NEURAL NETWORK ALGORITHMS FOR FRAUD DETECTION: A COMPARISON OF THE COMPLEMENTARY TECHNIQUES IN THE LAST FIVE YEARS

Alberto Clavería Navarrete, Universidad de Sevilla
Amalia Carrasco Gallegos, Universidad de Sevilla

ABSTRACT

Purpose: *The purpose of this research is to analyse the complementary updates and techniques in the optimization of the results of neural network algorithms (NNA) in order to detect financial fraud, providing a comparison of the trend, addressed field and efficiency of the models developed in current research.*
Design/Methodology/Approach: *The author performed a qualitative study where a compilation and selection of literature was carried out, in terms of defining the conceptual analysis, database and search strategy, consequently selecting 32 documents. Subsequently, the comparative analysis was carried out, in turn being able to determine the most used and efficient complementary technique in the last five years.*
Findings: *The results of the comparative analysis depicted that in 2019 there was a greater impact of research based on NNA with 11 studies. 27 complementary updates and techniques were identified related to NNA, where deep neural network algorithms (DNN), convolutional neural network (CNN) and SMOTE neural network. Finally, the evaluation of effectiveness in the collected techniques achieved an average accuracy ranging between 79% and 98.74% with an overall accuracy value of 91.32%.*
Originality/Value: *Being a technique which is applied and compared in diverse studies, ANNs uses a wide range of mechanisms concerning training and classification of data. According to the findings of this research, the complementary techniques contribute to the progress and optimization of algorithms regarding financial fraud detection, having a high degree of effectiveness concerning on-line and credit card fraud.*

Keywords: Neural Networks, Fraud Detection, Algorithm, Finance and Financial Fraud.

INTRODUCTION

Financial fraud has become relevant in the digital era due to the significant increment of these criminal acts as a result of the available technological advances (Pérez, 2018). The actions taken against fraud are focused on two points: fraud prevention and fraud detection. Fraud prevention tries to block fraudulent transactions, whereas fraud detection relates to successful fraudulent transactions which are identified after being committed (Sandoval, 2019). In fraud detection, the inspection of financial statements requires conventional audit techniques in order to prevent the consequences of fraud, such techniques must distinguish between abnormal data and authentic data, therefore allowing early decision making and strategies that diminish the impact of fraud. Currently, new technologies are being used which are capable of processing large volumes of information, allowing to detect abnormal patterns that would possibly be imperceptible to the human eye (Shwartz, 2014). The development of these technologies utilizes data mining as an exploratory mechanism in the detection, drawing from other methods such as automatic data learning, data bases and artificial intelligence (Mishra et. al, 2013).

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

In the last decades, complex algorithms have been created for the detection of financial anomalies that allow relating artificial intelligence with fraud detection processes; these algorithms constantly learn to react to situations that are regarded as warning signs, and therefore to early determine an event that may occur in the future (Portela et. al, 2019). Fraud detection is a discipline implemented when prevention mechanisms have failed, maintaining a continuous evolution that overshadows evasive methods adopted by criminals (Pérez, 2018). These fraud detection systems must be cost-effective and efficient, that is to say, the cost of investing in the system must not exceed the loss caused by the fraud, and therefore, it is essential to use models and statistic rules to minimize those costs (Sandoval, 2019).

The research will be a documental study that will use bibliographic collection techniques and statistical comparison with the purpose of determining the feasibility concerning neural network algorithms in the detection of financial fraud, since they are considered as one of the most implemented algorithms in the community. A systematic mapping of the bibliography was carried out in order to identify the most implemented and updated components. The result of the bibliographic collection and analysis must answer: Which have been the updates or complements applied to the algorithm? Which has been the implementation and efficacy of the algorithm in the detection of fraud?

LITERATURE REVIEW

Financial Fraud Detection Methods

An intrusion detection system monitors the activity in a server or network, in such a way that it can obtain behavioral patterns, code signings or protocol analyses concerning possible attacks or attempts to breach security (Morales, 2018). The statistical methods for fraud detection vary depending on the size and type of data to be used. The majority of techniques compare the observed data with the expected data (Pérez, 2018).

Statistical methods for fraud detection might be supervised and non-supervised. Supervised methodologies utilize methods which are capable of distinguishing fraudulent behaviors from the ones that are not, nevertheless, in their construction, initial reliable data concerning the classification of individuals is used, therefore, this methodology exclusively detects types of fraud which have been previously identified; the system receives data sets with different sample, values and classification parameters, which are processed by a mathematical function that maps an input and output signal, thanks to this, the machine discovers what to do (Cáceres & Velásquez, 2018) (Singh & Jain, 2019). Simultaneously, non-supervised fraud detection methods detect patterns in conjunction with fraudulent components, not only in previous occurrences but also in the detection of new patterns. This is carried out by detecting which individuals deviate from the norm (Rodríguez Pérez, 2018). Initially, these methods have a poor performance, but as they calibrate, their actions improve (Cáceres & Velásquez, 2018) (Singh & Jain, 2019). Finally, mixed learning methods are implemented, which mix supervised and non-supervised mathematical algorithms for the detection of fraud. For its execution, they use a limited amount of previously known and unknown data, mainly used in credit card fraud detection (Singh & Jain, 2019).

Artificial Neural Networks

Artificial neural networks are similar in their mathematical model to the biological organization and behavior of neurons, which act as a device that is activated when it receives stimuli or disruption in their nerve terminals. These stimuli come from adjacent neurons or nerves. Once the neuron is activated (binary state 1), it begins to stimulate another by means

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

of extending and progressing towards the nerve terminal of adjacent neurons (Alvarado, 2003) (Rodríguez Pérez, 2018), as visualized in Figure 1.

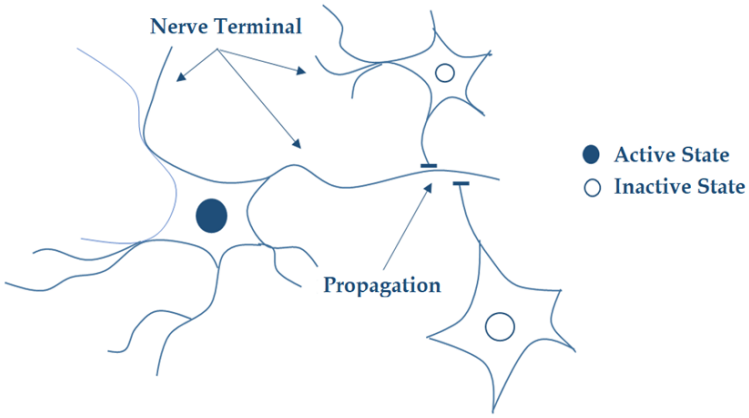

FIGURE 1
REAL NEURAL NETWORK

According to biological behavior, neurons have the ability to activate other neurons, causing a chain reaction that, depending on the amount of neurotransmitter fluid, can reduce or increase the initial stimulus (Alvarado, 2003).

Neural Network Algorithms (NNA)

A neural network probabilistic model is constituted by nodes that act as input, output, or middle processors, linking each node with the next node set by a series of weighted trajectories (Han & Pei, 2014). In financial fraud detection, feed-forward networks with only three layers are used (input, hidden and output). Input stimuli to the neural network are called feature vectors (X1, …, Xn). Weight vector (Wl , …, Wn) indicates the amount of stimuli that reaches the neuron. Finally, the signal emitted by the output unit (Y1, …, Yn) represents the probability of activity (1) or inactivity (0), used as measurement of criminal behavior suspicion (Alvarado, 2003), as shown in Figure 2.

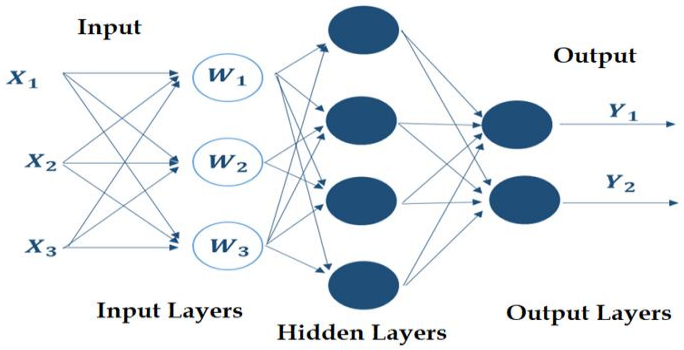

FIGURE 2
ARTIFICIAL NEURAL NETWORK

This method is capable of recognizing a complex behavior pattern and classifying each of its regions. Moreover, they are capable of manipulating a number of features that will allow them to perform their functions. Once the neural network is specified, it present a

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

quicker and more efficient response when analyzing input data (Alvarado, 2003; Rodríguez Pérez, 2018).

RESEARCH METHODOLOGY

The research stems from a document review, focusing on collecting studies of relevant cases, statistical analysis and data interpretation that supervised fraud detection systems use, by means of neural networks (Arias, 2012; Tamayo & Tamayo, 2003). Using the selected literature, the performance of NNA, its implementation as a method for detecting fraud, the updates or added complements, and analysis of its efficacy were examined.

Collection Strategy and Document Selection

The literature review concerning financial fraud detection examines the performance of different types of mathematical algorithms with the purpose of obtaining a background knowledge that provides information related with the most relevant ANNs in the last five years. Similarly, complementary techniques in ANN will be studied. The literature review was carried out in three stages. The first stage consisted in a conceptual analysis where keywords were selected for the search string related to the title of this research and according to the researcher's criteria, using the keywords "Mathematical Algorithms", "Neural Network", and "Financial fraud detection". The keywords were combined and implemented in Spanish and English in order to broaden the search range in the web platform.

The second stage is related to the data base used in the research. Google Scholar (http://scholar.google.es/) and Scopus (http://www.scopus.com/scopus/home.url) were used, since they allow Boolean operators in their advanced search tools, implementing keywords and narrowing the search results. Concerning temporal coverage, the literature search ranged from 2015 to 2020 and the type of document included journal articles, papers, reports, and research (Benavent et. al, 2011).

Finally, the search strategy was based on a Boolean operator scheme, where the keywords were placed in order to establish the conditions that the documents should meet. With the logical sum operator OR (In Spanish "O"), the keywords, synonyms and relevant concepts to the study were related. By means of the operator AND (In Spanish "Y"), the specific keywords that should appear in a document were established (Benavent et. al, 2011). Figure 3 displays the implemented search scheme.

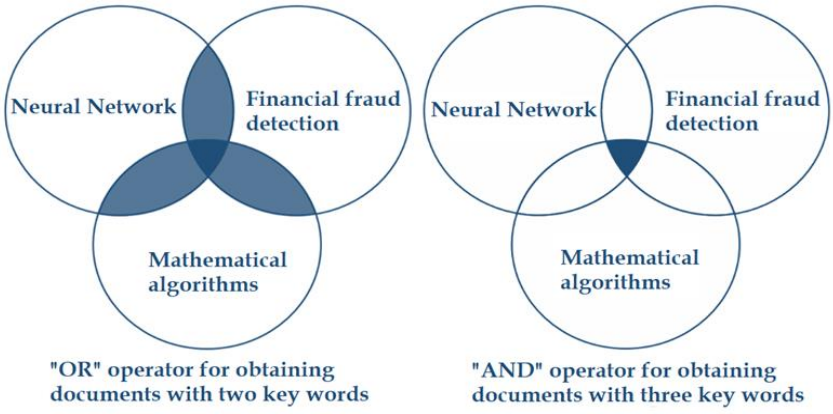

FIGURE 3
SEARCH SCHEME APPLYING BOOLEAN OPERATORS

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

According to the literature review, from each data base 118 documents were extracted: 87 from Google Scholar and 31 from Scopus. 21 duplicates were excluded as well as 65 documents whose access was restricted. Consequently, documents that meet the following conditions were included:

- The title indicated the application of neural networks in cases related to finance.
- Documents in Spanish and English
- Scientific documents (articles, reports and undergraduate works)

Documents with the following conditions were excluded:

- They were not primary studies.
- They were not related to financial fraud.
- They did not carry out a statistical comparison in their algorithm.

32 documents were obtained according to Kitchenham's, 2003, selection process. The documents were tabulated in Excel, where data concerning the authors, year of publication, main objective of the document, type of addressed problem, neural network models implemented, mathematical complements for the processing of data, and conclusions were extracted.

Comparative Analysis

The study of ANN was carried out by means of a comparative method, that allowed to describe each of the complementary techniques and therefore, to sustain the feasibility for its application (Pérez, 2007). Similarly, each of the algorithms is compared and analyzed by means of similarity and difference matrixes so as to determine which is the ideal one for the detection of financial fraud. This assessment was performed by means of pair matrixes or prioritization matrixes; these are a tool that allows making decisions using established criteria or conditions to rate the problem so as to determine the best option based on the decision-making methodology by Linán (2007). The feasibility and efficacy criteria for the rating were determined based on the literature review and the results provided by it, where the following questions were posed: Does the document clearly explain the algorithm along with the implemented components? Is the study experimental? Does the study give answer to the accuracy parameters of the algorithm? The level of importance of each question will be established based on a rating scale, as shown in Table 1.

Table 1
LEVEL OF IMPORTANCE OF THE QUESTIONS

Level of Importance	Rating Scale
Very good information	10
Good information	5
Acceptable information	1
Little information	0,2
Does not fulfill with the information	0,1

The comparison concerning the feasibility criteria by means of the pair matrix will allow calculating the Weighting Factor (WF) and Option Weight (OW) that will be used to determine the final rating of each of the algorithms, according to the procedure posed by Liñán (2007).

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

Efficacy of the Algorithm

When determining the efficacy in the model, the direct or indirect use of the bidimensional matrix was verified in each document, with a binary scheme that displays the behavior of the variables in each analyzed document. For the accuracy assessment when identifying the thematic classes visualized in Figure 4, where the columns are results given by the forecasting of the algorithm, the rows represent the real classification of the subject, while the diagonal of such matrix indicates the subjects that were correctly classified by the model (Sandoval, 2019; Liñán, 2007).

		Prediction	
		Positives	Negatives
Observation	Positives	True Positives(TP)	False Negatives (FN)
	Negatives	False Positives(FP)	True Negatives (TN)

FIGURE 4
CONFUSION MATRIX (CHAVÉZ SANDOVAL, 2019)

In the previous figure, the four terms to predict indicate the TP; amount of positive predictions that are correctly classified by the model, TN; fraudulent predictions that are correctly classified by the model, FP; number of positive predictions incorrectly classified by the model, and the FN that identify the fraudulent predictions which were incorrectly classified by the model (Sandoval, 2019).

From the evaluation of the algorithm by means of the confusion matrix, complementary performance indicators emerge that allow assessing the efficacy and quality of the studied algorithm. The accuracy establishes the quality of the predictions made, evaluating the ability of the model to correctly classify the positive and negative cases (Sandoval, 2019).

$$Global_{accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

RESULTS AND DISCUSSION

The literature compilation and selection presented a total of 32 documents that implement neural network algorithms for fraud detection. Each document was identified with the reference code D[x], where [x] is the document identifier in the bibliography. In Table 2 the distribution of each document by year can be appreciated. According to the aforementioned table, in 2019 a high tendency towards using the studied algorithm was noticed with 11 documents, whereas in 2015 and 2016 its use was rarely implemented by research, with one and two documents respectively.

Table 2
DOCUMENT DISTRIBUTION BY YEAR

Year	Amount of Documents	Document Identification
2020	4	D[1], D[18], D[38] y D[43],
2019	11	D [47], D[24], D[11], D[13], D[4], D[33], D[23], D[48], D[19], D[3] y D[40]

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

2018	8	D[6], D[5], D[2], D[32], D[26], D[51], D[46] y D[7]
2017	6	D[30], D[50], D[27], D[12], D[10] y D[14]
2016	1	D[34]
2015	2	D[45] y D[16]

Identification of the Boom of Neural Network Techniques Applied to Financial Fraud Detection

The documents present studies of the principal Neural Network Algorithm (NNA) and 27 complementary techniques were identified for the optimization of the ANN. In order to answer the posed question concerning which complements or updates have been applied to the algorithm, we begin from the information compiled in Table 3, were the techniques used in each document are displayed.

Tabla 3
IDENTIFICATION OF ANN COMPLEMENTARY TECHNIQUES

Assigned Variable	Complementary Technique	Document Identification
Y1	ANN with HAA (Harmony Annealing Algorithm) and HSA (Harmony Search Algorithm)	D[38]
Y2	ANN with	D[18]
Y3	Recurrent long-short term memory ANN (LSTM ANN)	D[43] y D[48]
Y4	Bidirectionnal recurrent ANN (BRNN)	D[1]
Y5	Twin ANN based on convolutional neural networks (CNN) and long-short term memory (LSTM)	D[47]
Y6	ANN with Denoiser autoencoder (DAE)	D[24] y D[4]
Y7	Probabilistic Neural Network (PNN)	D[11] y D[32],
Y8	Multilayer Feedforward Neural Networks	D[11] y D[26],
Y9	ANN with Genetic algorithm (GA)	D[33] y D[16]
Y10	ANN with SMOTE	D[10], D[33] y D[23]
Y11	ANN with data mining	D[40]
Y12	Deep Neural Network (DNN)	D[3], D[6] y D[5],
Y13	Deep Neural Network (DNN) with Latent Dirichlet Allocation (LDA)	D[6]
Y14	Neural network with Monarch Butterfly Optimization (MBO) algorithm	D[16]
Y15	Convolutional Deep Neural Networks (CDNN)	D[2]
Y16	Multilayer perceptron ANN (MLP)	D[50] y D[30]
Y17	ANN with Gradient Descent Adaptive (GDA) learning	D[27]
Y18	ANN with bayesian regularization learning (BR)	D[27]
Y19	ANN with bayesian regularization learning (LM)	D[27]
Y20	ANN with hidden layers	D[12] y D[14]
Y21	Convolutional ANN based on functional sequencing	D[51]
Y22	ANN with Radical Basis Functions (RBF)	D[7]
Y23	ANN with Back Propagation Algorithm (BP) y Particle Swarm Optimization (PSO)	D[45]
Y24	ANN with Particle Swarm Optimization (PSO)	D[16]
Y25	ANN with Gradient Boosting Decision Tree (XGBoost)	D[13] y D[5]
Y26	ANN with logic regression	D[19] y D[46]
Y27	ANN with Cortical Learning Algorithm (CLA) y hierarchical temporal memory algorithm (HTM)	D[34]

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

The study of ANN has been complemented by several techniques for optimizing its results. The table above showed that the main most studied complementary techniques have been deep neural network algorithms (DNN), convolutional neural networks (CNN) and neural networks with SMOTE. The DNNs present different versions of its implementations in documents D[2], D[6], D[3], y D[5]. In most current documents, specifically in the 2019 compilation; D[3] uses a sequential model based on DNN which is able to spot the sequential pattern of online transactions, drawing from memory networks in order to optimize the efficacy and interpretation of the model data. In 2018, document D[6] proposed a model for fraud detection in automobile insurance where an analysis of the features and description of the text was performed, in turn training the DNN based on such features and thus being able to detect anomalies on the claims. Although the studies found in D[2] and D[3] concerning DNN are studies in different fields of financial fraud, the results obtained in D[5] were more optimal when implementing these techniques on neural networks, since configurations in the parameters and structure of the network of up to 1000 series were made, with a learning ratio that ranges between 0,01 and 0,05; these experiments generated the efficient architecture of the DNN.

In the convolutional neural network studies (CNN), D[47], D[2] and D[51] can be found. The most updated research concerning this technique was presented in D[47], where a twin convolutional network to solve data sample imbalance problems of online transactions and implementation of the LSTM structure to generate user data in the memory of the model is displayed. In 2018 online transactions were approached with this technique from another angle in D[51], where the CNN elaborates a sequence layer of input features that induces the reorganization of the patterns of unprocessed transactions in order to generate different convolutional shapes. In the same year D[2] was published, which combined the two aforementioned techniques, where deep learning complements, detailed records of frauds by clients and extraction of learning features and classification of fraudulent events in order to generate a convolutional deep neural network model (CDNN) were used, outperforming other traditional automatic learning algorithms.

The third most implemented technique in neural networks is SMOTE, studied in D[10], D[33] and D[23]. In the three documents, SMOTE was used for preliminary data sampling, improving the forecasting, and identifying criminal anomalies. In 2017, D[10] puts SMOTE to test by applying it to different automatic learning methodologies, adding a cost matrix to the treatment of preliminary data. As a result, favorable results were obtained in the variables of the confusion matrix, as well as over 90% accuracy with the neural network algorithm.

It is evident that in the last 5 years the updates and complementary techniques in neural network algorithms has been varied, with research sustained by two pieces of research or in particular cases, by innovative models. From this array of applied techniques, the final objective of each study was emphasized, in order to indicate the projection and the best field for further development of the ANN, answering which has been the implementation of the fraud detection algorithm. By synthesizing the data, the aim of the algorithm update was extracted with the complementary technique. In table 4, the specific cases in the fraud detection field towards which the documents were focused on are displayed.

Table 4
APPLICATION ON FINANCIAL FRAUD DETECTION

Complementary Technique Objective	Document Identification
Credit Card Fraud Detection	D[43], D[1], D[27], D[50], D[12], D[24], D[4], D[33], D[48], D[40], D[34], D[26], D[46], D[7], D[45] y D[16]
Online Transactions Fraud Detection	D[18], D[10], D[47], D[11], D[13], D[23], D[19], D[3], D[51], D[2], D[32] y D[30]

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

Inadequate User Behavior Fraud Detection	D[38] y D[14]
Automobile Insurance Fraud Detection	D[6]
Online Security Breach Detection	D[5]

From the 32 compiled documents, 16 address credit card fraud detection, 12 documents address online transaction fraud and the remaining 4 were focused on automobile insurance fraud and inadequate user behavior.

Comparative Analysis of the Complementary Techniques for Neural Network Algorithms

Concerning the comparative results of efficacy and feasibility in each of the compiled techniques, the following criteria were determined: sustained theoretical background of the algorithm, description and mathematical development of the algorithm, experimental study of the algorithm and accuracy of the algorithm. The sustained theoretical background provides scientific support from previous research that guarantees the reliability and logic of the applied technique. The description and mathematical development establish the essential characteristics of the algorithm. The experimental study proves the verification of the algorithm implemented in the studies and the accuracy assesses the result of the algorithm in financial fraud detection.

In table V, the data matrix with the studied complementary techniques and the criteria to analyze are displayed. Such criteria are represented in the following fashion: X1 (sustained theoretical background of the algorithm), X2 (description and mathematical development of the algorithm), X3 (experimental study of the algorithm) and X4 (accuracy of the algorithm). The results shown in table 5 indicate the assessment of the criteria in each applied technique according to the previously mentioned rating scale. According to the criteria and rating scale, the displayed documents will present a total sum of over 20 points, considering it as research that provides results classified as “Good Information”.

Table 5
EFFICACY AND FEASIBILITY CRITERIA OF THE NEURAL NETWORK COMPLEMENTARY TECHNIQUES (DIFFERENCE AND SIMILARITY MATRIX)

Assigned variable	X1	X2	X3	X4	∑ Total
Y1	5	1	5	10	21
Y2	5	10	10	10	35
Y3	10	5	5	5	25
Y4	5	1	5	10	21
Y5	5	1	5	5	16
Y6	10	5	10	10	35
Y7	1	5	5	5	16
Y8	5	1	5	5	16
Y9	1	5	5	5	16
Y10	10	5	10	10	35
Y11	1	0.1	0.2	5	6.3
Y12	5	5	10	10	30
Y13	5	1	5	5	16
Y14	1	5	5	10	21
Y15	5	1	5	5	16

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

Y16	1	1	5	5	12
Y17	1	1	1	5	8
Y18	1	1	1	5	8
Y19	1	1	1	5	8
Y20	1	1	1	5	8
Y21	10	10	10	10	40
Y22	0.2	0.2	5	10	15.4
Y23	1	1	1	1	4
Y24	1	5	5	5	16
Y25	5	10	10	10	35
Y26	5	5	5	10	25
Y27	1	5	10	10	26

As seen in the previous table, 12 of the compiled documents fulfill several established criteria but convolutional ANN based on functional sequencing is the only one that met all of the feasibility and efficacy conditions with a total of 40 points. In the same vein, it is appreciated that ANN with automatic ontology learning, ANN with denoiser autoencoder (DAE), ANN with SMOTE, and ANN with Gradient Boosting Decision Tree (XGBoost) maintain the displayed characteristics of the experimental study and the accuracy results by means of a confusion matrix in each research, providing them a total of 35 points. However, given that the main purpose of the techniques is the detection of financial fraud, it was expected that all of them met the four criteria.

The similarity and difference matrix allows an initial comparative analysis of the complementary techniques. However, it does not provide a reliable foundation for the determination of the ideal technique in fraud detection by means of the neural network algorithm. To that effect, considering the analysis of the bibliographic review and the results in Table 6, the level of importance of each criterion for obtaining the complementary technique with the greater efficacy and feasibility is displayed. Table 6 shows the pair matrix according to the level of importance of each criteria for the calculation of the FP.

Table 6
PAIR MATRIX FOR THE LEVEL OF IMPORTANCE OF THE CRITERIA

	X1	**X2**	**X3**	**X4**	**Σ**	**FP=ΣXi/ ΣTotal**
X1	0	1	0.2	0.1	1.3	0.03
X2	5	0	1	0.2	6.2	0.13
X3	5	5	0	5	15	0.32
X4	10	10	5	0	25	0.53
Total					47.5	

Below, table VII with the calculation results concerning the weight of the option, expressed as PO=ΣYi/ΣTotal, are shown for each of the complementary techniques considering the established criteria. The obtention of the WO stems from the comparative matrixes of the complementary techniques, whose result demonstration can be appreciated in Table 7, found in the annex section.

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

Table 7
WEIGHTING OPTION FOR THE ANN COMPLEMENTARY TECHNIQUES FOR FINANCIAL FRAUD DETECTION

	PO_{x1}	PO_{X2}	PO_{X3}	PO_{X4}
Y1	0.04	0	0.04	0.11
Y2	0.04	0.14	0.12	0.11
Y3	0.14	0.04	0.04	0.04
Y4	0.04	0	0.04	0.11
Y5	0.04	0	0.04	0.04
Y6	0.14	0.04	0.13	0.11
Y7	0	0.04	0.04	0.04
Y8	0.04	0	0.04	0.04
Y9	0	0.04	0.04	0.04
Y10	0.14	0.04	0.13	0.11
Y11	0	0	0	0.04
Y12	0.04	0.04	0.13	0.11
Y13	0.04	0	0.04	0.04
Y14	0	0.04	0.04	0.11
Y15	0.04	0	0.04	0.04
Y16	0	0	0.04	0.04
Y17	0	0	0	0.04
Y18	0	0	0	0.04
Y19	0	0	0	0.04
Y20	0	0	0	0.04
Y21	0.14	0.14	0.13	0.11
Y22	0	0	0.04	0.11
Y23	0	0	0.12	0
Y24	0	0.04	0.04	0.04
Y25	0.04	0.14	0.13	0.11
Y26	0.04	0.04	0.04	0.11
Y27	0	0.04	0.13	0.11

Once having obtained the weight option and factor, the final assessment matrix for each technique is created; multiplying $FP_{Xi}\ x\ PO_{Xi}$ in the complementary techniques studied, visualized in Table 8.

Table 8
FINAL RATING OF THE ANN COMPLEMENTARY TECHNIQUES FOR FINANCIAL FRAUD DETECTION

	X1 FP x PO	**X2 FP x PO**	**X3 FP x PO**	**X4 FP x PO**	**Final Rating**
Y1	0,001	0,000	0,014	0,060	0,08
Y2	0,001	0,018	0,040	0,060	0,12
Y3	0,004	0,006	0,014	0,023	0,05
Y4	0,001	0,000	0,014	0,060	0,08
Y5	0,001	0,000	0,014	0,023	0,04
Y6	0,004	0,006	0,041	0,060	0,11

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

Y7	0,000	0,006	0,014	0,023	0,04
Y8	0,001	0,000	0,014	0,023	0,04
Y9	0,000	0,006	0,014	0,023	0,04
Y10	0,004	0,006	0,041	0,060	0,11
Y11	0,000	0,000	0,001	0,023	0,02
Y12	0,001	0,006	0,041	0,060	0,11
Y13	0,001	0,000	0,014	0,023	0,04
Y14	0,000	0,006	0,014	0,060	0,08
Y15	0,001	0,000	0,014	0,023	0,04
Y16	0,000	0,000	0,014	0,023	0,04
Y17	0,000	0,000	0,001	0,023	0,02
Y18	0,000	0,000	0,001	0,023	0,02
Y19	0,000	0,000	0,001	0,023	0,02
Y20	0,000	0,000	0,001	0,023	0,02
Y21	0,004	0,018	0,041	0,060	0,12
Y22	0,000	0,000	0,014	0,060	0,07
Y23	0,000	0,000	0,040	0,001	0,04
Y24	0,000	0,006	0,014	0,023	0,04
Y25	0,001	0,018	0,041	0,060	0,12
Y26	0,001	0,006	0,014	0,060	0,08
Y27	0,000	0,006	0,041	0,060	0,11

The results in Table VIII depict that the most efficient and feasible techniques, according to the four established criteria are: ANN with automatic ontology learning, convolutional ANN based on functional sequencing and ANN with Gradient Boosting Decision Tree (XGBoost). Since the comparative analysis considered not only the result of the research but also the theoretical background, algorithm development and experimental demonstration; these three techniques are well supported, and they fulfill the main objective of financial fraud detection by means of the neural network algorithm.

Studies that nearly obtain the highest score of the final rating are ANN with denoiser autoencoder, ANN with SMOTE, deep neural network (DNN) and ANN with cortical learning algorithm (CLA) and hierarchical temporal memory (HTM). The aforementioned studies achieve a good rating in the X3 (experimental study) and X4 (accuracy of the algorithm) criteria; however, they require a better theoretical background and a broader explanation of its algorithm development that reliably sustains the results obtained in the research.

Accuracy of the Neural Network Techniques for Financial Fraud Detection

The efficiency and optimization of the updates and complementary techniques in ANN were assessed through the accuracy result of the experimental models. Some compiled documents refer to more than one technique for neural networks, thus averaging the accuracy samples in such cases is necessary. In Figure 5 the average accuracy of the compiled techniques in the 32 documents is displayed.

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

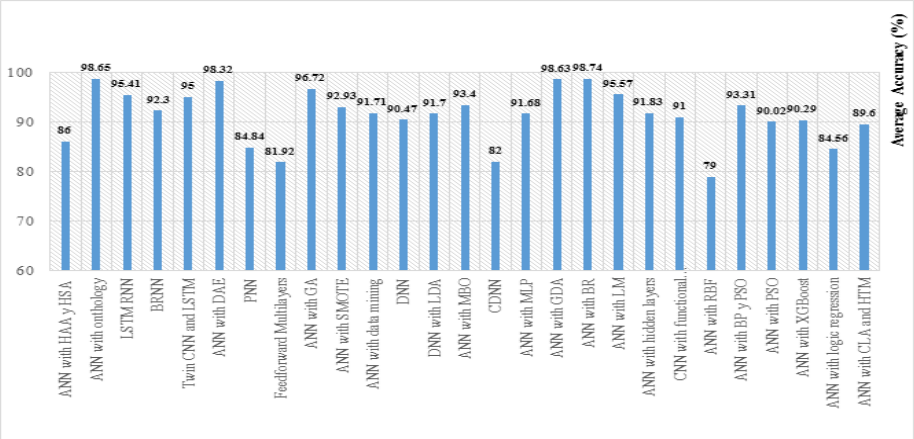

FIGURE 5
ACCURACY OF ANN COMPLEMENTARY TECHNIQUES

The figure shows an average accuracy range between 79% and 98.74%. In more noticeable techniques with an average accuracy percentage above 95%, D[27] can be found, where learning bases on Bayesian regularization Gradient Descent Adaptive GDA (98,63%) were utilized (98.74%) for the optimization of the neural network. D[18] utilized an ontology neural network (98.65%), in such research the mixture of automatic learning with an ontology based on payment systems was explained. On the other hand, in D[24] y D[4] the training of the automatic codifier and denoising for the reconstruction of normal data by means of an denoiser autoencoder (DAE) neural network were explained (98.32%). In D[33] and D[16] an artificial neural network with a genetic algorithm (GA) was configured (96.27%) with the purpose of maximizing the prediction in the fraud detection models. Finally, in D[43] y D[48], the learning was applied on long-short term memory recurrent neural network (LSTM RNN) for credit card fraud detection with an average percentage of 98%. Globally, the updates and ANN complementary techniques in the last 5 years have had an average accuracy of 91.32%, according to the compilation of this research.

CONCLUSIONS

The main problem in financial fraud detection is the recurrent illegal methods that, thanks to the technological and cybernetic advances, are reinvented and seek different methods to commit fraud. Since neural network algorithms are one of the most renowned financial fraud detection methods, it is necessary to have knowledge concerning its updates, scope and efficacy for its implementation in organizations which are vulnerable to financial fraud. By means of a bibliographic compilation, 32 documents that address the development of neural network algorithms for fraud detection were selected in the 2015 to 2020 period. It was proved that in 2019 there was a greater impact of research and techniques for neural networks in 11 studies, followed by 2018 with 8 documents and 2017 with 6 scientific articles. 27 updates and ANN complementary techniques were identified, thus deep neural network algorithms (DNN), convolutional neural networks (CNN) and neural networks with SMOTE being the most remarkable ones with greater implementation in the compiled pieces of research. However, a variety of techniques sustained by one or two pieces of research is observed, justifying the tendency of researchers towards innovating in financial fraud detection with ANN. In turn, the objectives of the studies were extracted, consequently noticing that credit card fraud detection was the most noticeable focus, applied in 16 documents as well as online transaction with 12 documents.

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

The final rating of the comparative analysis demonstrated that the ANN complementary techniques with automatic ontology learning, convolutional ANN based on functional sequencing and ANN with Gradient Boosting Decision Tree (XGBoost) fulfill the theoretical background that sustains the algorithm, description and mathematical development of the algorithm, experimental study of the algorithm and accuracy of the results, as established criteria that set the reliability of the research. For the efficacy assessment in the compiled techniques, the results of the experimental accuracy were extracted, where an average accuracy range of 79% to 98,74% with a global accuracy rate of 91,32%. This demonstrates that complementary techniques have a high rate of efficacy specifically in studies that mix different ANN automatic learning processes and preliminary data treatment such as ANN with automatic ontology learning, ANN with denoiser autoencoder (DAE), ANN with Gradient Descent Adaptive (GDA) learning and ANN with Bayesian regularization and learning, (BR) and (LM). The study of future research concerning the subject matter needs to further look into the training time of neural networks. Although the complementary techniques have had a high rate of efficacy in their results, the documents do not detail the cost and time invested in developing their ANN models. Therefore, it is recommended that the algorithm generation simultaneously considers the optimization time, cost, and data characterization.

REFERENCES

Adeniji Oluwashola, D., & Olatunji Oluwadare, O. (2020). Zero day attack prediction with parameter etting using bi-direction recurrent neural network in cyber security. *International Journal of Computer Science and Information Security (IJCSIS), 18*(3), 111-118.

Adetunmbi, A., Awoyemi, J. & Oluwadare, S. (2018). Effect of feature ranking on credit card fraud detection: comparative evaluation of four techniques. *2nd International Conference on Information and Communication Technology and Its Applications*.

Alae, C. & EL Hassane, I.E.H. (2018). ConvNets for fraud detection analysis. *Procedia Computer Science, 127*, 133-138.

Aleixandre, B.R., González, A.G., Gonzalez de Dios, J. & Alonso, A.A. (2011). Acta Pediátrica Española suspends its publication. *Acta Pediatr Esp*, 131-136.

Alvarado, J. (2003). Data mining algorithms. *ICM-ESPOL, 1*(2).

Álvarez, J.J., Badal, V.E. & Pavía, J. (2017). Using machine learning for financial fraud detection in the accounts of companies investigated for money laundering. *Working papers*.

Al-Shabi, M.A. (2019). Credit card fraud detection using auto encoder model in unbalanced

Anggraeny, A.S. (2020). The effect of implementing the financial management information system on the quality of the presentation of the pangkep regency government's financial statements. *Journal of Advanced Research in Economics and Administrative Sciences, 1*(1), 32-44.

Ankita, S., Mayank, P. & Manish, T. (2019). A comparative study to detect fraud financial statement using data mining and machine learning algorithms. *International Research Journal of Engineering and Technology (IRJET), 6*(8), 1492-1495.

Ankur, R. (2017). Comparative analysis of various classification algorithms in the case of fraud detection. *International Journal of Engineering Research & Technology (IJERT), 6*(9), 118-122.

Apoorv, T., Durvesh, S.D., Nitish, S., Aditya, R. & Viswanath, M. (2019). Fraud detection using deep learning. *International Journal of Research in Engineering, Science and Management*.

Ardavan, R. (2017). Identification of fraud in banking data and financial institutions using classification algorithms. *International Journal of Information, Security and Systems Management*, 663-667.

Arias, F.G. (2012). The research project, introduction to scientific methodology (6th ed.). *Episteme*.

Ashkan, Z., Ekrem, D. & Azamat, K. (2015). Profit-based artificial naural network (ANN) trained by migrating birds optimization: A case study in credit card fraud detection.

Chavéz, S.P. (2019). Comparison of statistical methods for detecting fraud in remote channels applied to the banking area. University of Concepción: Chile.

El Orche, A. & Bahaj, M. (2020). Approach to combine an ontology-based on payment system with neural network for transaction fraud detection. *Advances in Science,Technology and Engineering Systems Journal, 5*(2), 551-560.

Ermatita & Indrajani, S. (2019). Detection of frauds for debit card transactions at automated teller machine in Indonesia using neural network. *Journal of Physics: Conference Series, 1196*.

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

Gonzalez, E. (2018). Credit card fraud detection using data mining techniques. Santo Tomas University: Colombia.

Gutiérrez, P.F., Moreno, H.J., Echeverry, B. & Jaramillo, A. (2019). Use of intelligent systems for the detection of financial fraud. *Revista sinergia*, 25.

Han, J., Kamber , M. & Pei, J. (2014). Data mining, concepts and techniques. Elsevier science.

Huanzhuo, Y., Lin X. & Yanping, G. (2019). Detecting financial statement fraud using random forest with SMOTE. IOP Conference Series: Materials Science and Engineering.

Jinliang, Z., Junyi, Z. & Ping, J. (2019). Credit card fraud detection using autoencoder neural network.

Kitchenham, B. (2003). Procedures for performing systematic reviews. *British Journal of Management, 14*, 207-222.

Kumar, G.D. & Goyal, S. (2018). Credit risk prediction using artificial neural network algorithm. *Modern Education and Computer Science*.

Kunlin, Y. & Wei, X. (2019). Fraudmemory: Explainable memory-enhanced sequential neural networks for financial fraud detection. *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Mishra, C., Lal Gupta, D. & Singh, R. (2017). Credit card fraud identification using artificial neural networks. *International Journal of Computer Systems, 4*(7).

Mishra, P., Padhy, N. & Panigrahi, R. (2013). The survey of data minig applications and feature scope. *Asian Journal of Computer Science & Information Technology, 2*(3), 43-58.

Monirzadeh, Z., Habibzadeh, M. & Farajian, N. (2018). Detection of violations in credit cards of banks and financial in-stitutions based on artificial neural net-work and metaheuristic optimization algorithm. *International Journal of Advanced Computer Science and Applications, 9*(1).

Morales, C. (2018). Intruder Detection Model Using Learning Techniques.

Mubarek, M. & Adali, E. (2017). Multilayer perception neural network technique for fraud detection. *Computer Science and Engineering (UBMK)*, 383-387.

Ngai, E., Hu, Y., Wong, Y., Chen, Y. & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and anacademic review of literature. *Decision Support Systems, 50*(3), 559-569.

Nikfar, S. & Touraj, B. (2018). Detection of the suspicious transactions by integrating the neural network and bat algorithm. *Science Arena Publications Specialty Journal of Electronic and Computer Sciences, 4*(1), 9-19.

Nikita, S., Pratikesh, M., Rohit, S.M., Rahul, S., Chaman, K.M. & Shailendra, A. (2019). Credit card fraud detection techniques. *Zeichen Journal*.

Oghenekaro, L. & Ugwu, N.C. (2016). A novel machine learning approach to credit card fraud detection. *International Journal of Computer Applications, 140*(5), 45-50.

Pérez Liñán, A. (2007). The comparative method: fundamentals and recent developments. *University of Pittsburgh*.

Ramírez, A.A., Jenkins, M., Martínez, A. & Quesada, L.C. (2020). Using data mining and machine learning techniques for fraud detection in financial statements: A systematic literature mapping. *Iberian Journal of Information Systems and Technologies, 4*, 97-109.

Rodríguez, P.E. (2018). Analysis and detection of tax fraud using machine learning techniques. Universidad Politécnica de Madrid: Madrid.

Sajjad, D. (2020). Using harmony search algorithm in neural networks to improve fraud detection in banking system. *Computational Intelligence and Neuroscience*.

Salamanca, C.J. & Velásquez, V.P. (2018). Machine learning applied to financial data. Catholic University of Valparaiso: Valparaiso.

Sarika, J., Yashvi, J., Namrata, T. & Shripriya, D. (2019). A comparative analysis of various credit card fraud detection techniques. *International Journal of Recent Technology and Engineering (IJRTE), 7*(5S2), 402-407.

Shalev, S.B. (2014). Understanding machine learning: From theory to algorithms. Retrieved from http://shorturl.at/cmwQ4.

Singh, A. & Jain, A. (2019). An Empirical Study of AML approach for credit card fraud detection-financial transactions. *International Journal of Computers Communicatins & Control, 14*(6), 670-690.

Souad, L.M., Sainte, M.BA., Deem, A.G. & Albakri, J.Z. (2020). Enhancing credit card fraud detection using deep neural network. *Intelligent Computing, 2*, 301-313.

Tamayo, T.M. (2003). The process of scientific inquiry (4th Edition). Mexico: LIMUSA.

Tanmay, K. & Suvasini, P. (2015). Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network. *International Conference on Advances in Computing and Communication Engineering*.

Venkata, S.S., Balaji, G. & Venkateswara, R.G. (2018). Machine learning approaches for credit card fraud detection. *International Journal of Engineering & Technology, 7*(2).

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.

Vinayakumar, R., Ganesh, H.B., Prabaharan, P., Anand, K.M. & Soman, K.P. (2018). Deep-net: Deep neural network for cyber security use cases.

Xinxin, Z., Zhaohui, Z., Lizhi, W. & Pengwei, W. (2019). A model based on the Siamese neural network for the detection of fraud in online transactions. *International Joint Conference on Neural Networks (IJCNN)*.

Yibo, W. & Wei, X. (2018). Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. Retrieved from https://doi.org/10.1016/j.dss.2017.11.001.

Yogesh, P., Karim, O., Vassil, V., & Jun, L. (2019). Remote bank fraud detection framework using sequence learners. Internet banking and commerce magazine.

Zanin, M., Romance, M., Moral, S. & Criado, R. (2017). Credit card fraud detection through parenclitic network analysis. *Complexity, 48.*

Zhaohui, Z., Xinxin, Z., Xiaobo, Z., Lizhi, W. & Pengwei, W. (2018). A model based on convolutional neural network for online transaction fraud detection. Retrieved from https://doi.org/10.1155/2018/5680264.

Citation Information: Navarrete, A.C. & Gallegos, A.C. (2020). Neural Network Algorithms for Fraud Detection: A Comparison of the Complementary Techniques in the Last Five Years. *Journal of Management Information and Decision Sciences, 24*(S1), 1-16.