchical Self-Organizing Map (GHSOM), Int. J. Comput. Appl. 109 (2015), 16–17.
[39] K.V. Størkersen, S. Antonsen, T. Kongsvik, One size fits all? Safety management regulation of ship accidents and personal injuries, J. Risk Res. 20 (2016), 1154–1172.
[40] A. Embankment, Anexo Directrices Relativas A La Masa Bruta Verificada De Los Contenedores Con Carga 1 Introducción, 2014. http://www.imo.org/es/MediaCentre/HotTopics/container/Documents/1475.pdf.
[41] M. Kaur, M. Sandhu, N. Mohan, P.S. Sandhu, RFID technology principles, advantages, limitations & its applications, Int. J. Comput. Electr. Eng. 3 (2011), 1793–8163.
[42] K. Fu, D. Ranta, P. Das, C. Guest, Layer separation for material discrimination cargo imaging system, in: D. Fofi, K.S. Niel (Eds.), IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics, 2010.
[43] P. Cortés, J.R. Fernández, J. Guadix, J. Muñuzuri, Fuzzy logic based controller for peak traffic detection in elevator systems, J. Comput. Theor. Nanosci. 9 (2012), 310–318.
[44] S.-L. Shieh, I.-E. Liao, A new approach for data clustering and visualization using self-organizing maps, Expert Syst. Appl. 39 (2012), 11924–11933.
[45] M.H. Ghaseminezhad, A. Karami, A novel Self-Organizing Map (SOM) neural network for discrete groups of data clustering, Appl. Soft Comput. 11 (2011), 3771–3778.
[46] D. Powers, Evaluation: from precision, recall and F-factor to ROC, informedness, markedness & correlation, 2007. david.wardpowers.info/BM/index.htm.
[47] T. Fawcett, An introduction to ROC analysis, Pattern Recognit. Lett. 27 (2006), 861–874.
[48] J. Boukachour, C.H. Fredouet, M.B. Gningue, Building an expert-system for maritime container security risk management, Int. J. Appl. Logist. 2 (2011), 35–56.
[49] H. Kaps, Securing the product in the container, German Insurance Association, Berlin, 2016. Retrieved from https://www.containerhandbuch.de/chb_e/stra/index.html?/chb_e/stra/stra_03_02_00.html.
[50] G. Chen, Understanding X-ray cargo imaging, Nucl. Instrum. Methods Phys. Res. Sec. B Beam Interact. Mater. Atoms. 241 (2005), 810–815.
[51] NIST, NIST: X-ray mass attenuation coefficients, 2016. http://www.nist.gov/pml/data/xraycoef/.