Optimal Single-Valued Neutrosophic Sine Trigonometric Aggregation Operators for Accurate Financial Fraud Detection Model

Fadoua Kouki[1,*]

[1] Department of Financial and Banking Sciences, Applied College at Muhail Aseer, King Khalid University, Saudi Arabia.
Emails: falkoki@kku.edu.sa

Abstract

Financial fraud may be regarded as any fraud targeting financial organisations including crypto exchanges, banks, fintech, and lending organizations, or any criminal activity associated with the payment process. Financial fraud detection cites protocol set prepared to circumvent the destruction produced by fraudulent activities happening in financial service suppliers. Ecological financial fraud detection (FD) includes the usage of ethical and sustainable performs within fraud actions recognition from the financial area. In recent times, DL and ML techniques have been used in CCF recognition owing to their ability to construct a robust mechanism to discover fraud businesses. Therefore, this study develops an Optimal Single Valued Neutrosophic Sine Trigonometric Aggregation Operator (O-SVNSTAO) for Accurate Financial Fraud Detection Model. The genetic-inspired particle swarm optimization (GIPSO) feature selection model efficiently discerns the relevant attribute from sophisticated financial databases, improving the model's discriminative power while alleviating dimensionality problems. Consequently, the SVNSTAO classifier leverages the features selected to discern complicated features inherent in fraudulent actions, which facilitates accurate diagnosis. Moreover, the COA parameter tuning mechanism enhances the SVNSTAO model's parameter, which ensures adaptability and optimum performance to varied fraud settings. Empirical analysis of real-time financial datasets demonstrates the superiority of O-SVNSTAO technique over classical methods, underlining its effectiveness in discovering financial fraud with exceptional efficiency and reliability

Keywords: Fraud Detection; Credit Card Fraud; Chimp Optimization Algorithm; Feature Selection; Sine Trigonometric Aggregation Operators

1. Introduction

Digital expenses of numerous methods are speedily increasing all over the world. Payments corporations are undergoing fast development in their transaction size [1]. Beside this renovation, there is also a fast upsurge in economic fraud that occurs in these payment methods. Averting online economic fraud is a crucial fragment of the work completed by cybercrime and cybersecurity groups. Numerous economic institutions and banks have given teams of dozens of experts constructing automatic methods to analyse dealings that take place over their products and flag eventually fake ones [2]. So, it is vital to discover the tactic to resolve the issue of identifying fake transactions/ entries in huge extents of data to be well organized to resolve cases of cybercrime [3]. However, traditional fraud recognition model counts on rule-based methods that have few limits and can't well recognize classy fraud threats. That is why financial fraud recognition utilizing machine learning (ML) comes into play [4].

Tradition models of perceiving fraudulent actions utilizing rule-based methods have become expired in present technology-driven period [5]. Since these methods function on pre-defined instructions, they can efficiently recognise transaction patterns, but their skills are restricted when it comes to recognizing novel and developing ones. Likewise, they repeatedly make false positives, weakening legitimate transactions as fake activity [6]. The main advantage of utilizing ML for fraud recognition is its capability to adjust a novel fraud pattern and decrease false positives. ML techniques will be obtained from past fraud cases and adjusted to novel patterns, making them highly effective in recognizing and averting fraud. ML is a branch of AI that delivers methods with the capability

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

to automatically acquire and enhance knowledge [7]. The learning procedure begins with data or observations, like instruction or direct experience, to observe for forms in data and generate superior choices in the prospect dependent upon the models that we deliver [8]. The major objective is to absorb mechanically without human involvement or help and modify actions accordingly [9]. DL is a subsection of ML in AI which has capable of learning unsupervised from data that is unlabelled or unstructured. DL is a method utilized in order to make face recognition, identify it as fake or real by utilizing profile imageries, and define the dissimilarities among them [10].

This study develops an Optimal Single Valued Neutrosophic Sine Trigonometric Aggregation Operator (O-SVNSTAO) for Accurate Financial Fraud Detection Model. The genetic-inspired particle swarm optimization (GIPSO) feature selection model efficiently discerns the relevant attribute from sophisticated financial databases, improving the model's discriminative power while alleviating dimensionality problems. Consequently, the SVNSTAO classifier leverages the features selected to discern complicated features inherent in fraudulent actions, which facilitates accurate diagnosis. Moreover, the COA parameter tuning mechanism enhances the SVNSTAO model's parameter, which ensures adaptability and optimum performance to varied fraud settings. Empirical analysis of real-time financial datasets demonstrates the superiority of O-SVNSTAO technique over classical methods, underlining its effectiveness in discovering financial fraud with exceptional efficiency and reliability.

2. Literature Works

Zioviris et al. [11] projected a hybrid method that is a consecutive system for relating dual DL methods and well identifying potential economic frauds. The method enlarges on the mixture of an autoencoder (AE), Recurrent Neural Networks (RNN) and LSTM trained upon databases that are handled over the usage of an oversampling model. The authors [12] concentrated on inventing a smart credit card FD and classification model employing the Garra Rufa Fish optimizer process with the ensemble-learning (CCFDC-GRFOEL) technique. This technique creates a novel GRFO-FSS model to pick a group of features. An EL method, containing an ELM, BiLSTM, and AE was employed for the recognition of fraudulent transaction. At last, the POA has been employed for the hyperparameter fine-tuning of 3 classifier models. In [13], a new credit card fraud recognition method is presented utilizing sequence labelling dependent upon both DNN and probabilistic graphical methods (PGM). Furthermore, the projected model presented a new undersampling system, which aids in upholding the consecutive patterns of data throughout the random undersampling procedure.

Chaudhry et al. [14] summarise a complete strategy to increase economic safety through the use of advanced AI models. The recommended structure contains 3 foremost parts namely a K-Means clustering for preparation of dataset, an extended deep Q network (EDQN) for prediction and analysis, and a principal component analysis (PCA) for FS. An improved K-Means clustering model can manage difficult and larger-scale economic data is the main contribution. In [15], a BN Based Autoencoder GRU (BN-AGRU) technique is projected for economic fraud recognition that utilises an AE to capture local patterns. We combined BN into the AE-GRU approach employing a pretrained real-time vector in order to yield an exclusive structure for economic fraud recognition. The procedure of choosing feature is controlled using the Seahorse Optimizer (SHO). The Chaotic SHO (CSHO) was presented as a hybrid technique which attacks a novel balance among abuse phases and exploration. The method also used prolonged short-term memory as alternative.

Tang and Liu [16] recommend a dispersed knowledge distillation structure dependent upon Transformer. At first, the multi-attention mechanism is utilized to provide weight to the feature, tracked by feed-forward neural network to remove higher-level features that contain relevant data, and lastly, neural networks are utilized to classify economic fraud. Next, for the issue of inconsistent economic data indicators and uneven data distribution concentrated on dissimilar trades, a dispersed knowledge distillation technique is projected. The authors [17] proposed a two-phase structure to recognize fake transactions which includes a DAE as a depiction learning method, and supervised-DL methodologies. Precisely, the utilized DL classifiers proficient on the altered data gained by the DAE considerably beat their standard classifiers proficient on the unique data under every measure. Also, methods generated utilizing deep AE exceed those generated utilizing the PCA-attained database and the existing methods.

3. The Proposed Model

In this work, we have established an O-SVNSTAO method for accurate financial fraud detection model. The main purpose of the O-SVNSTAO methodology is to have different kinds of processes involved as GIPSO-based FS, SVNSTAO classifier, and COA-based parameter tuning. Fig. 1 represents the working process of O-SVNSTAO methodology.

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

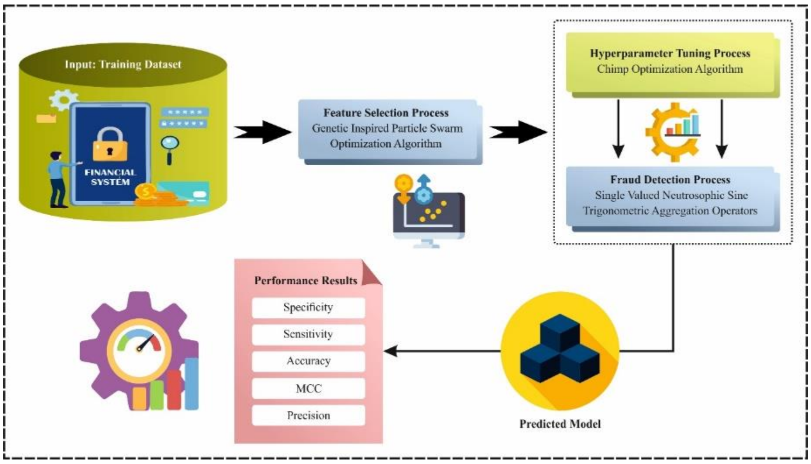

Figure 1: Working procedure of O-SVNSTAO method

A. Feature Selection using GIPSO

Primarily, the GIPSO-based FS model efficiently discerns the relevant attributes from sophisticated financial databases. In 1995, Eberhart and Kennedy developed original PSO [18]. The grouping of fish and birds was the foremost motivation for this meta-heuristic. Particles are signified as searching agents and are intended as a population fragment. Separate and nonstop issues are resolved by the PSO.

$$\begin{cases} \vec{v_i} \leftarrow \vec{v_i} + \vec{u}(0,\phi_1) \otimes (\vec{p_i} - \vec{x_i}) + \vec{u}(0,\phi_2) \otimes (\vec{p_g} - \vec{x_i}) \\ \vec{x_i} \leftarrow \vec{xi} + \vec{v_i}, \end{cases} \tag{1}$$

In Eq. (1), the range of each module from v_i is $[-V_{\max}, +V_{\max}]$. The value of p_i signifies the optimal solution for particle i. Any particle is a probable result from D dimension space and its location has been definite by Eq. (2), the optimal position attained before the upgrade has been presented in Eq. (3), and the velocities are assumed in Eq. (4):

$$X_i = (x_{i1}, x_{i2}, \dots, x_{iD}) \tag{2}$$

$$P_i = (Pi1, Pi2 \dots, p_{iD}) \tag{3}$$

$$V_i = (v_{i1}, v_{i2'} \dots, v_{iD}) \tag{4}$$

The optimal solutions in the cluster are represented as p_i and p_g, correspondingly.

This behavior can be exhibited as in Eq. (5):

$$v_{id} = W * v_{id} + c_1 * r_1 * (P_{id} - X_{id}) + c_2 * r_2 * \left(P_{gd} - X_{id}\right) \tag{5}$$

The inertia factors have been exposed in Eq. (5) as w, c_1, and c_2, applied for social and cognitive modules, correspondingly. r_1 and r_2 signifies the number of random, while the current position and particle velocity are assumed, correspondingly as v_{id} and x_{id}. p_{id} and p_{gd} are the p_i and p_g, separately.

$$w = w_{\max} - \frac{w_{\max} - w_{\min}}{T} \cdot t \tag{6}$$

While the new PSO displays good performance, it shows definite faults when estimated utilizing normal CEC estimation functions. To find out these concerns and improve the PSO, this research presents hybridized models.

Here, a new outline device has been stimulated after every iteration. It picks an arbitrary agent and integrates it with an optimal solution attained so far. Empirically the optimum value for pc is defined to be 0.1.

Every agent A holds a vector of rates that signify the genetic configuration as

$$A_i = (a_1, a_2, \dots a_D) \tag{7}$$

$$c_j = \alpha \cdot a_j + (1 - \alpha) \cdot b_j \tag{8}$$

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

where c_j represents the resultant child parameter, a_j and b_j signifies the j-th parameters of agents A and an arbitrarily designated second agent B.

$$A_{ik} = A_{ik} + md \cdot rnd \text{ or } A_{ik} = A_{ik} - md \cdot rnd \quad (9)$$

This formulation signifies the mutation of the k-th parameter, where md refers to the parameter of mutation direction, and rnd denotes the random value. Once an agent is joined and changed, the worst solution is substituted. The objective function $f(obj)$ is altered reliant on the optimizer issue being undertaken.

In GIPSO method, the objectives are united into single objective equation thus an existing weight detects all the objective importance [19]. Here, an FF fuses both objectives of FS as follows.

$$Fitness(X) = \alpha \cdot E(X) + \beta * \left(1 - \frac{|R|}{|N|}\right) \quad (10)$$

here $Fitness(X)$ is the fitness rate of X subset, $E(X)$ refers the classifier error, $|R|$ and $|N|$ are the count of attributes chosen and the quantity of new features, α and β displays the weighted of classifier error and decline ratio, $\alpha \in [0,1]$ and $\beta = (1 - \alpha)$.

B. SVNSTAO Classification

Next, the SVNSTAO classifier leverages the features selected to discern complicated features inherent in fraudulent actions, which facilitates accurate diagnosis. The sine trigonometric operational law (STOL) using single-valued neutrosophic environment (SVNN) is proposed in this section [20].

Consider $= \{ב_\partial, ד_\partial, ב_\partial\} \in SVNN(\aleph)$. Thus, STOL of SVNN ∂ is given by,

$$sin(\partial) = \left\{\left(\hbar, sin\left(\frac{\pi}{2}ב_\partial(\hbar)\right), 1 - sin\left(\frac{\pi}{2}1 - ד_\partial(h)\right) 1 - sin\left(\frac{\pi}{2}1 - ב_\partial h\right)\right) | \hbar \in \aleph\right\}$$

Note that the $sin(\partial)$ is SVNS. For any $h \in \aleph$, the truth, indeterminacy, and false membership, $ב_\partial : \aleph \to \Theta, ד_\partial : \aleph \to \Theta$ and $i_\partial : \aleph \to \Theta$, correspondingly, of h component to SVNS ∂, whereas $\Theta = [0,1]$ is the unit range. Moreover, it can be essential to provide$0 \leq ב_\partial(\hbar) + ד_\partial(h) + i_\partial(\hbar) \leq 3$, for $\hbar \in \aleph$.

Moreover, the degree of truth membership is

$sin\left(\frac{\pi}{2}ב_\partial\right) : \aleph \to \Theta$, for each $\hbar \in \aleph \to sin\left(\frac{\pi}{2}ב_\partial(h)\right) \in [0,1]$,

The degree of indeterminacy membership is

$1 - sin\left(\frac{\pi}{2}1 - ד_\partial\right) : \aleph \to \Theta$, for each $\hbar \in \aleph \to 1 - sin\left(\frac{\pi}{2}1 - ד_\partial(\hbar)\right) \in [0,1]$,

The degree of false membership is

$1 - sin\left(\frac{\pi}{2}1 - ד_\partial\right) : \aleph \to \Theta$, for each $\hbar \in \aleph \to 1 - sin\left(\frac{\pi}{2}1 - ד_\partial(\hbar)\right) \in [0,1]$.

Thus,

$$sin(\partial) = \left\{\left(\hbar, sin\left(\frac{\pi}{2}ב_\partial(\hbar)\right), 1 - sin\left(\frac{\pi}{2}1 - ד_\partial(\hbar)\right) 1 - sin\left(\frac{\pi}{2}1 - ד_\partial\hbar\right)\right) | \hbar \in \aleph\right\}$$

Consider $= \{ב_\partial, ד_\partial, j_\partial\} \in SVNN\ (\aleph)$. If

$$sin(\partial) = \left\{\left(\begin{matrix}\hbar, sin\left(\frac{\pi}{2}ב_\partial(\hbar)\right), 1 - sin\left(\frac{\pi}{2}1 - ד_\partial(\hbar)\right) \\ 1 - sin\left(\frac{\pi}{2}1 - ד_\partial(h)\right)\end{matrix}\right) | h \in \aleph\right\}$$

Next, the function $sin(\partial)$ is known as STOL and the $sin(\partial)$ value is named as STSVNN.

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

Consider $= \{\beth_{\partial}, \daleth_{\partial}, \daleth_{\partial}\} \in SVNN()$. Thus, the operator value $sin(\partial)$ is SVNN.

Consider $0 \leq \daleth_{\partial} \leq 1$ then $0 \leq \frac{\pi}{2}1 - \daleth_{\partial} \leq \frac{\pi}{2}$, which indicates $0 \leq sin\left(\frac{\pi}{2}1 - \daleth_{\partial}\right) \leq 1$. Consequently, we obtain $0 \leq 1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial}\right) \leq 1$. Thus we get $0 \leq 1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial}\right) \leq 1$.

Assume $= \{\beth_{\partial}, \daleth_{\partial}, \daleth_{\partial}\} \in SVNN(\aleph)$. Thus, the score and accuracy ∂ are represented as

1. $\overline{sc}(\partial) = \beth_{\partial} - \daleth_{\partial} - \beth_{\partial}$, and

2. $\underline{ac}(\partial) = \beth_{\partial} + \daleth_{\partial} + \beth_{\partial}$.

Consider $\partial_1 = \{\beth_{\partial_1}, \daleth_{\partial_1}, \beth_{\partial_1}\}$ and $\partial_2 = \{\beth_{\partial_2}, \daleth_{\partial_2}, \beth_{\partial_2}\} \in SVNN(\aleph)$. Thus,

1. If $\overline{sc}(\partial_1) < \overline{sc}(\partial_2)$; $\partial_1 < \partial_2$,

2. If $\overline{sc}(\partial_1) > \overline{sc}(\partial_2)$; $\partial_1 > \partial_2$,

3. If $\overline{sc}(\partial_1) = \overline{sc}(\partial_2)$;

$(a)\underline{ac}(\partial_1) < \underline{ac}(\partial_2)$; $\partial_1 < \partial_2$,

$(b)\underline{ac}(\partial_1) > \underline{ac}(\partial_2)$; $\partial_1 > \partial_2$,

$(c)\underline{ac}(\partial_1) = \underline{ac}(\partial_2)$; $\partial_1 = \partial_2$.

Assume $\partial_g = \left\{\beth_{\partial_g}, \daleth_{\partial_g}, \beth_{\partial_g}\right\} \in SVNN(\aleph)$ $(g = 1,2)$ and $\psi, \psi_1, \psi_2 > 0$. Thus, we get $sin(\partial_1) = \left\{\begin{pmatrix} sin\left(\frac{\pi}{2}\beth_{\partial_1}\right), \\ 1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial_1}\right), \\ 1 - sin\left(\frac{\pi}{2}1 - \beth_{\partial_1} - \daleth_{\partial_1}\right) \end{pmatrix}\right\}$ and $sin(\partial_2) = \left\{\begin{pmatrix} sin\left(\frac{\pi}{2}\beth_{\partial_2}\right), \\ 1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial_2}\right), \\ 1 - sin\left(\frac{\pi}{2}1 - \beth_{\partial_1} - \daleth_{\partial_2}\right) \end{pmatrix}\right\}$ as two STSVNNs. Thus, we get

$$sin(\partial_1) \boxplus sin(\partial_2) = \begin{pmatrix} 1 - \left(1 - sin\left(\frac{\pi}{2}\beth_{\partial_1}\right)\right)\left(1 - sin\left(\frac{\pi}{2}\beth_{\partial_2}\right)\right) \\ \left(1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial_1}\right)\right)\left(1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial_2}\right)\right) \\ \left(1 - sin\left(\frac{\pi}{2}1 - \beth_{\partial_1}\right)\right)\left(1 - sin\left(\frac{\pi}{2}1 - \beth_{\partial_2}\right)\right) \end{pmatrix}$$

For $\psi > 0$, we get

$$\psi(sin(\partial_1) \boxplus sin(\partial_2))$$

$$= \begin{pmatrix} 1 - \left(1 - sin\left(\frac{\pi}{2}\beth_{\partial_1}\right)\right)^{\psi}\left(1 - sin\left(\frac{\pi}{2}\beth_{\partial_2}\right)\right)^{\psi}, \\ \left(1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial_1}\right)\right)\left(1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial_2}\right)\right)^{\psi}, \\ \left(1 - sin\left(\frac{\pi}{2}1 - \beth_{\partial_1}\right)\right)^{\psi}, \left(1 - sin\left(\frac{\pi}{2}1 - \beth_{\partial_2}\right)\right)^{\psi} \end{pmatrix}^{\psi}$$

$$= \begin{pmatrix} 1 - \left(1 - sin\left(\frac{\pi}{2}\beth_{\partial_1}\right)\right)^{\psi}, \left(1 - sin\left(\frac{\pi}{2}1 - \daleth_{\partial_1}\right)\right)^{\psi}, \\ \left(1 - sin\left(\frac{\pi}{2}1 - \beth_{\partial_1}\right)\right)^{\psi} \end{pmatrix}$$

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

$$=\boxplus\begin{pmatrix}1-\left(1-sin\left(\frac{\pi}{2}ב_{\partial_2}\right)\right)^{\psi},\left(1-sin\left(\frac{\pi}{2}1-ד_{\partial_2}\right)\right)^{\psi},\\ \left(1-sin\left(\frac{\pi}{2}1-ב_{\partial_2}\right)\right)^{\psi}\end{pmatrix}$$

$= \psi\ sin(\partial_1) \boxplus \psi\ sin(\partial_2)$.

For any $\psi_1, \psi_2 > 0$, we get

$$\psi_1\ sin(\partial_1) = \begin{pmatrix}1-\left(1-sin\left(\frac{\pi}{2}ב_{\partial_1}\right)\right)^{\psi_1},\left(1-sin\left(\frac{\pi}{2}1-ד_{\partial_1}\right)\right)^{\psi_1},\\ \left(1-sin\ \left(\frac{\pi}{2}1-ב_{\partial_1}\right)\right)^{\psi_1}\end{pmatrix}$$

and

$$\psi_2\ sin(\partial_1) = \begin{pmatrix}1-\left(1-sin\left(\frac{\pi}{2}ב_{\partial_1}\right)\right)^{\psi_2},\left(1-sin\left(\frac{\pi}{2}1-ד_{\partial_1}\right)\right)^{\psi_2},\\ \left(1-sin\left(\frac{\pi}{2}1-ב_{\partial_1}\right)\right)^{\psi_2}\end{pmatrix}$$

Therefore, we get

$$\psi_1\ sin(\partial_1) \boxplus \psi_2\ sin(\partial_1)$$

$$= \begin{pmatrix}1-\left(1-sin\left(\frac{\pi}{2}ב_{\partial_1}\right)\right)^{\psi_1},\left(1-sin\left(\frac{\pi}{2}1-ד_{\partial_1}\right)\right)^{\psi_1},\\ \left(1-sin\left(\frac{\pi}{2}1-ב_{\partial_1}\right)\right)^{\psi_1}\end{pmatrix}$$

$$\boxplus\begin{pmatrix}1-\left(1-sin\left(\frac{\pi}{2}ב_{\partial_1}\right)\right)^{\psi_2},\left(1-sin\left(\frac{\pi}{2}1-ד_{\partial_1}\right)\right)^{\psi_2},\\ \left(1-sin\left(\frac{\pi}{2}1-ב_{\partial_1}\right)\right)^{\psi_2}\end{pmatrix}$$

$$= \begin{pmatrix}1-\left(1-sin\left(\frac{\pi}{2}ב_{\partial_1}\right)\right)^{\psi_1+\psi_2},\left(1-sin\left(\frac{\pi}{2}1-ד_{\partial_1}\right)\right)^{\psi_1+\psi_2},\\ \left(1-sin\left(\frac{\pi}{2}1-ב_{\partial_1}\right)\right)^{\psi_1+\psi_2}\end{pmatrix}$$

$$= (\psi_1 + \psi_2)sin(\partial_1)$$

C. COA-based Parameter Tuning

Eventually, the COA parameter tuning mechanism enhances the SVNSTAO model's parameter, which ensures adaptability and optimum performance to varied fraud settings. COA is a novel optimization algorithm stimulated by the natural behavior of chimpanzees [21]. Eqs (11) to (13) represent the critical mathematical phrases used in the CHOA model:

$$\Psi_{chimp}(z+1) = \Psi_{prey}(z) - \beta \cdot \left|\nu \cdot \Psi_{prey}(z) - \Gamma \cdot \Psi_{chimp}(z)\right| \quad (11)$$

$$\beta = 2 \cdot \xi \cdot rand_1 - \xi \quad (12)$$

$$\nu = 2 \times rand_2 \quad (13)$$

Now, number of iterations is denoted by z, and the best solution discovered is represented as tΨ_{prey}, the optimum position of the chimpanzee indicated by Ψ_{chimp}, and β, ν, and Γ are the chaotic coefficient vectors. The $rand_1$ and $rand_2$ values are chosen randomly between [0,1]. Fig. 2 depicts the steps involved in COA.

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

COA will maintain and select the top four chimpanzees according to Eqs. (14) and (15) to attain a detailed simulation of chimpanzee behaviors:

$$\Psi(z+1)=\frac{1}{4}\times(\Psi_1+\Psi_2+\Psi_3+\Psi_4) \quad (14)$$

Where

$$\Psi_1=\Psi_{Ataker}-\beta_1.|v_1\Psi_{Attacker}-\Gamma_1\Psi|$$

$$\Psi_2=\Psi_{Barrier}-\beta_2.|v_2\Psi_{Barrier}-\Gamma_2\Psi|$$

$$\Psi_3=\Psi_{Chaser}-\beta_3.|v_3\Psi_{Chaser}-\Gamma_3\Psi|$$

$$\Psi_4=\Psi_{Driver}-\beta_4.|v_4\Psi_{Driver}-\Gamma_4\Psi| \quad (15)$$

$$\Psi_{chimp}(z+1)=\begin{cases}Eq.(14) & rand_m<0.5\\ \Gamma & rand_m\geq 0.5\end{cases} \quad (16)$$

Where $rand_m$ is a probability value within [0,1].

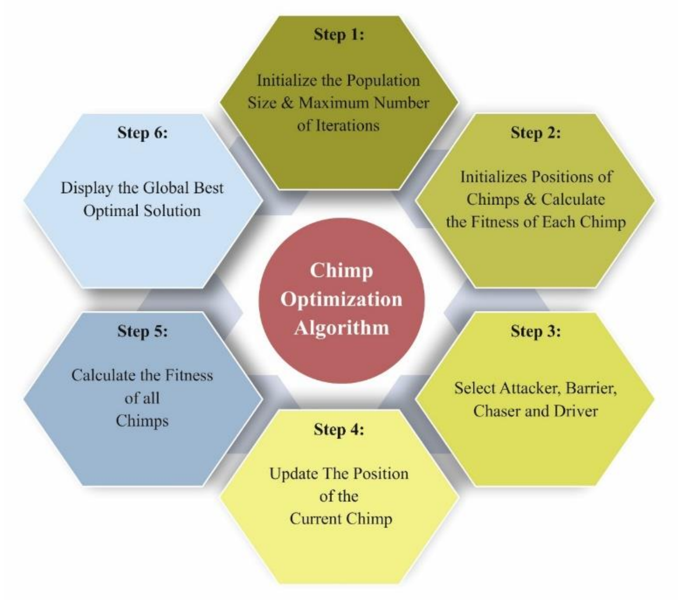

Figure 2: Steps involved in COA

The fitness selection is the key factor affecting the outcome of COA. The hyperparameter selection technique has the solution encoding method to measure the effectiveness of the solution candidate. Here, the COA assumes performance as the key condition to develop the FF.

$$Fitness\ =\ \max(P) \quad (17)$$

$$P=\frac{TP}{TP+FP} \quad (18)$$

Here TP and FP are the true positive and false positive rates.

4. Result Analysis

The performance validation outcomes of O-SVNSTAO methodology using financial dataset. The dataset comprises 900 samples with fraud and non-fraud classes as represented in Table 1.

Table 1: Details on datasets

Class	No. of instances
Non-Fraud	450

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

Fraud	450
Total instances	900

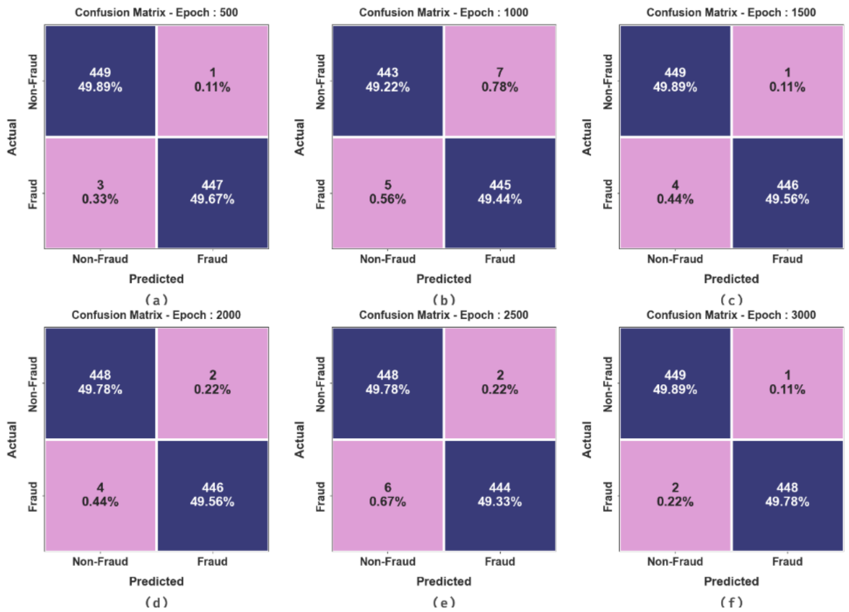

Figure 3: Confusion matrices of O-SVNSTAO method (a-f) Epochs 500-3000

Fig. 3 reports a set of confusion matrices attained by the O-SVNSTAO algorithm on various epochs. On 500 epochs, the O-SVNSTAO model has recognized 449 samples into fraud and 447 samples into non-fraud. Moreover, on 1500 epochs, the O-SVNSTAO model has detected 449 samples of fraud and 446 samples of non-fraud. As well, on 2500 epochs, the O-SVNSTAO model has detected 448 samples as fraud and 444 samples as non-fraud. Furthermore, on 3000 epochs, the O-SVNSTAO model has detected 449 samples of fraud and 448 samples of non-fraud.

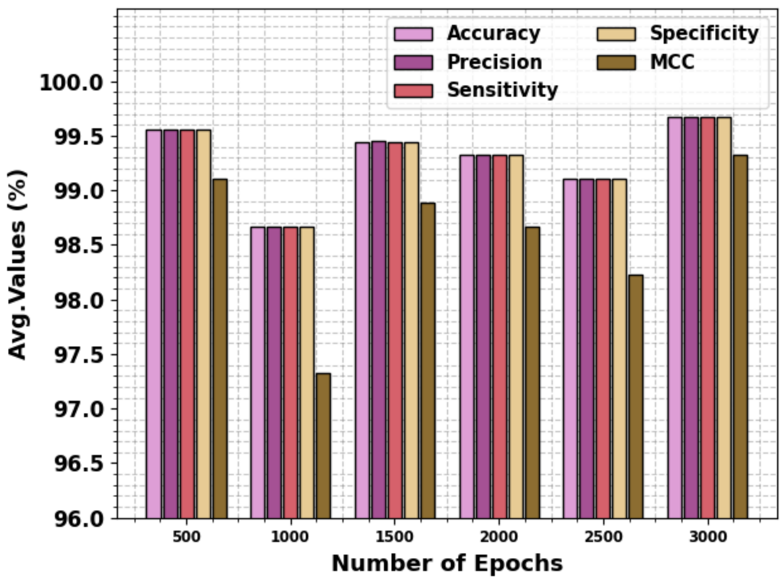

Figure 4: Average outcome of O-SVNSTAO system under various epochs

In Fig. 4, the fraud detection outcomes of O-SVNSTAO system under various epochs. The experimental values inferred that the O-SVNSTAO methodology has properly identified fraud and non-fraud samples. With 500 epochs, the O-SVNSTAO technique offers average $accu_y$ of 99.56%, $prec_n$ of 99.56%, $sens_y$ of 99.56%, $spec_y$ of 99.56%, and MCC of 99.11%. In addition, with 1000 epochs, the O-SVNSTAO method provides average $accu_y$

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

of 98.67%, $prec_n$ of 98.67%, $sens_y$ of 98.67%, $spec_y$ of 98.67%, and MCC of 97.33%. Besides, with 1500 epochs, the O-SVNSTAO model offers average $accu_y$ of 99.44%, $prec_n$ of 99.45%, $sens_y$ of 99.44%, $spec_y$ of 99.44%, and MCC of 98.89%. Followed by, with 2000 epochs, the O-SVNSTAO model provides average $accu_y$ of 99.33%, $prec_n$ of 99.33%, $sens_y$ of 99.33%, $spec_y$ of 99.33%, and MCC of 98.67%. Afterwards, with 2500 epochs, the O-SVNSTAO model provides average $accu_y$ of 99.11%, $prec_n$ of 99.11%, $sens_y$ of 99.11%, $spec_y$ of 99.11%, and MCC of 98.23%. However, with 3000 epochs, the O-SVNSTAO methodology offers average $accu_y$ of 99.67%, $prec_n$ of 99.67%, $sens_y$ of 99.67%, $spec_y$ of 99.67%, and MCC of 99.33%.

Table 2: $Accu_y$ analysis of O-SVNSTAO system with recent models

Methods	Accuracy
DSGBT Model	98.25
DTGBT Model	98.99
RFGBT Model	98.03
MLP Algorithm	98.91
Decision Tree	98.30
OCSODL-CCFD	99.23
CCFDC-GRFOEL	99.56
O-SVNSTAO	99.67

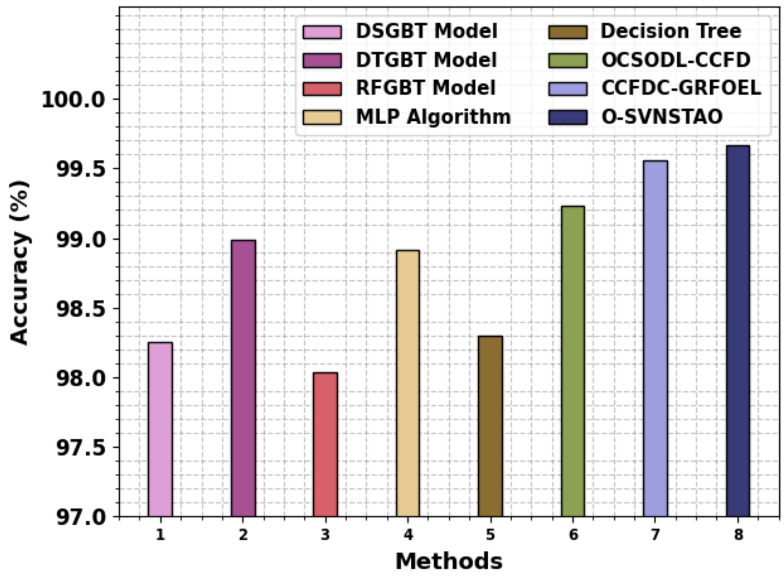

Figure 5: $Accu_y$ analysis of O-SVNSTAO system with recent models

In Table 2 and Fig. 5, a brief comparative examination of O-SVNSTAO system with other approaches [12]. The simulation outcomes implied that the O-SVNSTAO methodology has exhibited optimum performances. Based on $accu_y$, the O-SVNSTAO system has maximum $accu_y$ of 99.67% while the DSGBT, DTGBT, RFGBT, MLP, DT, OCSODL-CCFD, and CCFDC-GRFOEL approaches have lesser $accu_y$ of 98.25%, 98.99%, 98.03%, 98.91%, 98.30%, 99.23%, and 99.56%, respectively.

5. Conclusion

In this article, we have established an O-SVNSTAO methodology for accurate financial fraud detection model. The GIPSO-based FS model efficiently discerns the relevant attributes from sophisticated financial databases, improving the model's discriminative power while alleviating dimensionality problems. Consequently, the SVNSTAO classifier leverages the features selected to discern complicated features inherent in fraudulent actions,

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

which facilitates accurate diagnosis. Moreover, the COA parameter tuning mechanism enhances the SVNSTAO model's parameter, which ensures adaptability and optimum performance to varied fraud settings. Empirical analysis of real-time financial datasets demonstrates the superiority of O-SVNSTAO technique over classical methods, underlining its effectiveness in discovering financial fraud with exceptional efficiency and reliability.

Funding: “The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/48/44)”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] Zhang, X.; Han, Y.; Xu, W.; Wang, Q. HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Inf. Sci. 2021, 557, 302–316.
[2] Benchaji, I.; Douzi, S.; El Ouahidi, B.; Jaafari, J. Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. J. Big Data 2021, 8, 1–21.
[3] Chang, V.; Di Stefano, A.; Sun, Z.; Fortino, G. Digital payment fraud detection methods in digital ages and Industry 4.0. Comput. Electr. Eng. 2022, 100, 107734.
[4] Mustaqim, A.Z.; Adi, S.; Pristyanto, Y.; Astuti, Y. The effect of recursive feature elimination with cross-validation (RFECV) feature selection algorithm toward classifier performance on credit card fraud detection. In Proceedings of the 2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST), Yogyakarta, Indonesia, 29–30 June 2021; pp. 270–275.
[5] Malik, E.F.; Khaw, K.W.; Belaton, B.; Wong, W.P.; Chew, X. Credit card fraud detection using a new hybrid machine learning architecture. Mathematics 2022, 10, 1480
[6] Alam, M.N.; Podder, P.; Bharati, S.; Mondal, M.R.H. Effective machine learning approaches for credit card fraud detection. In Innovations in Bio-Inspired Computing and Applications: Proceedings of the 11th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2020) Held during December 16–18, 2020; Springer International Publishing: Berlin/Heidelberg, Germany, 2021; Volume 11, pp. 154–163.
[7] Sharma, P.; Banerjee, S.; Tiwari, D.; Patni, J.C. Machine learning model for credit card fraud detection-a comparative analysis. Int. Arab J. Inf. Technol. 2021, 18, 789–796.
[8] Prabhakaran, N.; Nedunchelian, R. Oppositional Cat Swarm Optimization-Based Feature Selection Approach for Credit Card Fraud Detection. Comput. Intell. Neurosci. 2023, 2023, 2693022.
[9] Strelcenia, E.; Prakoonwit, S. Improving Classification Performance in Credit Card Fraud Detection by Using New Data Augmentation. AI 2023, 4, 172–198.
[10] Han, S.; Zhu, K.; Zhou, M.; Cai, X. Competition-driven multimodal multiobjective optimization and its application to feature selection for credit card fraud detection. IEEE Trans. Syst. Man Cybern. Syst. 2022, 52, 7845–7857
[11] Zioviris, G., Kolomvatsos, K. and Stamoulis, G., 2024. An intelligent sequential fraud detection model based on deep learning. The Journal of Supercomputing, pp.1-24.
[12] Maashi, M., Alabduallah, B. and Kouki, F., 2023. Sustainable financial fraud detection using garra rufa fish optimization algorithm with ensemble deep learning. Sustainability, 15(18), p.13301.
[13] Forough, J. and Momtazi, S., 2022. Sequential credit card fraud detection: A joint deep neural network and probabilistic graphical model approach. Expert Systems, 39(1), p.e12795.
[14] Chaudhry, R., Kaur, S., Singla, J., Mittal, R. and Malik, V., 2024, March. Fraud Detection and Prevention for a Secure Financial Future Using Artificial Intelligence. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1-6). IEEE.
[15] Krishna, V.R. and Boddu, S., 2023. Hybrid Deep Learning with CSHO based Feature Selection Model for Financial Fraud Detection. International Journal of Intelligent Systems and Applications in Engineering, 11(10s), pp.734-745.
[16] Tang, Y. and Liu, Z., 2024. A Distributed Knowledge Distillation Framework for Financial Fraud Detection based on Transformer. IEEE Access.
[17] Fanai, H. and Abbasimehr, H., 2023. A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection. Expert Systems with Applications, 217, p.119562.
[18] Toskovic, A., Jovanovic, L., Bacanin, N., Stoean, C., Zivkovic, M., Spalevic, P., Petrovic, A., Dobrojevic, M. and Stoean, R., 2023. Applying Recurrent Neural Networks for Anomaly Detection in Electrocardiogram Sensor Data. Sensors, 23(24), p.9878.

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024

[19] Mafarja, M., Thaher, T., Al-Betar, M.A., Too, J., Awadallah, M.A., Abu Doush, I. and Turabieh, H., 2023. Classification framework for faulty-software using enhanced exploratory whale optimizer-based feature selection scheme and random forest ensemble learning. Applied Intelligence, pp.1-43.
[20] Ashraf, S., Abdullah, S., Zeng, S., Jin, H. and Ghani, F., 2020. Fuzzy decision support modeling for hydrogen power plant selection based on single valued neutrosophic sine trigonometric aggregation operators. Symmetry, 12(2), p.298.
[21] Yang, C., Wu, T. and Zeng, L., 2023. Enhancing the chimp optimization algorithm to evolve deep LSTMs for accounting profit prediction using adaptive pair reinforced technique. Evolving Systems, pp.1-20.

Doi: https://doi.org/10.54216/IJNS.230434
Received: November 10, 2023 Revised: January 25, 2024 Accepted: March 25, 2024