Modelling Credit Card Payment Fraud Detection System For Financial Institutions In Nigeria Using An Improved Firefly Algorithm

4 authors:

Rufai Kazeem Idowu
Tai Solarin University of Education
13 PUBLICATIONS **27** CITATIONS
SEE PROFILE

Usman Opeyemi Lateef
Tai Solarin University of Education
36 PUBLICATIONS **88** CITATIONS
SEE PROFILE

Ravie Chandren Muniyandi
Universiti Kebangsaan Malaysia
107 PUBLICATIONS **632** CITATIONS
SEE PROFILE

Lateef O. Adewale Oyinkanola
The Polytechnic, Ibadan
8 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Modelling Credit Card Payment Fraud Detection System For Financial Institutions In Nigeria Using An Improved Firefly Algorithm

Kazeem Idowu RUFAI[1*], Opeyemi Lateef USMAN[2], Ravie Chandren MUNIYANDI[3] , Lateef O.A OYINKANOLA[4]

[1,2]Computer Science Department, Tai Solarin University of Education, P.M.B. 2118, Ijagun, Ijebu-Ode, Ogun State, Nigeria.

[2,3]Research Centre for Cyber Security, Faculty of Information Science and Technology, University Kebangsaan Malaysia,43600 UKM Bangi, Selangor, Malaysia.

[4]Physics Department, The Polytechnic, Ibadan, Oyo State, Nigeria.

Emails: rufaiki@tasued.edu.ng; usmanol@tasued.edu.ng; ravie@ukm.edu.my; oyinkanola2003@gmail.com

Abstract

The need to develop an ICT-based mechanism for detecting and preventing fraudulent financial transactions from large volumes of available financial datasets, such as credit cards, motivated this study. Existing methods are either based on machine learning algorithms or on meta-heuristic optimization algorithms to achieve the aforementioned goals. The convergence of an algorithm is one of its most important characteristics as it is possible to analyze and prove whether an algorithm converges using mathematical theoretical knowledge. Therefore, an appropriate strategy for improving the speed of convergence randomization of a nonlinear optimization algorithm must be implemented. In this paper, a nonlinear convergence factor based on tangent trigonometric function is proposed and embedded into the existing Firefly Algorithm (FA). Using credit card transaction datasets from a Nigerian financial institution's website, the goal is to find the best global solution and improve convergence search speed. When compared to state-of-the-art methods, the proposed improved FA has a high randomized convergence speed with a success rate of 3724±573 (100%). Finally, when it comes to problems like detecting credit card payment fraud with a greater emphasis on convergence speed, the proposed algorithm has an excellent success rate for finding global optima.

Keywords: *Credit card; Firefly algorithm, Fraud detection, Optimization, Convergence factor*

1. Introduction

Fraud is one of the most serious legal problems bedeviling the credit card industry, and it has been on the rise in recent years (Poongodi & Kumar, 2021). In Nigeria, there is a growing interest in banking ethics, as well as the morality of financial sector fraud. Fraud is the illegal acquisition of goods, services, and/or money, and it deals with criminal activity situations that are frequently difficult to classify. Credit cards are one of the most common targets for fraudsters; others in this category include personal loans, mortgages, and retail. Furthermore, the face of fraud has changed greatly over the last few decades as a result of technological advances and innovations. It is then necessary to assist companies, particularly financial institutions such as banks, in detecting critical frauds and providing effective counter-measures as they emerge (Alhazmi & Aljehane, 2020; Amanze & Onukwugha, 2018; Anderson, 2007; Maniraj et al., 2019; More et al., 2020). Credit card fraud can manifest itself in a variety of ways, depending on the type of fraud involved; it includes bankruptcy fraud, theft or counterfeit fraud, fraud in application, and fraud in conduct. According to the European Central Bank (ECB), the total amount of credit card payment-related fraud committed in the single Euro payment regions in 2010 reached €1.26 billion (Bahnsen et al., 2013). Also, according to Juniper Research Unit in Basingstoke, England, companies in e-commerce and financial institutions worldwide will lose more than $200 billion in credit card payment fraud between 2020 and 2024. Meanwhile, gross losses from UK credit card fraud have risen dramatically since 1997, from £122 million in 1997 to over £423 million in 2020 (Association for Payment Clearing Services, 2020; Juniper Research, 2020). Furthermore, according to recent reports, Nigeria's financial institutions lost, in a total of 19,531 fraudulent transactions, total sum of N18.2 billion in 2016, with electronic platforms accounting for 77% of these transactions and credit cards accounting for 85% of the loss (Amanze & Onukwugha, 2018). As a result of the foregoing statistics, detecting and preventing fraudulent financial transactions from large volumes of available financial datasets, such as credit cards, is an important research topic in banking and financial institutions today, thereby justifying the need for this study.

Several approaches to detecting fraud in credit card payment systems have been proposed in previous studies, the majority of which are based on machine learning and meta-heuristic optimization algorithms. Dornadula and Greetha (2019) designed and developed a fraud detection method for Streaming Transaction Data (STD) with the goal of analyzing, clustering, and extracting behavioural patterns of cardholders' historical transactions using a European credit card fraud dataset and various machine learning algorithms. Lucas et al. (2020) used the Hidden Markov Model (HHM) and the Random Forest classifier to model and extract features for predicting the likelihood of fraud in a sequence of credit cardholders' historical transactions. To detect credit card fraud, Jain et al. (2016) proposed using rough collection and decision tree methods. Similarly, Vadoodparast et al. (2015) proposed a dynamic KDA model that combines three clustering algorithms: K-Means, DBScan, and Agglomerative Clustering Algorithm (ACA) to detect electronic fraudulent transactions in credit cards with the advantage of fast processing time, allowing multiple customers to detect suspicious transactions at the same time. Bahnsen et al. (2013) proposed using the Bayes minimum risk classifier to detect cost-sensitive credit card fraud. This study demonstrated that using the real cost parameter when developing a cost-sensitive minimal risk classifier from Bayes results in much better fraud detection and higher savings. However, the aforementioned machine learning methods have several limitations, including high false alarm rates, low detection rates, long processing times, local optimal problem, data imbalance, the curse of dimensionality (Usman et al., 2021), and the inability to detect credit card fraud as a series of events. To address local optimal problem that characterized backpropagation algorithm, Bentley et al. (2000) also proposed a meta-heuristic optimization based on genetic algorithm and genetic programming. This algorithm was developed with some logic rules for categorizing credit card transactions into suspected and unsuspected transactions. Duman and Ozcelik (2011) proposed combining two meta-heuristic algorithms: genetic algorithm and scatter search, with the introduction of a novel cost function to be minimized, to identify fraudulent transactions in credit card payment systems. Darwish (2020) proposed a two-level credit card fraud tracking model based on the K-means algorithm and the Artificial Bee Colony (ABC) algorithm that, when implemented with imbalanced datasets, helps to accelerate the convergence of fraud detection global search. Lastly, Duman et al. (2013) used a meta-heuristic Migrating Bird Optimization (MBO) algorithm to develop a credit card fraud detection solution for a major Turkish bank.

Firefly Algorithm (FA), proposed by Xin-She Yang at Cambridge University and first published in 2008, has attracted significant attention in many applications such as image processing, engineering, scheduling pattern, load dispatch, travel salesman problem (TSP) and financial fraud detection, to mention but a few (Apostolopoulos & Vlachos, 2011; Chatterjee et al., 2012; Sayadi et al., 2010; X.-S. Yang, 2013; X. Yang & Karamanoglu, 2020; Yousif et al., 2011). It employs the unique flashing behaviour of fireflies to generate an objective function within an optimization problem. FA can solve extremely nonlinear, multimodal design problems effectively by selecting the best features with consistently better timing and optimal search performance than its equivalents with the best global convergence, such as ABC, Ant Colony Optimization (ACO), and Particle Swam Optimization (PSO). Based on the FA principle, Folorunso (2015) developed a method for generating and detecting fraudulent transactions on credit card payment systems. Most existing optimization algorithms for detecting credit card frauds have a few key parameters that steer them in the direction of the best global solution. In FA, attractiveness, distance, and movement between fireflies are examples of these parameters. To avoid divergence, these parameters must be reasonably adjusted. One of the most important characteristics of an algorithm is its convergence. With the help of mathematics theoretical knowledge, it is possible to analyze and prove whether the algorithm converges. As a result, an appropriate strategy must be integrated to further improve the speed of convergence randomization of a nonlinear optimization algorithm. In this study, a nonlinear convergence factor based on tangent trigonometric function is embedded into existing FA and proposed. The goal is to find the best global solution and improve convergence search speed by using credit card transaction data from a Nigerian financial institution's website. As a result, the primary objective of this paper is to model the credit card fraud detection system for Nigerian financial institutions using an improved firefly meta-heuristic optimization algorithm.

The remaining part of this paper is organized as follows: Section 2 discusses related works. Section 3 describes the materials and methods used in the study in detail, including parameter definition, data sources, proposed architecture, and implementation setup. Sections 4 and 5 discuss key findings, implications, and wrap up the paper.

2. Related Works

Several attempts made over the last two decades to address the problem of credit card transactions fraud using soft-computing paradigms are discussed below:

Srivastava et al. (2008) used the Hidden Markov Model (HMM) to describe the credit card transaction process. For this analysis, HMM was used as a detector for fraudulent transactions after being programmed with specific cardholder behaviour. Following the training phase, the incoming credit card transactions were checked using the model. If HMM did not accept the incoming credit card transaction, it would be considered a fraud. The main disadvantage of this approach is that HMM generates a high rate of false alarms in both positive and negative situations.

Khan et al. (2014) proposed a simulated annealing algorithm based on Artificial Neural Network (ANN) weight randomization to improve the detection of credit card fraud. The simulated annealing algorithm was used during ANN training to randomize the weights of each neural connection based on previous transaction values and current temperature. The above configuration was then used to classify the test data that was not used during the training process into fraudulent and non-fraudulent cases, with a success rate of 65%. The study is limited by a high false alarm rate due to the non-uniform activities of credit card users.

Grammar-based Multi-Objective Genetic Programming with Statistical Selection Learning (GBMGP-SSL) was developed by Li and Wong (2015) to improve the efficiency of detecting financial fraud. Token competition was used in this method to change the objective values of each solution. Similar objective values of different definitions were separated to ensure diversity.

For detecting credit card fraud, Prakash and Chandrasekar (2015) proposed the Optimized Multiple Semi-Hidden Markov Model (OMSHMM). The proposed method was also used to identify the model's optimized parameters. Furthermore, the Cuckoo Search Algorithm (CSA) was used in conjunction with OMSHMM to determine the number of states and model parameters. CSA has a low convergence rate, and the local optimal value is defined.

Halvaiee and Akbari (2014) proposed an Artificial Immune System-based Fraud Detection Model (AIS-FDM) for detecting credit card fraudulent behaviour. In this approach, AIS was used as the artificial immune detection mechanism. An algorithm inspired by the immune system was developed to improve the accuracy of fraud detection. It does not, however, improve classification accuracy.

Van Vlasselaer et al. (2015) proposed Anomaly Prevention Using Advanced Transaction Exploration (APATE) for credit card fraud detection. The proposed approach combines past transactional trends and customer actions into useful features that are then matched with incoming transactions. APATE has the advantage of being able to detect fraudulent transactions in as little as six seconds. The proposed method, however, was inapplicable to defining a group of fraudulent behaviour.

Duman and Ozcelik (2011) addressed the issue of detecting fraudulent credit card transactions. For better classification performance, the authors first introduced a new classification cost function for fraud detection, and then combined two meta-heuristic algorithms, such as genetic algorithms, with the scatter search. However, when classification issues arise during the identification process, additional classification methods are required to resolve them. Duman et al. (2013), as an alternative, developed a credit card fraud detection solution for a major Turkish bank using a meta-heuristic Migrating Bird Optimization (MBO) algorithm capable of distinguishing fraud when the number of alerts involved is relatively small.

Mahmoudi and Duman (2015) proposed the Fisher Discriminant Function (FDF) for credit card fraud detection. The Fisher Linear Discriminant Classifier (FLDC) has modified the dimensionality reduction process to find the best solution and divide dimensional space into two or more subspaces. The aim of the separation is to reduce class overlap. Some adjustments were also made to enhance the efficiency of the classification, considering far less fraudulent transactions from the dataset. Meanwhile, costs of misclassification were not put into consideration. Mahmoudi and Duman (2015) further proposed the Modified Fisher Discriminant Function (MFDF) for detecting credit card fraud. This method increases the sensitivity of the traditional FDF to important instances and maximizes profit for both fraudulent and legitimate transactions. The high rate of misclassification of negative alerts remains a major bottleneck in this approach.

Krivko (2010) used a data-customized approach to detect plastic card fraud. To compensate for the shortcomings of the individual methods, the proposed approach combined supervised and unsupervised methodologies. The proposed method first tracked changes in transaction behaviour over time, and then assigned scores to each fraudulent transaction based on the assumption of fraud behaviour. The rule-based filters were fed a sequence of transactions with scores greater than a certain threshold value. The rules were then generated from those transactional records with the goal of improving the detection's performance. However, it is also critical to keep the saving information in order to improve detection.

Olszewski (2014) proposed a method for detecting fraud based on visualization and classification using an unsupervised Self-Organized Map (SOM). SOM was used to visualize the multidimensional data of typical user accounts on a regular basis in order to detect fraudulent transactions. The detected fraud was then analyzed using a threshold-type binary classification algorithm from a specific user's actual transactions. The proposed method has a limitation in that it affects the detection capability of supervised data mining methods.

To detect fraudulent behavior, Lei and Ghorbani (2012) proposed an Improved Competitive Learning Network (ICLN) and a clustering algorithm of the Supervised Improved Competitive Learning Network (SICLN). To represent the data centre, ICLN's neural network was programmed to use the reward-punishment update rule. SICLN then used the updated rule and achieved better results during clustering by assigning class labels to guide the training process. Improving the SICLN's convergence speed necessitates the use of an efficient method.

Ravisankar et al. (2011) compared data-driven fraud detection approaches based on past fraudulent behaviour and financial ratios. The authors compared methods for detecting fraud in business financial statements, including Multilayer Feed Forward Neural Network (MFFNN), Support Vector Machines (SVM), Genetic Programming (GP), Group Method of Data Handling (GMDH), Logistic Regression (LR), and Probabilistic Neural Network (PNN). Then, feature selection methods were used to extract fraudulent transactions from the dataset, and fraud behaviour was found to be effective. GP which was found to be the best method among others suffers from the delivery of marginally less accuracy.

To detect fraudulent financial reporting activities, Glancy and Yadav (2011) proposed a Computational Fraud Detection Model (CFDM). CFDM discovered incorrect details in annual filings with the assistance of the US Securities and Exchange Commission (SEC) using information presented in a text document for the detection process.

The Beneish m-score was evaluated in the detection of financial fraud by Tarjo and Herawati (2015). The proposed method was a probabilistic model that was used to identify companies that appeared to be involved in financial transaction fraud. If a company has a high m-score, it is more likely that fraud will occur. This approach, however, does not result in maximum detection accuracy.

Based on the FA principle, Folorunso (2015) created a method for generating and detecting fraudulent transactions on credit card payment systems. The FA is implemented using INSTAT+V3.36 and MATLAB, with a few parameters changed to adapt it to fraud detection in credit card payment systems. Other recent methods for detecting credit card fraud include supervised learning, Support Vector Machine with Information Gain (SVMIG), and Deep Learning (DL) (Azhan & Meraj, 2020; More et al., 2020; Najadat et al., 2020; Poongodi & Kumar, 2021). FA is a metaheuristic algorithm that uses the unique flashing behaviour of fireflies to create an objective function within an optimization problem. This was introduced in 2008 by Xin-She Yang at Cambridge University (Yang & Karamanoglu, 2020) and has seen widespread use in solving engineering and other real-world problems such as fracture optimization, privacy preservation, and financial fraud detection (Kakandikar & Kulkarni, 2020; Langari et al., 2020). Farahani et al. (2011) proposed a multiswarm FA-based approach in which the exclusion parameter was used to make each swarm interact locally and the anti-convergence operator was used to make each swarm interact globally. FA has been investigated in addition to the multiswarm method, which can select the best solution from a swarm of relevant swarms. However, due to swarm's missed peaks, this approach reduces detection efficiency. FA parameters have undergone several modifications and enhancements since their introduction to date in order to adapt the algorithm to specific problems or improve algorithm convergence (Bidar et al., 2018; Wu et al., 2020). This study proposes a typical example.

3. Materials and Methods

3.1 Proposed System Architecture

Figure 1 depicts a simplified architecture of the proposed system. The proposed architecture makes use of an improved FA to analyze all credit card transactions and report any suspicious or confirmed fraudulent transactions to the appropriate authorities (bank/security agency). Professionals investigate these reports and contact cardholders to determine whether the transaction was legitimate or fraudulent. The investigators provide feedback to the automated system, which is then used to train and update the parameters of FA in order to improve its fraud detection performance over time.

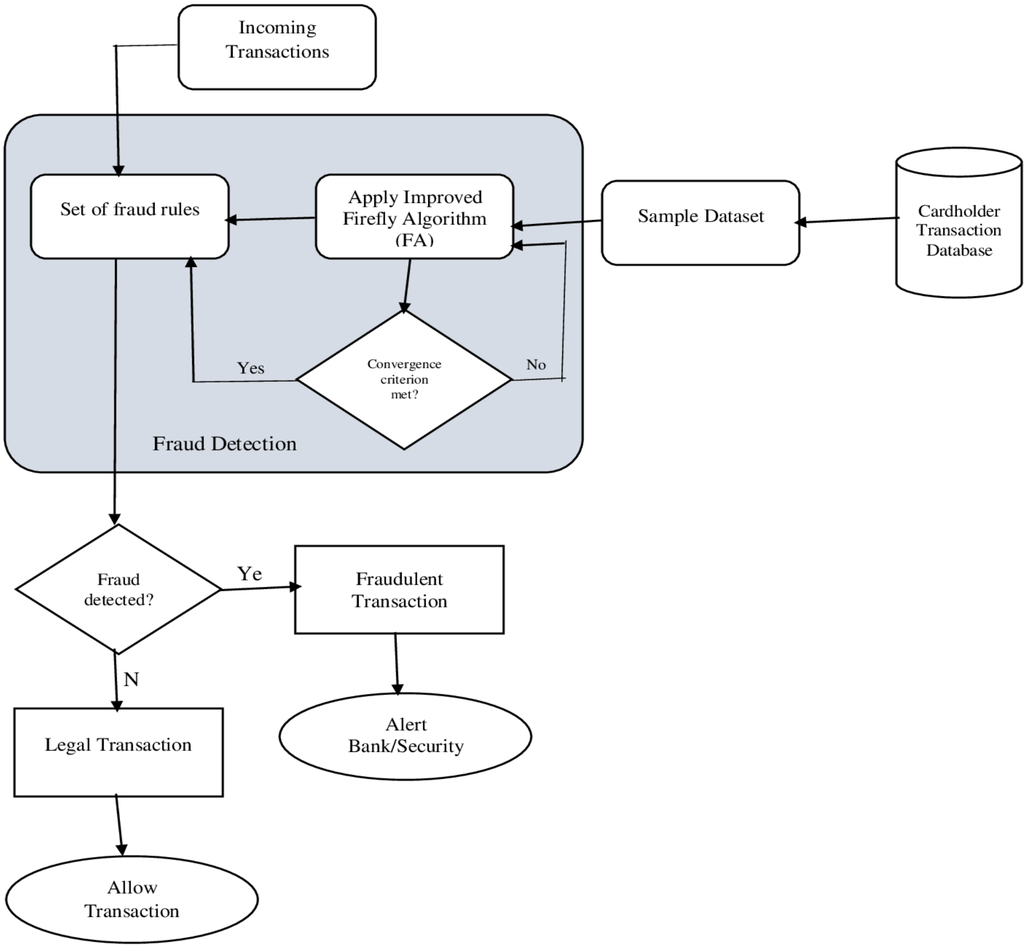


Figure 1. Proposed System Architecture

3.2 Parameter Definition and Improve FA Modelling

The flashing light of FA can be expressed in such a way that three idealized rules, which serve as the foundation for developing a mathematical model for the FA, are linked to an objective function. These rules include (Yang, 2010, 2013b; Yang & Karamanoglu, 2020):

i. Since all fireflies are unisex, one firefly will be attracted to another firefly irrespective of sex.
ii. Their attractiveness is proportional to their brightness. Therefore, for any two flashing fireflies, the less bright one will move towards the brighter one. The attractiveness is proportional to the brightness, and inversely proportional to the distance between them.
iii. The landscape of the objective function influences or determines the brightness of a firefly.

For a maximization problem, the brightness can be directly proportional to the value of the objective function. (Raja et al., 2013). Because both light intensity and attractiveness influence firefly movement in the FA, their variations should be defined.

3.2.1 Attractiveness

For the sake of simplicity, the attractiveness (*β*) of a firefly is assumed to be determined by its brightness (*I*), which varies with distance (*r*) and is thus correlated with the encoded objective function. Equations (1)-(6) can be used to model the attractiveness (*β*) of fireflies in FA as follows (Yang & He, 2013):

$$I(r) = I_0 * e^{-\gamma r^2} \tag{1}$$

$$I(r) = \frac{I_0}{1+\gamma r^2} \tag{2}$$

$$e^{-\gamma r^2} \approx 1 - \gamma r^2 + \frac{1}{2}\gamma^2 r^4 + \cdots \tag{3}$$

$$\frac{1}{1+\gamma r^2} \approx 1 - \gamma r^2 + \gamma^2 r^4 + \cdots \tag{4}$$

$$\beta(r) = \beta_0 * e^{-\gamma r^2} \tag{5}$$

$$\beta(r) = \beta_0 * e^{-\gamma r^m}, for\ m \geq 1 \tag{6}$$

where β_0 signifies the maximum attractiveness (at r=0) which defines the light absorption coefficient (γ) that controls the decrement of light intensity. The light absorption parameter is assumed exponentially and monotonically.

3.2.2 Distance

The distance (r_{ij}) between two fireflies *i* and *j* at position x_i and x_j according to (Yang & He, 2013), is defined by equation (7) as follows:

$$r_{ij} = \|X_i - X_j\| = \sqrt{\sum_{k=1}^{d}(x_{i,k} - x_{j,k})^2} \tag{7}$$

where $x_{i,j}$ is the *k*-th component of spatial coordinate x_i of *i*-th firefly and *d* is the number of dimensions.

3.2.3 Movement

The movement of a firefly i is defined by the equation (8) as follows:

$$X_i = X_i + \beta_0 * e^{-\gamma r^2}\left(X_j - X_i\right) + \alpha\left(rand - \tfrac{1}{2}\right) \qquad (8)$$

where X_I (the first term of the equation) denotes a firefly *i*'s current position, the second term of the equation denotes a firefly *i*'s attractiveness towards firefly *j*, and the third term of the equation is used for random movement if no brighter firefly exists (rand is a random number generator uniformly distributed in the range [0,1]). In the vast majority of cases $\alpha \epsilon (0,1)$, $\beta_0=1$. In practice, the light absorption coefficient ranges between 0.1 and 10. This parameter describes the variation in attractiveness, and its value determines the rate of FA convergence.

It is worth noting that the distance *r* is not limited to the Euclidean distance. Two important limiting constraints include:

If $\gamma \rightarrow 0$, then $\beta(r)=\beta_0$ implying particle swam optimization (PSO), and

If $\gamma \rightarrow \infty$, then $\beta(r)=\delta(r)$ implying random search.

To improve the convergence speed of FA, a nonlinear convergence factor based on the tangent trigonometric function is incorporated into equation (8) as follows:

$$\gamma = \gamma_{initial} - \left(\gamma_{initial} - \gamma_{final}\right) * \tan\left(\pi \frac{l}{\varepsilon * l_{max}}\right) \qquad (9)$$

where γ_{initial}, γ_{final} are the initial and final values of light absorption coefficient γ respectively, ε is the adjusted coefficient and is taken as (ε=4), *l* is the initialized iteration number while $l_{\max}$ is the maximum iteration number. Figure 2 depicts the linear and nonlinear convergence factor curves. The improved convergence factor has a small absolute value at the beginning of the iteration, which is conducive to finding the global optimal solution. The absolute value of the slope is large in the later stages of iteration, which improves the speed and capability of attractiveness. As a result, the improved FA has greater brightness and attractiveness.

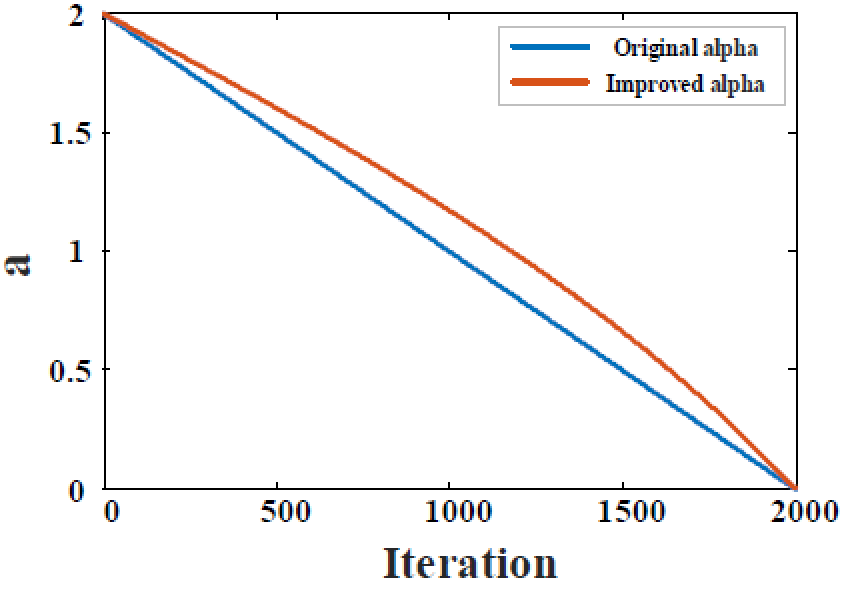


Figure 2. The linear and nonlinear convergence (Source: Guo et al., 2020)

3.3 An Improved Firefly Algorithm for Credit Card Fraud Detection

The pseudo-code of an improved FA can be summarized in Algorithm 1 of Figure 3 using the above idealization rules and nonlinear convergence factors, while Figure 4 shows the flowchart of procedure to implement the proposed algorithm.

```
Algorithm 1: An Improved Firefly Algorithm for Credit Card Fraud Detection.
Input: classical FA and nonlinear convergence factor based on tangent function.
Output: Fast convergence FA
Objective function $f(x)$, $x = (x_1, \ldots, x_d)^T$
Generate initial population of fireflies $x_i$ ($i$=1, 2, …, $n$)
Calculate the light intensity $I_i$ at $x_i$ by $f(x_i)$
Initialize the iteration number $l_i$ ($i$=1, 2, …, $n$), maximum iteration number, $l_{max} = 100$
Define light absorption coefficient $\gamma$
Update light absorption coefficient $\gamma$ using convergence factor of equation (9)
While ($t < MaxGeneration$)
    for $i$ = 1: $n$ all $n$ fireflies
        for $j$ = 1: $i$ all $n$ fireflies
            Calculate the distance $r$ between $x_i$ and $x_j$ using Cartesian distance of equation (7)
            if ($I_j > I_i$),
                Attractiveness varies with distance $r$ via $\beta_0$*exp[-$\gamma r^2$]
                Move firefly $i$ towards $j$ in all $d$-dimensions
            end if
                Evaluate new solutions and update light intensity
        end for $j$
    end for $i$
    Rank the fireflies and find the current best solution
end while
Postprocess results and visualization
```

Figure 3. An improved firefly algorithm for credit card fraud detection.

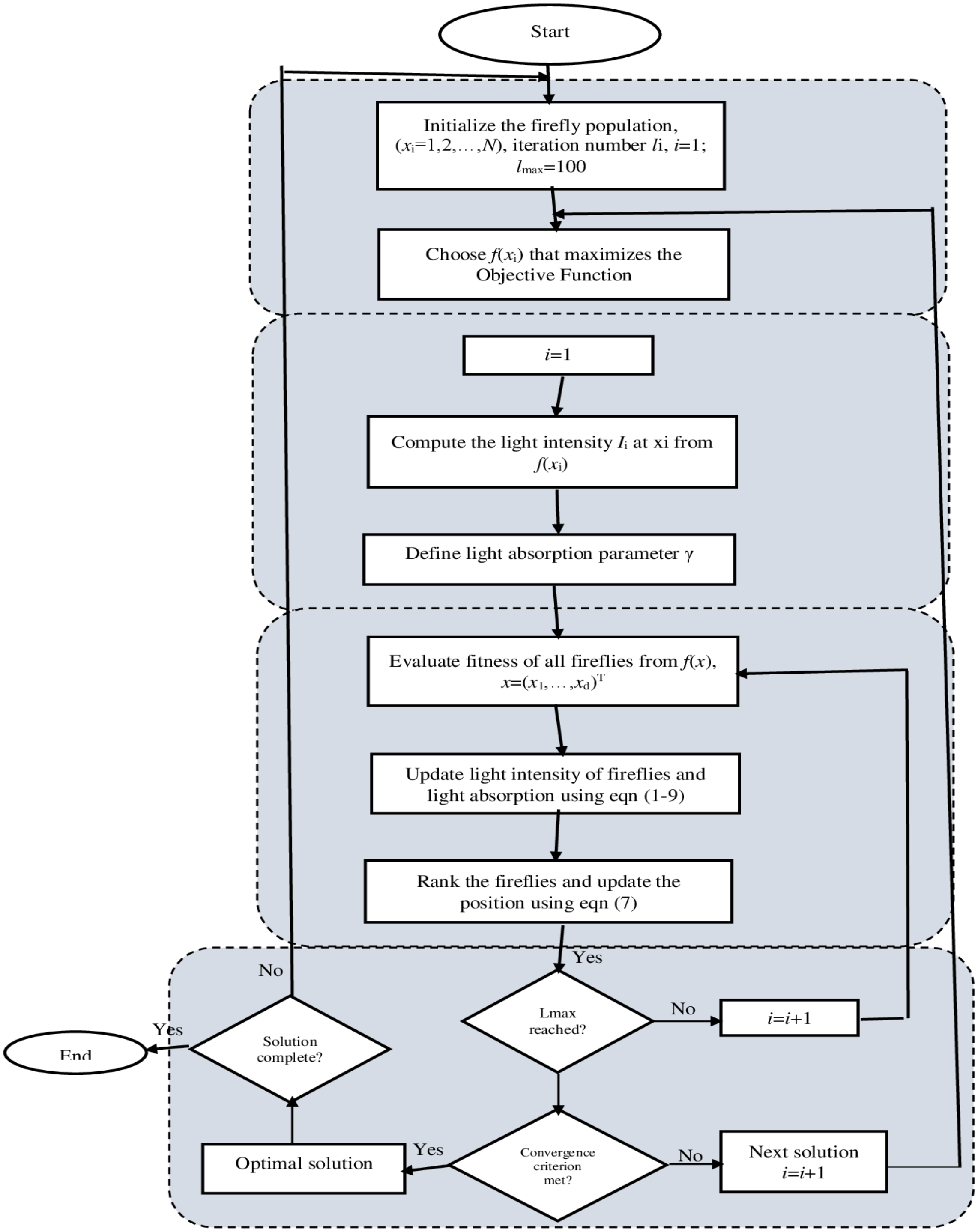

Start
Initialize the firefly population, (x_i=1,2,…,N), iteration number li, i=1; l_{max}=100
Choose $f(x_i)$ that maximizes the Objective Function
i=1
Compute the light intensity I_i at xi from $f(x_i)$
Define light absorption parameter γ
Evaluate fitness of all fireflies from $f(x)$, $x=(x_1,\ldots,x_d)^T$
Update light intensity of fireflies and light absorption using eqn (1-9)
Rank the fireflies and update the position using eqn (7)
Yes
Lmax reached?
No
i=i+1
Convergence criterion met?
No
Next solution i=i+1
Yes
Optimal solution
Solution complete?
No
Yes
End

Figure 4. Flowchart of procedure to implement Algorithm 1

3.4 Source of Experimental Dataset

We obtained approximately 2,600 e-payment transaction datasets from Nigeria Inter-Bank Settlement System (NIBBS) Plc (https://nibbs-plc.com.ng) for this study. The datasets include both fraudulent and legitimate credit card, check, internet banking, mobile, and POS transactions made in 2017. Since the focus of the study is on credit card fraud, data related to credit card transactions (both legitimate and fraudulent) were segregated from the entire data volume collected and used for the simulation of the proposed improved FA. The entire credit card transaction dataset was divided into two parts: training 75% and testing/validation 25%. The training set was presented to the proposed improved FA in order to approximate some global convergence, whereas the testing/validation set was later used to evaluate the convergence speed of eight different randomization convergence times defined as (α1-α8).

3.5 Implementation Setup

The proposed improved Firefly Algorithm (FA) was simulated using MATLAB 7.10.0 (R2017b) software installed on Graphics Processing Unit based processor with a speed of 2.70 GHz and 8.00 GB of RAM. Table 1 shows the summary of FA parameters used for the proposed simulations at dimensions 2 and 5 respectively.

Table 1. Firefly Algorithm Parameters

Parameter	Value
No. of fireflies	25
No. of iterations	100
Randomization parameter (α)	0.5
Attractiveness (β)	0.2
Light absorption coefficient (γ)	1

4. Experimental Results and Discussion

During the simulation, 25 fireflies were used in each iteration, and they all searched in a random feature space for an optimal solution for the maximum number of iterations, which was set to 100. The firefly's light intensity is proportional to the objective function that yields classifier accuracy. The optimal feature subset is the subset of features that maximizes the classification accuracy of improved FA until the termination condition (i.e. the maximum number of iterations) is reached. Because the algorithm was coded and implemented in MATLAB, it was run for 100 iterations without the threshold stopping condition. Table 2 displays the convergence speed results for eight different randomization values obtained from the proposed algorithm's implementation. Convergence speed increases significantly with increasing number of iterations as the algorithm quickly converges to global optima with improved FA. The fireflies converged to optimal solutions after 100 iterations by automatically subdividing their population into four subgroups, as shown in Figure 5. Since the FA is stochastic in nature, having randomness involved, the results were computed as the average of 100 runs, to provide statistically valid data. The proposed improved FA's success rate is 3724573 (100%) implying that the average of function evaluation is 3724 with a standard deviation of 573. As a result, the proposed algorithm has an excellent success rate for finding global optima.

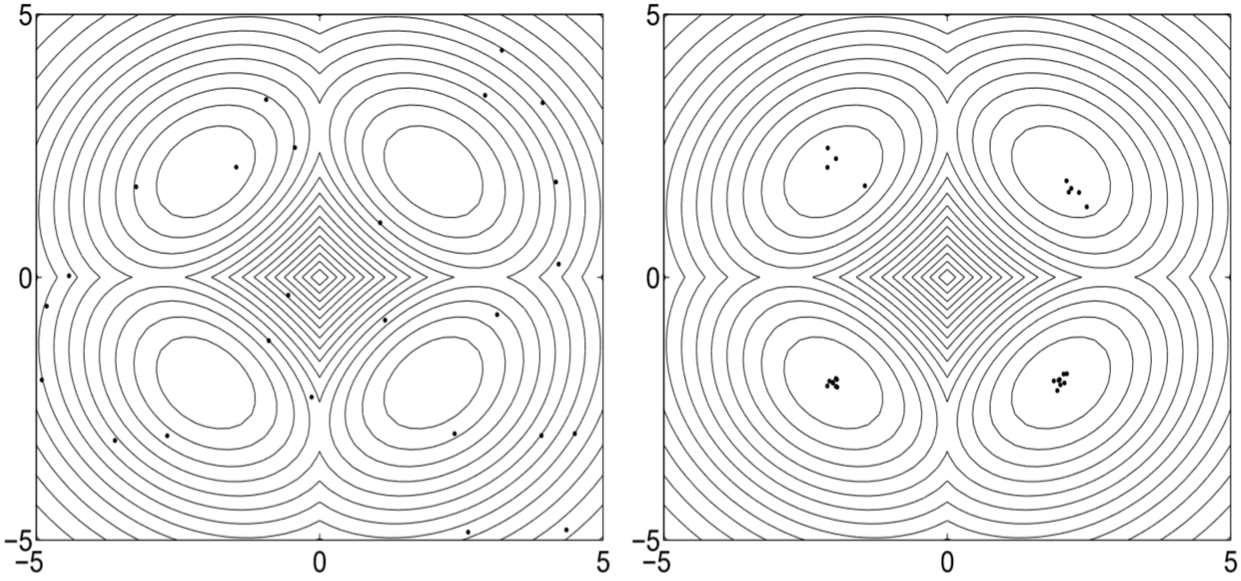
At 0 iteration, Figure 5(a) indicates that all the 25 fireflies were randomly displaced all over the search space with dim illuminations. This indicates their initial location (position) prior to the beginning of the search. The distance between adjacent fireflies is very wide with no attractiveness and little brightness. The total average distance between all the 25 fireflies modelled during the simulation experiment was found to be very high with individual firefly searching for a fraudulent transaction in the credit card dataset search space used. Immediately some fraudulent transactions were detected in the search space, other fireflies moved in the directions of those fireflies having greater brightness and converge to global optima. This is illustrated in Figure 5(b) with four different fireflies' subgroups. This procedure was repeated for 10 different initial iteration number (l_i=10, 20, …, 100) while varying absorption coefficient (γ) between [0.4-2.1] as shown in Table 2. The best randomization convergence values (α) were achieved at constant β=0.2 and γ=1. The decreasing randomization convergence times as the number of iterations increases until 100 iterations indicate an improved convergence speed, thus attesting to the efficiency of the proposed algorithm. Figure 6 further shows the curves of eight randomization convergence parameters obtained during the proposed experiment. From the figure, it can be deduced that the best solutions (fraud detections) was found at 23 iterations for α_1, between 24-26 iterations for α_2, at 27 iterations for α_3, 28 iterations for α_4, 41 iterations for α_5 and 48 iterations α_7 respectively. These were obtained at light absorption coefficient γ=0.4. Three different best solutions were found for α_6 as the value of γ increases from 0.4 to 2.1. These best solutions for this randomization parameter was obtained at 45 iterations and light absorption coefficient, γ=0.9, 46 iterations at γ=1.8 and 50 iterations at γ=2.1 respectively. For randomization parameter α_7 and α_8, the best solution for credit card fraud detection was found at 48 iterations in both cases.

After running and analyzing the written MATLAB program codes for the proposed improved FA, a few possible program enhancement problems arose. First, the distance between fireflies was calculated between every possible pair of fireflies, which has the greatest effect on randomization convergence speed. This is not required; the distance must only be calculated when the firefly intends to move towards another. This reduces the number of distances calculated per iteration and the time required for convergence, thus improving the speed of the proposed algorithm. The implication of the above development is that after randomly displacing fireflies at different light absorption coefficient parameters, they flashed and were attracted to one another. As a result, the proposed algorithm is capable of matching fraudulent transactions (x_i) with equivalent transactions that have already been registered as fraudulent (x_j) and detecting them accordingly.

Table 2. Results for best randomization convergence solutions for improve FA after 100 iterations

Iteration (l_i)	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8
0	1.300	2.500	0.300	2.300	2.500	2.500	2.500	2.500
10	0.400	1.500	0.300	0.900	2.300	2.300	2.290	2.500
20	0.400	0.900	0.300	0.380	2.100	2.100	1.410	2.420
30	0.390	0.550	0.300	0.260	1.850	1.850	1.300	2.330
40	0.385	0.380	0.300	0.100	1.780	1.780	1.100	2.285
50	0.380	0.300	0.300	0.020	1.490	1.490	0.860	1.980
60	0.380	0.200	0.290	0.000	1.300	1.300	0.800	1.810
70	0.380	0.150	0.280	0.000	1.000	1.000	0.650	1.400
80	0.380	0.100	0.250	0.000	0.800	0.800	0.600	1.100
90	0.370	0.050	0.230	0.000	0.700	0.700	0.480	0.700
100	0.370	0.000	0.200	0.000	0.400	0.400	0.400	1.300

With β= 0.2; γ = 1 (constant); α- randomization convergence parameter



(a) (b)

Figure 5. Search Space showing the randomized convergence of 25 fireflies after 100 iterations. (a) indicates the initial location of the 25 fireflies; (b) indicates their final locations (4 subgroups)

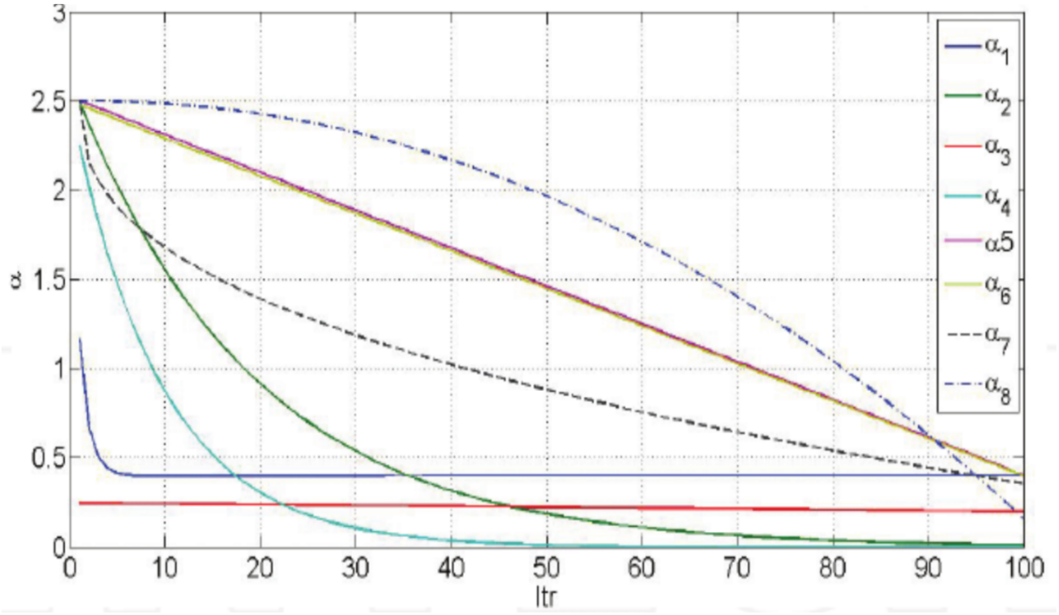


Figure 6. Graphical illustration of randomized convergence of 25 fireflies after 100 iterations.

To evaluate the performance of proposed improve FA, we compared it against three state-of-the-art meta-heuristic optimization algorithms for credit cards fraud detection. These algorithms include ordinary FA, Particle Swarm Optimization (PSO) and Genetic Algorithms (GA). The same population size of n=25 was maintained during the experiments. The PSO used is the standard version with no inertia function, and the implemented genetic algorithm has a mutation probability of 0.05 and a crossover probability of 0.95 without superiority. We ran extensive simulations after implementing these algorithms in MATLAB, and each algorithm was run at least 100 times to perform meaningful statistical analysis. When the variations in function values are less than a given tolerance of $\lambda \leq 10^{-5}$, the algorithms stop. The results are summarized in Table 3. It can be deduced that improved FA outperformed the three meta-heuristic algorithms that were compared with it at detecting credit card frauds.

Table 3. Performance comparison of meta-heuristic algorithms for credit cards fraud detection

Algorithms	Average Function Evaluation	Standard Deviation	Success Rate (%)
Ordinary FA	7925	1609	98
GA	24701	3523	97
PSO	17522	7527	98
Proposed improved FA	3724	573	100

5. Conclusion

FA is one of the most recent meta-heuristic stochastic optimization algorithms that has been developed. The algorithm, which was inspired by the natural flashing behaviour of fireflies, has found widespread application in a variety of fields, including image processing, engineering, scheduling pattern, load dispatch, TSP, and credit card fraud detection system. Others in its class include GA, PSO, ACO, CS, hunting search (HuS), grey wolf optimization (GWO), and whale optimization algorithm (WOA), to name a few. Some of these have also been used for credit card fraud detection, albeit with varying success rates and randomization convergence.

Most existing optimization algorithms for detecting credit card fraud have a few key parameters that direct them toward the best global solution. These parameters must be reasonably adjusted to avoid divergence. The convergence of an algorithm is one of its most important characteristics. It is possible to analyze and prove whether the algorithm converges using mathematical theoretical knowledge and enhancing the existing optimization algorithms. The convergence speed of classical FA was improved in this study by using a tangent trigonometric function-based nonlinear convergence factor. The newly proposed improved FA was simulated using MATLAB and then used to categorize credit card transaction records as fraudulent or legitimate. We were able to demonstrate that by incorporating a nonlinear convergence factor into the FA, the randomization convergence speed improves significantly high towards global optima, as evidenced by the interpreted simulation results presented in eight different simulations shown in Section 4. When compared to its equivalent state-of-the-art meta-heuristic optimization algorithms for credit card fraud detection, the proposed algorithm outperforms them by generating an average evaluation function of 3724±573 with a success rate of 100%. The graphical representation in Figure 6 confirmed that the fireflies use a maximum of 100 iterations to achieve high randomized convergence speed.

The social nature of fireflies provides an efficient method for traversing a search space in an optimization problem and avoiding local minima. The medium of search, the amount of attraction between fireflies, and the amount of randomness all play important roles in FA modelling. As a result, they must be properly adapted to the problem at hand. With the addition of randomness reduction and distance scaling, the proposed improved FA can be modified even further to improve performance. The results of this study indicate that the proposed algorithm is a very powerful algorithm for detecting credit card fraud. In the simulation experiment, it was discovered that the proposed improved FA achieved better randomization convergence in a fraction of the time. When it comes to problems like detecting credit card payment fraud, it appears that the FA is a powerful algorithm. When convergence speed is critical, the proposed algorithm is extremely efficient.

Reference

Alhazmi, A. H., & Aljehane, N. (2020). A Survey of Credit Card Fraud Detection Use Machine Learning. 2020 International Conference on Computing and Information Technology, ICCIT 2020, 137–142. https://doi.org/10.1109/ICCIT-144147971.2020.9213809

Amanze, B. C., & Onukwugha, C. G. (2018). Credit card fraud detection system in nigeria banks using adaptive data mining and intelligent agents: A review. *International Journal of Scientific and Technology Research, 7*(7), 175–184.

Anderson, R. (2007). The Credit Scoring Toolkit - Theory and Practice for Retail Credit Risk Management and Decision Automation. Oxford University Press.

Apostolopoulos, T., & Vlachos, A. (2011). Application of the Firefly Algorithm for Solving the Economic Emissions Load Dispatch Problem. *International Journal of Combinatorics, 2011*, 1–23. https://doi.org/10.1155/2011/523806

Association for Payment Clearing Services. (2020). The Handbook of International Financial Terms. Oxford Reference. https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095429996

Azhan, M., & Meraj, S. (2020). Credit card fraud detection using machine learning and deep learning techniques. Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020, Nov 2018, 514–518. https://doi.org/10.1109/ICISS49785.2020.9316002

Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2013). Cost sensitive credit card fraud detection using bayes minimum risk. Proceedings - 2013 12th International Conference on Machine Learning and Applications, ICMLA 2013, 1(December), 333–338. https://doi.org/10.1109/ICMLA.2013.68

Bentley, P. J., Kim, J., Jung, G., & Choi, J. (2000). Fuzzy Darwinian Detection of Credit Card Fraud. 14th Annual Fall Symposium of the Korean Information Processing, 14(January 2000), 1–4. http://faculty.ksu.edu.sa/ALFURAIH/Credit Card Fraud/Fuzzy_ Darwinian_ Detection_ of_ Credit_ Card _Fraud.PDF

Bidar, M., Sadaoui, S., Mouhoub, M., & Bidar, M. (2018). Enhanced Firefly Algorithm Using Fuzzy Parameter Tuner. Computer and Information Science, 11(1), 26–51. https://doi.org/10.5539/cis.v11n1p26

Chatterjee, A., Mahanti, G. K., & Chatterjee, A. (2012). Design of a fully digital controlled reconfigurable switched beam concentric ring array antenna using firefly and particle swarm optimization algorithm. Progress In *Electromagnetics Research B, 36*, 113–131. https://doi.org/10.2528/PIERB11083005

Darwish, S. M. (2020). A bio - inspired credit card fraud detection model based on user behavior analysis suitable for business management in electronic banking. *Journal of Ambient Intelligence and Humanized Computing, 11*, 4873–4887. https://doi.org/https://doi.org/10.1007/s12652-020-01759-9

Dornadula, V. N., & Greetha, S. (2019). Credit Card Fraud Detection Using Machine Learning Algorithms. Proceedings of the International Conference on Recent Trends in Advanced Computing (ICRTAC 2019), 631–641. https://doi.org/10.1109/ICICCS48265.2020.9121114

Duman, E., Buyukkaya, A., & Elikucuk, I. (2013). A Novel and Successful Credit Card Fraud Detection System Implemented in a Turkish Bank. 2013 IEEE 13th International Conference on Data Mining Workshops, 162–171. https://doi.org/10.1109/ICDMW.2013.168

Duman, E., & Ozcelik, M. H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications, 38*(10), 13057–13063. https://doi.org/10.1016/j.eswa.2011.04.110

Farahani, S. M., Nasiri, B., & Meybodi, M. R. (2011). A multiswarm based firefly algorithm in dynamic environments. Third Int. Conf. on Signal Processing Systems (ICSPS2011), 3(January 2011), 68–72.

Folorunso, O. (2015). Credit Card Fraud Detection using Firefly Algorithm. *International Journal of the Nigeria Association of Mathematical Physics, 31*, 101–106. http://e.nampjournals.org/product-info.php?pid2255.html

Guo, K., Mao, M., Zhou, L., & Zhang, Q. (2020). An Improved Gray Wolf Optimizer MPPT Algorithm for PV System With BFBIC Converter Under Partial Shading. *IEEE Access, 8*, 103476–103490. https://doi.org/10.1109/ACCESS.2020.2999311

Halvaiee, N. S., & Akbari, M. K. (2014). A novel model for credit card fraud detection using Artificial Immune Systems. *Applied Soft Computing Journal, 24*, 40–49. https://doi.org/10.1016/j.asoc.2014.06.042

Jain, R., Gour, B., & Dubey, S. (2016). A Hybrid Approach for Credit Card Fraud Detection using Rough Set and Decision Tree Technique. *International Journal of Computer Applications, 139*(10).

Juniper Research. (2020). Online Payment Fraud Losses to Exceed $200 Billion Over Next 5 Years. Business Wire. https://www.businesswire.com/news/home/20200224005675/en/Juniper-Research-Online-Payment-Fraud-Losses-Exceed

Kakandikar, G. M., & Kulkarni, O. (2020). Optimising fracture in automotive tail cap by firefly algorithm Sujata Patekar Trupti Bhoskar. *International Journal of Swarm Intelligence, 5*(1), 136–150.

Khan, A. U. S., Akhtar, N., & Qureshi, M. N. (2014). Real-Time Credit-Card Fraud Detection using Artificial Neural Network Tuned by Simulated Annealing Algorithm. Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing, ITC (ACEEE), 113–121. https://doi.org/02.ITC.2014.5.65

Krivko, M. (2010). A hybrid model for plastic card fraud detection systems. *Expert Systems with Applications, 37*(8), 6070–6076. https://doi.org/10.1016/j.eswa.2010.02.119

Langari, R. K., Sardar, S., Mousavi, S. A. A., & Radfar, R. (2020). Combined fuzzy clustering and firefly algorithm for privacy preserving in social networks. *Expert Systems with Applications, 141*, 1–15.

Lei, J. Z., & Ghorbani, A. A. (2012). Improved competitive learning neural networks for network intrusion and fraud detection. *Neurocomputing, 75*(1), 135–145. https://doi.org/10.1016/j.neucom.2011.02.021

Li, H., & Wong, M. L. (2015). Financial Fraud Detection by using Grammar-based Multi-objective Genetic Programming with ensemble learning. 2015 IEEE Congress on Evolutionary Computation, CEC 2015 - Proceedings, 1113–1120. https://doi.org/10.1109/CEC.2015.7257014

Lucas, Y., Portier, P. E., Laporte, L., He-Guelton, L., Caelen, O., Granitzer, M., & Calabretto, S. (2020). Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *Future Generation Computer Systems, 102*(September), 393–402. https://doi.org/10.1016/j.future.2019.08.029

Mahmoudi, N., & Duman, E. (2015). Detecting credit card fraud by Modified Fisher Discriminant Analysis. *Expert Systems with Applications, 42*(5), 2510–2516. https://doi.org/10.1016/j.eswa.2014.10.037

Maniraj, S. P., Saini, A., Sarkar, S. D., & Ahmed, S. (2019). Credit card fraud detection using machine learning and data science. *International Journal of Engineering Research and Technology, 8*(09), 110–115. https://doi.org/10.1109/ICISS49785.2020.9316002

More, R. S., Awati, C. J., Shirgave, S. K., Deshmukh, R. J., & Patil, S. S. (2020). Credit Card Fraud Detection Using. *International Journal of Scientific and Technology Research, 9*(10), 149–153.

Najadat, H., Altiti, O., Aqouleh, A. A., & Younes, M. (2020). Credit Card Fraud Detection Based on Machine and Deep Learning. 2020 11th International Conference on Information and Communication Systems, ICICS 2020, Section IX, 204–208. https://doi.org/10.1109/ICICS49469.2020.239524

Olszewski, D. (2014). Fraud detection using self-organizing map visualizing the user profiles. *Knowledge-Based Systems, 70*, 324–334. https://doi.org/10.1016/j.knosys.2014.07.008

Poongodi, K., & Kumar, D. (2021). Support vector machine with information gain-based classification for credit card fraud detection system. *International Arab Journal of Information Technology, 18*(2), 199–207. https://doi.org/10.34028/IAJIT/18/2/8

Prakash, A., & Chandrasekar, C. (2015). An optimized multiple semi-hidden Markov model for credit card fraud detection. *Indian Journal of Science and Technology, 8*(2), 176–182.

Raja, N. S. M., Manic, K. S., & Rajinikanth, V. (2013). Firefly algorithm with various randomization parameters: An analysis. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8297 LNCS (PART 1), 110–121. https://doi.org/10.1007/978-3-319-03753-0_11

Ravisankar, P., Ravi, V., Raghava Rao, G., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems, 50*(2), 491–500. https://doi.org/10.1016/j.dss.2010.11.006

Sayadi, M. K., Ramezanian, R., & Ghaffari-Nasab, N. (2010). A discrete firefly meta-heuristic with local search for make span minimization in permutation flow shop scheduling problems. *International Journal of Industrial Engineering Computations, 1*(1), 1–10. https://doi.org/10.5267/j.ijiec.2010.01.001

Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. K. (2008). Credit card fraud detection using Hidden Markov Model. *IEEE Transactions on Dependable and Secure Computing, 5*(1), 37–48. https://doi.org/10.1109/TDSC.2007.70228

Tarjo, & Herawati, N. (2015). Application of Beneish M-Score Models and Data Mining to Detect Financial Fraud. *Procedia-Social and Behavioral Sciences, 211(September)*, 924–930. https://doi.org/10.1016/j.sbspro.2015.11.122

Usman, O. L., Muniyandi, R. C., Omar, K., & Mohamad, M. (2021). Advance Machine Learning Methods for Dyslexia Biomarker Detection: A Review of Implementation Details and Challenges. *IEEE Access, 9*, 36879–36897. https://doi.org/10.1109/ACCESS.2021.3062709

Vadoodparast, M., Hamdan, A. R., & Hafiz. (2015). Fraudulent Electronic transaction detection using KDA Model. *International Journal of Computer Science and Information Security (IJCSIS), 13*(3), 90–99. http://arxiv.org/abs/1503.03208

Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A Novel Approach for Automated Credit Card Transaction Fraud Detection using Network-Based Extensions. *Decision Support Systems, 75*(20), 38–48. https://doi.org/10.1016/j.dss.2015.04.013

Wu, J., Wang, Y., Burrage, K., Tian, Y., Lawson, B., & Ding, Z. (2020). An improved firefly algorithm for global continuous optimization problems. *Expert Systems with Applications, 149*, 1–12.

Yang, X.-S. (2010). Firefly Algorithm, Lévy Flights and Global Optimization. In Springer. https://link.springer.com/chapter/10.1007/978-1-84882-983-1_15

Yang, X.-S. (2013a). Multiobjective firefly algorithm for continuous optimization. *Engineering with Computers, 29*(2), 175–184. https://doi.org/10.1007/s00366-012-0254-1

Yang, X.-S. (2013b). Multiobjective Firefly Algorithm for Continuous Optimization. In Engineering with Computers (Vol. 29). https://link.springer.com/article/10.1007/s00366-012-0254-1

Yang, X.-S., & He, X. (2013). Firefly algorithm: recent advances and applications. *International Journal of Swarm Intelligence, 1*(1), 36. https://doi.org/10.1504/ijsi.2013.055801

Yang, X.-S., & Karamanoglu, M. (2020). Nature-inspired computation and swarm intelligence: a state-of-the-art overview. In X.-S. Yang (Ed.), Nature-Inspired Computation and Swarm Intelligence: Algorithms, Theory and Applications (pp. 3–18). Elsevier Ltd. https://doi.org/https://doi.org/10.1016/C2019-0-00628-0

Yousif, A., Abdullah, A. H., Nor, S. M., & Abdelaziz, A. A. (2011). Scheduling jobs on grid computing using firefly algorithm. *Journal of Theoretical and Applied Information Technology, 33*(2), 155–164.