Financial Fraudulent Statements Detection through a Deep Dense Artificial Neural Network

Georgios S. Temponeras
Computational Intelligence Laboratory (CILab)
Department of Mathematics
University of Patras
GR-26110 Patras, Greece
temgeo@math.upatras.gr

Stamatios-Aggelos N. Alexandropoulos
Computational Intelligence Laboratory (CILab)
Department of Mathematics
University of Patras
GR-26110 Patras, Greece
alekst@math.upatras.gr

Sotiris B. Kotsiantis
Computational Intelligence Laboratory (CILab)
Department of Mathematics
University of Patras
GR-26110 Patras, Greece
sotos@math.upatras.gr

Michael N. Vrahatis
Computational Intelligence Laboratory (CILab)
Department of Mathematics
University of Patras
GR-26110 Patras, Greece
vrahatis@math.upatras.gr

***Abstract*—A very important issue in the financial field is to identify and reliably predict *Fraudulent Financial Statements (FFS)*. For this purpose, several Machine Learning models have been developed that identify the issues that are directly related to *FFS*. In this paper, we present a new predictive model for fraudulent detection through a deep dense artificial neural network. Specifically, a new forecasting model was tested experimentally using data from Greek companies. The obtained results showed that the proposed scheme is robust and promising.**

***Index Terms*—machine learning, fraudulent financial detection, deep learning techniques, prediction models**

I. Introduction

Over the past decade, financial scandals and *Fraudulent Financial Statements (FFS)* that shook the business world were quite a bit (*Enron* (2001), *Tyco* (2002), *American International Group (AIG)* (2005), *Lehman Brothers* (2008) etc.). Over the last decade, both in Europe, in U.S. and all over the globe this phenomenon has not disappeared (*Satyam* (2009), *Volkswagen Emissions* (2015), *Turing Pharmceuticals* (2015), *Bitconnect* (2018) etc.). For this reason, and taking into account the economic crisis that is particularly plaguing the countries of the European South, the need for timely and reliable prevention of such phenomena is particularly important. The interest in this problem is not just about financial scientists but concerns both businesses, investors, economic analysts, accountants, governments, and ordinary citizens among others. In order to avoid such incidents, the relevant European and U.S. committees have increased their corporate control and published financial data in order to ensure transparency. It is worth noting that, according to research carried out in Europe and U.S. [3], the reasons for such scandals are different. Mainly, human factor and management frauds contributed to most of these cases. However, attention is also concentrated in accounting systems.

The majority of business scandals are directly linked to accounting frauds. However, it is difficult to define precisely the term of "financial fraud" as it has different aspects [9]. Thus, the main features of an accounting fraud are the following: (a) *Misrepresentation*: Someone (an employee or the company) made a wrong statement either by mistake or intentionally (often intentionally), (b) *Significance of Misrepresentation*: The wrong statement is of high importance, (c) *Responsibility*: The person who made the misrepresentation financially damages the company and its prestige and (d) *Victim*: As a result, the shareholders, the investors and the state are financially impaired. Therefore, the main kinds of a financial fraud are two [3]: (a) *Misappropriation of assets*: In this case, a person, who is usually well-trusted and has an important position in the company, deceiving the company by stealing assets. These assets may be office supplies, intellectual property, cash etc. and (b) *Fraudulent financial reporting*: In this kind of fraud, someone misrepresents the accounting reports in order to present healthy financial statements. Thus, the company can secure a loan, in order to achieve financial goals in the markets, etc.

The progress that have been made in identifying and preventing accounting frauds in recent years is important. However, the techniques and algorithms used are necessary to be reliable and fast as possible. The models that have been used in past years are many and varied [4]. In the present work, we study the financial statements of different companies.

Supported by Hellenic State Scholarships Foundation (IKY).

Thus, we derive conclusions about possible accounting fraud using a deep dense artificial neural network. In our research, data from 164 Greek companies was used in order to reliably identify *FFS*. Thus, our primary purpose was to test a neural network architecture in predicting FFS. Specifically, our motivation was to examine if a deep architecture could perform robustness against well-known classifiers regarding FFS binary classification task in researching Greek data.

The rest of the paper is organized as follows. In the next section, a literature review and recent related works are presented. In *Section III*, the dataset of our work and the feature selection process are described. *Section IV* presents the experimental results and the comparison between the tested algorithms. Finally, *Section V* discusses the conclusion remarks and some future research aspects.

II. Literature review and related work

Finding a financial statement error, checking business's books, timely and valid recognition of a fraud are processes that require experience and are very difficult to be tackled. There may exist financial controls but sometimes these controls do not ensure the interests of investors or the company. This is so because someone is trying to mislead controllers or because the controller is not trusted. In [9] the authors present a comprehensive survey paper in relation to financial reporting fraud and other forms of misconduct. Among other things they mention: "*...financial frauds stem from the failure of gatekeepers, most significantly auditors, whose independence and concern for reputation had robbed their profession of the ability to protect investor interests*". Thus, one can easily conclude that there is a need to escape the formal controls. For this purpose, there are various models of *Machine Learning (ML)* that provide good, reliable solution to fraudulent detection problem.

An extensive presentation of statistical and computational models that automate controls to detect financial fraud was presented in [3]. In particular, the authors focused their research on models using *Computational Intelligence* techniques. They also presented the performance of algorithms for specific types of fraud. The reader interested in clustering techniques may study the review paper [5]. The authors in that work present well-known clustering techniques for unsupervised anomaly detection in the financial fraud detection task.

Over the past decade, many researchers have tested prediction models and several *ML* techniques in order to identify *FFS* and obtained some useful findings. In [15] the author presented a predicting model for *FFS* identification problem using *Support Vector Machines (SVMs)*. In his study he considered 117 *FFS* reports and 143 *non-FFS* reports from Chinese firms separated appropriately for model training and testing. According to the experimental results the provided method was more accurate regarding 10 and 6 financial ratio variables. In a similar context, in [16] Logistic Regression model was used in order to determine *FFS*. The authors tested their model using statements from 174 China firms. The experiments showed that the proposed model has the lower cost for *FFS* detection than the compared ones. A more extensive work in terms of the forecasting tested models was carried out by [17]. In this research *Artificial Neural Networks*, *Support Vector Machines*, *Genetic Programming*, *Logistic Regression* and *Group Method of Data Handling* methods were tested on 202 Chinese firms. The obtained results showed that *Probabilistic Neural Networks* achieve better accuracy than the other models.

In recent years, the rapid increase in data which we are looking to process, makes automate fraud detection task more necessary. This makes sense, since new technologies and information on the web makes the audits by people an unrealistic goal. A text mining method was proposed in [11] in order to tackle and analyze financial fraud cases. Recently, in [14] the authors presented a new model for detecting financial fraud, called *Artificial Fraud Detection Model (AFDM)*. Specifically, it was based on *Artificial Immune Systems* and improved fraud detection in relation to credit cards, in terms of forecasting accuracy, speed and cost compared to other basic models. A well-known visualization method, the *Self-Organizing Map (SOM)*, was used in an attempt to handle fraud detection problem. The authors in [13] proposed a method that used *SOM* technique in order to visualize user accounts and detect threshold-type. Their experimental results showed that the proposed method was effective. Furthermore, in [12] is presented a research which focused its attention in textual information of companies in financial statements. In particular, the failure of traditional auditing manners is overcome through the use of *Statistical Language Model* and *Latent Semantic Analysis*. The combination of these two techniques generated an *Integrated Language model* for fraudulent strategies identification with high accuracy.

A very informative and useful presentation regarding the use of data mining methods in *FFS* detection was provided in [2]. The main models that were tested are *Logistic Regression*, *Decision Trees*, and *Artificial Neural Networks*. The experiments conducted by the authors showed that the *ANNs* reached more accurate results than the other two models. In addition, in their research, the comparison between models' and experts' decision took place. In a similar project, the author in [1] developed a hybrid scheme through several data mining methods. Specifically, *Classification and Regression Trees (CART)* and *Chi squared Automatic Interaction Detector (CHAID)* both with *ANNs*, *SVMs* and *Bayesian belief network* were used in order to build a new model, called *CHAID-CART* model, with high accuracy. Moreover, multi-class learners and cost-sensitive learning for handling both class imbalance and asymmetric misclassification costs were used in the context of *FFS* detection by [6].

As it has been noted in [4], equally important with financial fraud is the unintentional financial statement. This occurs because both transactions entail similar negative results. The authors conducted a comparative study concerning well-known data mining techniques on the topic of both *FFS* and erroneous financial restatements recognition. They have pointed out that,

ANNs seem to overcome the performance of the other models. The main objective of such studies is to reliably recognize the features of a fraud. This goal is really hard to identify and most of the times is impractical without the use of *ML* techniques. In [8] a novel approach, called *CoDetect*, which can support both network information and feature information for *FFS* identification. Furthermore, the *CoDetect* tool can concurrently identifying financial fraud actions and the feature patterns correlated with the fraud actions. For an extensively study of Machine Learning methods in recognition of *FFS* and their applications in the business world, the interested reader is referred to the works [18] and [7].

In the Greek context, several attempts have been made in order to tackle *FFS* detection. In [20] a novel classification method for *FFS* identification was proposed. In particular, the approach of the *Multi-Criteria Decision Aid (MCDA)* idea and the application of the *UTilite's Additives DIScriminantes (UTADIS)* classification model was compared with well-known statistical models. The experimental results shown that the proposed method outperforms the others. In addition, a similar work to [4] was made by [19]. Recently, semi-supervised *ML* classification methods [22] and Active Learning techniques [21] were used in order to detect *FFS*.

III. Data description

In order to build a reliable classification model we used data from 164 Greek companies which are listed on the Athens Stock Exchange. For almost a quarter of the companies included in the dataset there were evidence or proof that they were involved in *FFS*. Our study focused in the following features in order to classify a statement as false statement:

(i) The auditors have reasonable uncertainties concerning the accuracy of the reports.
(ii) The competent audit authorities have found serious tax deficiencies.
(iii) The statement of Greek law regarding the negative net worth.
(iv) The addition of a firm in the Athens Stock Exchange classes of under observation and consultation omitted for objects connected with the falsification of the company's financial data
(v) The detection of serious tax offenses and / or pending court decision for reasons of false financial statement.

It it worth noting that the variables used in our research were quarried from approved financial statements, such as balance sheets and income accounts. This indicates that the value of this research is not defined by the fact that only Greek firm data was applied. Moreover, the variety of variables to be used as participants for support in the input vector was based upon earlier studies related to the binary problem of *FFS* detection. Further variables were additionally figured so as to make as many as possible predictors. In *Table I* is exhibited a brief description of the financial variables used in the current study.

In order to demonstrate how much each characteristic influences the induction, we estimate the influence of each attribute according to several statistical measures [23]. The *ReliefF* Score of each attribute is presented in *Table II*. In addition, a short description of each variable is exhibited in *Table I*. With respect to the unused variables, it seems that they do not affect the induction.

TABLE I
DESCRIPTION OF RESEARCH VARIABLES

Variable	Description
RLTC/RCR02	Return on Long-term capital/Return on Capital and Reserves 2002
TL/TA02	Total liabilities/Total assets 2002
AR/TA01	Accounts Receivable/Total Assets 2001
AR/TA02	Accounts Receivable/Total Assets 2002
DC/CA02	Deposits and cash/current assets 2002
NFA/TA	Net Fixed Assets/Total Assets
WC/TA 02	Working capital/total assets 2002
NDAP02	Number of days accounts payable 2002
LTD/TCR02	Long term debt/total capital and reserves 2002
CR/TL02	Capital and Reserves/total liabilities 2002
Z-SCORE02	Altman z-score 2002
EBT02/EBIT02	Earnings before tax 2002/Earnings before interest and tax 2002
CAR/NS	Change Accounts Receivable/Net Sales
EBIT/TA02	Earnings before interest and tax/total assets 2002
TA/CR02	Total Assets/Capital and Reserves 2002
WCL02	Working capital leveraged 2002
ITURN02	Inventory turnover 2002
CAR/TA	Change Accounts Receivable/Total Assets
CFO02	Cash flows from operations 2002
CR02	Current assets to current liabilities 2002
CFO01	Cash flows from operations 2001
GOCF	Growth of Operational Cash Flow
RCF/TA02	Results carried forward/total assets 2002
NDAR02	Number of days accounts receivable 2002
S/TA02	Sales/total assets 2002

TABLE II
AVERAGE RELIEFF SCORE OF RESEARCH VARIABLES

Variable	Score
RLTC/RCR02	0.02603371
TL/TA02	0.02577709
AR/TA01	0.02587121
AR/TA02	0.02257509
DC/CA02	0.01364156
NFA/TA	0.0133596
WC/TA02	0.02118785
NDAP02	0.01085013
LTD/TCR02	0.00798901
CR/TL02	0.00041943
Z-SCORE02	0.00047192
EBT02/EBIT02	0.00049986
CAR/NS	0.00071853
EBIT/TA02	0.00206301
TA/CR02	0.00208717
WCL02	0.00254562
ITURN02	0.00215535
CAR/TA	0.00320415
CFO02	0.00169573
CR02	0.00082761
CFO01	0.0009421
GOCF	0.00073566
RCF/TA02	0.00384807
NDAR02	0.00327257
S/TA02	0.00395956

IV. Proposed method and experimental results

In the current research, a *Deep Dense Multilayer Perceptron (DDMP)* is implemented. *ANNs* with two hidden layers can describe functions with any kind of shape. Currently, there are no theoretical aiming to use *ANNs* with more than two hidden layers for handling a simple dataset.

In order to test the effectiveness of our model, we compared the *DDMP* model with well-know learners, such as *Decision Trees (DT)*, $k-NN$, *Support Vector Machines (SVM)* and *Logistic Regression (LR)* model. In particular, from the first class of classifiers the widely used *C4.5* algorithm [24] was used, while the $3-NN$ algorithm [23] was included in our experiments concerning the $k-NN$ family. Moreover, the *Sequential Minimal Optimization (SMO)* method [23] was employed by the *SVM* class.

In the present work, we apply an *ANN* with two hidden layers. Determining the number of neurons in the hidden layers is a very crucial component of selecting the overall architecture of your *ANN*. Despite the fact that these layers do not instantly interact with the external environment, they have a huge impact on the final output. An important issue that has to be considered very thoroughly is the number of the neurons in these layers. If someone uses numerous neurons, this fact can occur in remarkable problems.

The first issue that worth noting is that, too many neurons in the hidden layers may occur in a very common problem, called *overfitting*. Overfitting occurs when an *ANN* is narrowly fitted to the training data that it is hard to generalize and make predictions for unknown data. An equally important difficulty may occur when the training input is large. Thus, if we use a huge amount of neurons in the hidden layers, this can increase the training time of the network noticeably. This phenomenon is not desirable. Therefore, the number of neurons need to be maintained as low as possible. This allows the *ANN* to have a good generalization ability. If one uses a big number of neurons, the ANN acquires a great memory ability. However, this occurs a network that can recall the training set to perfection but does not perform well on unknown examples.

Next, we explain in detail the characteristics of our *DDMP*. The first hidden layer consists of the 3/4 of the number of input attributes as neurons. In addition, the activation function that we used was the *ReLU* function. Following, the second hidden layer is composed by the 1/2 of the number of input attributes as the number of neurons. The *ReLU* activation function is also employed. Furthermore, the Drop-out technique of 10% is used and the *LOSSBinaryXENT* function was utilized as loss function. Moreover, the well-know Back Propagation (BP) method was used in order to perform the training of the network. According to the training procedure is worth noting the following properties: The data set consists of 41 fraudulent and 123 non-fraudulent instances that are described through 25 predictive variables, leading to a dataset with cardinality equal to 164. In addition, for each method, we run 10-fold cross-validation procedure and the average value of 10-fold cross-validations was measured.

In *Table III* the obtained accuracy of the compared methods and the F_1 score are exhibited. According to these, the proposed method of DDMP classified correctly the 93.7% of the total sample, 91.7% of the Fraud cases and 94.3% of the Non-Fraud cases. As a result, our model performs better than the other tested methods.

TABLE III
Accuracy of the compared methods in our dataset and F_1 score

	C4.5	**3-NN**	**LR**	**SMO**	**DDMP**
Total Accuracy (TA)	91.2	79.7	86.8	78.7	**93.7**
Fraud (F)	85.2	56.1	65.7	48.8	**91.7**
Non-Fraud (NF)	93.3	88.0	94.1	88.6	**94.3**
F_1 **score**	89.1	68.5	77.4	62.9	**93.0**

V. Conclusion remarks and future work

For a variety of reasons, financial fraud statements problem is rising in the business world. Huge information management conduces to a major problem and traditional control mechanisms cannot cope with this. In some cases, it is impossible to filter this information. For this reason, the field of Machine Learning with intelligent algorithms are necessarily entering the field of auditing principles and provide a reliable solution to the above issue [10].

Someone could argue that a comparatively short list of financial ratios mostly settles the classification outcomes. This information joined with *ML* techniques can present methods able to obtaining noteworthy classification efficiencies. Thus, the automated processes of *ML* field can provide a reliable solution to a time-consuming task. However, the role of experts remains very important in monitoring and evaluating the whole auditing procedure. The business world and the auditing systems through these algorithms can improve their skills and, also, can manage information that was impractical before.

In this paper, we presented a *Deep Dense Multilayer Perceptron* in order to tackle the problem of *FFS* detection. The experimental results showed that the provided model was performed better than the other methods. However, the robustness of our method has further to be studied. An interesting project for further testing could be the comparison of our *DDMP* with well-studied ensemble classifier models [25]–[27].

Acknowledgment

Stamatios-Aggelos N. Alexandropoulos is co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme «Human Resources Development, Education and Lifelong Learning»in the context of the project "Strengthening Human Resources Research Potential via Doctorate Research" (MIS-5000432), implemented by the State Scholarships Foundation (IKY).

References

[1] S. Chen, "Detection of fraudulent financial statements using the hybrid data mining approach" SpringerPlus, 5(1), 89, 2016.

[2] C. C. Lin, A. A., Chiu, S. Y., Huang and D. C. Yen, "Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts' judgments" Knowledge-Based Systems, 89, 459-470, 2015.
[3] J. West and M. Bhattacharya, " Intelligent financial fraud detection: a comprehensive review" Computers & security, 57, 47-66, 2016.
[4] I. Dutta, S. Dutta and B. Raahemi, "Detecting financial restatements using data mining techniques" Expert Systems with Applications, 90, 374-393, 2017.
[5] M. Ahmed, A. N. Mahmood and M. R. Islam, "A survey of anomaly detection techniques in financial domain" Future Generation Computer Systems, 55, 278-288, 2016.
[6] Y. J. Kim, B. Baik and S. Cho, "Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning" Expert Systems with Applications, 62, 32-43, 2016.
[7] Y. Li, W. Jiang, L. Yang and T. Wu, "On neural networks and learning systems for business computing" Neurocomputing, 275, 1150-1159, 2018.
[8] D. Huang, D. Mu, L. Yang and X. Cai, "CoDetect: financial fraud detection with anomaly feature detection" IEEE Access, 6, 19161-19174, 2018.
[9] D. Amiram, Z. Bozanic, J. D. Cox, Q. Dupont, J. M. Karpoff and R. Sloan, "Financial reporting fraud and other forms of misconduct: a multidisciplinary review of the literature" Review of Accounting Studies, 23(2), 732-783, 2018.
[10] J. Kokina and T. H. Davenport, "The emergence of artificial intelligence: How automation is changing auditing" Journal of Emerging Technologies in Accounting, 14(1), 115-122, 2017.
[11] M. Zaki and B. Theodoulidis, "Analyzing financial fraud cases using a linguistics-based text mining approach" Available at SSRN 2353834, 2013.
[12] W. Dong, S. S. Liao, B. Fang, X. Cheng, Z. Chen and W. Fan, "The Detection of Fraudulent Financial Statements: an Integrated Language Model" In PACIS (p. 383), 2014.
[13] D. Olszewski, "Fraud detection using self-organizing map visualizing the user profiles" Knowledge-Based Systems, 70, 324-334, 2014.
[14] N. S. Halvaiee and M. K. Akbari, "A novel model for credit card fraud detection using Artificial Immune Systems" Applied soft computing, 24, 40-49, 2014.
[15] Q. Deng, "Application of support vector machine in the detection of fraudulent financial statements" In 2009 4th International Conference on Computer Science & Education (pp. 1056-1059). IEEE, 2009.
[16] D. Yue, X. Wu, N. Shen and C. H. Chu, "Logistic regression for detecting fraudulent financial statement of listed companies in China" In 2009 International Conference on Artificial Intelligence and Computational Intelligence (Vol. 2, pp. 104-108). IEEE, 2009.
[17] P. Ravisankar, V. Ravi, G. R. Rao and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques" Decision Support Systems, 50(2), 491-500, 2011.
[18] P. Hajek and R. Henriques, "Mining corporate annual reports for intelligent detection of financial statement fraudŰA comparative study of machine learning methods" Knowledge-Based Systems, 128, 139-152, 2017.
[19] E. Kirkos, C. Spathis and Y. Manolopoulos, "Data mining techniques for the detection of fraudulent financial statements" Expert systems with applications, 32(4), 995-1003, 2007.
[20] S. Spathis, M. Doumpos and C. Zopounidis, "Detecting falsified financial statements: a comparative study using multicriteria analysis and multivariate statistical techniques" European Accounting Review, 11(3), 509-535, 2002.
[21] S. Karlos, G. Kostopoulos, S. Kotsiantis and V. Tampakas, "Using Active Learning Methods for Predicting Fraudulent Financial Statements" In International Conference on Engineering Applications of Neural Networks (pp. 351-362). Springer, Cham, 2017.
[22] S. Karlos, N. Fazakis, S. Kotsiantis and K. Sgarbas, "Semi-supervised forecasting of fraudulent financial statements" In Proceedings of the 20th Pan-Hellenic Conference on Informatics (p. 34). ACM, 2016.
[23] I. H. Witten, E. Frank, M. A. Hall and C. J. Pal, "Data Mining: Practical machine learning tools and techniques" Morgan Kaufmann, 2016.
[24] J. R. Quinlan, "C4. 5: Programs for machine learning" Morgan Kaufmann, San Francisco. C4. 5: Programs for machine learning. Morgan Kaufmann, San Francisco, 1993.
[25] L. Breiman, "Bagging predictors" Machine learning, 24(2), 123-140, 1996.
[26] Y. Freund and R. E. Schapire, "Experiments with a new boosting algorithm" In icml, Vol. 96, pp. 148-156, 1996.
[27] J. J. Rodriguez, L. I. Kuncheva and C. J. Alonso, "Rotation forest: A new classifier ensemble method" IEEE transactions on pattern analysis and machine intelligence, 28(10), 1619-1630, 2006.