INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 19, Issue: 2, Month: April, Year: 2024
Article Number: 6097, https://doi.org/10.15837/ijccc.2024.2.6097

CCC Publications

AGORA UNIVERSITY PRESS

Optimizing dynamic keystroke pattern recognition with hybrid deep learning technique and multiple soft biometric factors

V.Shanmugavalli, A.Rajiv Kannan

V. Shanmugavalli*
Department of Computer Science and Engineering
K.S.R. College of Engineering
Tiruchengode, India
shanmugavalliv@ksrce.ac.in

A. Rajiv Kannan
Department of Computer Science and Engineering
K.S.R. College of Engineering
Tiruchengode, India
rajivkannana@ksrce.ac.in
*Corresponding author: shanmugavalliv@ksrce.ac.in

Abstract

In this work, we propose an optimization approach for dynamic keystroke pattern recognition by leveraging a hybrid deep learning technique and multiple soft biometric factors. Our methodology begins with the introduction of a novel algorithm called dynamic drone squadron optimization (DDSO) to optimize the selection of optimal features from a pool of multiple keystroke features. We then present an enhanced version of the improved sperm swarm optimization (ISSO) algorithm, which effectively combines the optimal weight features derived from multiple biometric responses. Furthermore, we introduce the multi-stage recurrent neural network (MS-RNN) classifier to accurately recognize and classify keystroke patterns. The performance of our proposed ISSO+MS-RNN technique is evaluated using the benchmark KBOC dataset to validate its effectiveness. Comparative analysis is conducted against existing state-of-the-art techniques, employing various evaluation measures, to demonstrate the superior performance of proposed approach.

Keywords: keystroke pattern recognition, soft biometrics, feature optimization, feature fusion, deep learning technique.

1 Introduction

Keystroke pattern recognition [1] is a valuable technology that serves several important purposes. Firstly, it significantly enhances security in various applications. Keystroke patterns are unique to individuals, and by analyzing the dynamic aspects of typing, such as speed, rhythm, and timing, it becomes possible to establish a user's identity with a high level of accuracy [2, 3]. Moreover, keystroke pattern recognition enables continuous authentication, which is particularly beneficial in scenarios where users are logged in for an extended period or engage in sensitive tasks [4]. Unlike static authentication methods, which verify identity only at the time of login, keystroke recognition can monitor and verify the user's identity throughout a session. This ongoing authentication helps prevent unauthorized access and ensures that only authorized individuals have access to protected systems or information. Additionally, keystroke pattern recognition offers user convenience. It is a non-intrusive biometric modality that does not require additional hardware [5]. Users can simply type as they normally would, without the need for specialized devices or physical contact. This makes it a user-friendly authentication solution that seamlessly integrates into existing systems and workflows.

Dynamic keystroke pattern recognition refers to the process of identifying and authenticating individuals based on their unique typing patterns and behavioral characteristics while they are actively typing [6]. By analyzing these dynamic features, a system can create a unique biometric profile for each individual, allowing for reliable identification and verification. It is commonly used in scenarios where continuous authentication is required, such as online examinations, access control systems, and secure authentication for sensitive information. It offers several advantages, including low cost, user convenience, and the ability to passively monitor and authenticate users in real-time without additional hardware requirements [7]. Various machine learning and deep learning techniques are employed in dynamic keystroke pattern recognition systems to effectively model and classify individual keystroke patterns [8].

The use of biometric keystroke dynamics in authentication systems offers numerous advantages over more common alternatives like fingerprint or iris recognition [9]. Unlike other biometric modalities, keystroke dynamics do not require additional sensors or data collection, as they can be captured during regular typing activities, making it convenient for everyday use [10]. These advantages contribute to the growing acceptance of this technology in various domains. However, it is important to note that behavior patterns associated with keystroke dynamics can change over time. Factors such as increased usage, environmental changes, or user habits can lead to variations in typing behavior, potentially affecting the accuracy of authentication systems [11]. For instance, users may hastily enter passwords in certain applications, resulting in different keystroke patterns [12]. Nevertheless, keystroke dynamics possess unique features such as the timing of keystrokes and the applied pressure, which can be utilized to distinguish between different individuals [13, 14]. In the realm of biometric systems, keystroke dynamics offer an intriguing solution for access control due to several reasons [15]. Firstly, this modality does not require additional hardware or biometric identifiers, making it a cost-effective option [16]. Secondly, the timing of keystrokes aligns well with the natural flow of user authentication, enhancing user-friendliness and ease of integration [16]. Moreover, if a personal biometric identifier is compromised, users can easily change their passwords, ensuring security [16]. Additionally, keystroke dynamics can be collected without users' awareness or active cooperation, making it a discreet and non-intrusive biometric method [17]. The widespread use of computers enables continuous recognition using keystroke dynamics, eliminating the need for additional hardware or specialized software [18]. In summary, keystroke dynamics biometrics has the potential to offer a cost-effective, user-friendly, and accurate solution for consistent user authentication [19, 20]. Its unique characteristics make it an appealing option in the field of biometric authentication.

Our contributions. Our research presents a novel optimization approach aimed at enhancing dynamic keystroke pattern recognition. The key highlights of our proposed work are outlined below.

1. Dynamic drone squadron optimization (DDSO) is introduced to enhance the selection of optimal features from a pool of multiple keystroke features.

2. Improved sperm swarm optimization (ISSO) is specifically designed for the fusion of optimal weight features derived from multiple biometric responses. Finally, we introduce the multi-stage recurrent neural network (MS-RNN) as the classifier for recognizing and classifying keystroke patterns.

The remaining sections of the paper are structured as follows: Section 2 provides a comprehensive review of recent studies and research conducted in the field of keystroke recognition systems. In Section 3, we present the problem methodology and system design of our proposed technique. Section 4 delves into the detailed working process of our proposed technique. In Section 5, we present the outcomes and comparative analysis of our proposed technique. Finally, in Section 6, we draw conclusions based on the findings and contributions of our research.

2 Related works

In this section, we provide a comprehensive review of recent works related to the field of keystroke recognition systems. Table 1 describes the summary of research gaps which gathers from the previous works. Ho et al. [21] proposed two distinct methods for keystroke recognition: the mini batch bagging method (MINI-BAG) and the quality ranking of class naive bayes (AR-ONENB) method. MINI-BAG takes inspiration from the concept of packaging, where each attribute in the MINI-BAG database is divided into multiple sub-databases during the pre-processing stage. Alsultan et al. [22] proposed a user verification approach that utilizes free text keystroke dynamics combined with special keystroke features. To enhance the accuracy of the system, they employed decision views to categorize the user data after removing part-time functions and control functions from the typing stream. Ho et al. [23] utilized the ONENB method to evaluate the effectiveness of data characteristics in attacking the keys. They also introduced a speed inspection algorithm called speed inspection in typing skills that analyzes the typing speed of individuals based on their button typing patterns.

Lamiche et al. [24] proposed a multimodal authentication system aimed at enhancing smartphone authentication. This system combines gateway templates and keystrokes captured from the accelerometer, eliminating the need for explicit dynamics, gateway, or textual input during user login. Wang et al. [25] proposed a user authentication system called differential and adversarial noise based user authentication (DEANUA). This system aimed to enhance consistency by addressing error rates. They examined the existing key features and identified a set of 146 optimal features. To select these features, they employed the differential evolution (DE) algorithm. By applying the support vector regression (SVR) method to this feature set, they achieved an equal error rate (EER) of 0.12660% and reduced the energy consumption rate by 31.25%. Saini et al. [26] proposed a three-step authentication model that enables mobile users to authenticate themselves while walking or relaxing. The random forest (RF) and K-nearest neighbor (KNN) algorithms were employed for classification. By optimizing the feature set, the number of characteristics was reduced from 55 to 17, resulting in a slight increase of 2.2% in the equal error rate (EER). Huang et al. [27] investigated a novel approach based on core pressure in keystroke recognition. In this strategy, the user touch time and key features were extracted from the piezo electrical touch panel, a crucial hardware component. This analysis resulted in an impressive error rate of 0.720% (EER).

Kim et al. [28] presented a novel keystroke dynamics system that focuses on recognizing filter-based features within a recognizable environment. Their approach involves evaluating new features and utilizing keyboard dynamics to improve classification accuracy. Kiyani et al. [29] proposed a novel approach that captures the true essence of user behavior through biometric characteristics and introduces a method for user identification based on the specific nature of each activity. They developed a two-phase system, consisting of panel testing and a robust recurrent confidence model (R-RCM), which incorporates two gateways: the alarm gate and the exit gate. Kim et al. [30] presented a novel approach for mobile device user identification using a text-based keystroke dynamics analysis (KDA) system. The system incorporates text-generated keystrokes, accelerometer data, synchronization information, and mobile device timestamps. This approach enhances the accuracy and reliability of user identification on mobile devices.

Lu et al. [31] proposed a novel authentication approach that utilizes keystrokes when users type text. The key data is distributed across a specified key range and transformed into a key vector array based on the timing characteristics of the keystrokes. The effectiveness of the proposed model was evaluated using two benchmark databases, resulting in the best false rejection rates (FRR) of 2.07% and 6.61%, best FAR of 3.26% and 5.31%, and best EER of 2.67% and 5.97%. These results demonstrate the robustness and accuracy of the proposed authentication method. Toosi et al. [32] presented a user authentication system based on keyboard dynamics, which operates at a novel level of analysis. The system leverages time-frequency analysis to directly measure the similarity between the input model and the user's reference model. The input signal undergoes initial preprocessing to extract the main dynamic components. The dynamic time deviation method is employed to ensure that the signal lengths are appropriately aligned for accurate comparison and analysis. This approach enhances the effectiveness and reliability of user authentication based on keyboard dynamics.

3 Need of dynamic keystroke pattern recognition

3.1 Research Gaps

The need for a dynamic keystroke pattern recognition system arises from several factors. The static authentication methods such as passwords or PINs can be easily compromised, leading to security breaches and unauthorized access to sensitive information. A dynamic keystroke pattern recognition system adds an additional layer of security by analyzing the unique typing patterns and behavior of individual users. Continuous authentication systems based on dynamic keystrokes may suffer from a high false rejection rate, where genuine users are incorrectly identified as impostors. This can lead to user frustration and interruptions in the authentication process [21, 22, 23]. It requires users to constantly provide their keystroke patterns, which can be intrusive and may raise privacy concerns. User acceptance of this continuous monitoring can be a significant challenge, as individuals may feel their privacy is compromised. It generates a large amount of data, resulting in high-dimensional feature vectors. Processing and analyzing such high-dimensional data can be computationally expensive and may pose challenges in terms of storage and processing requirements [23]. Achieving high accuracy in continuous authentication systems is crucial. Overfitting is a common problem in machine learning-based authentication systems. It occurs when the model becomes too specific to the training data, leading to poor generalization on unseen data. Overfitting can impact the reliability and effectiveness of continuous authentication using dynamic keystrokes [24, 25]. Continuous authentication systems require regular updates and retraining to adapt to changes in user behavior and typing patterns. This ongoing training process can be time-consuming and resource-intensive, requiring additional efforts and resources [33]. Implementing continuous authentication methods may require additional hardware and infrastructure support, such as specialized keyboards or sensors. These requirements increase the cost and complexity of deploying such systems [26, 28]. Addressing these challenges is crucial to improving the performance, accuracy, and user acceptance of continuous authentication methods based on dynamic keystrokes [27, 34]. Ongoing research and advancements in machine learning algorithms [35, 36], data processing techniques [37, 38], and user-centric design approaches can contribute to overcoming these issues and enhancing the usability and effectiveness of such authentication systems [34]. To address the problems associated with continuous authentication using dynamic keystrokes, the following research objectives.

- To design and develop robust algorithms that can effectively handle variations in dynamic keystroke patterns and minimize the FRR.
- To improve user acceptance of continuous authentication systems by addressing privacy concerns and providing users with more control over their data.
- To explore data processing techniques and dimensionality reduction methods that can handle the high-dimensional nature of dynamic keystroke data.
- To address the issue of overfitting in dynamic keystroke-based authentication models.

Fig. 1 illustrates the overall conceptual design of the proposed technique for continuous authentication using dynamic keystrokes and soft biometrics. The design consists of several interconnected components that work together to achieve accurate and reliable authentication. The proposed research approach involves several steps to address the challenges of continuous authentication using dynamic keystrokes and soft biometrics. Firstly, user keystrokes and multiple soft biometrics are collected as input data. Keystrokes are considered as one set of features, while soft biometrics is treated as another set. Next, feature extraction techniques are applied to both the keystroke and soft biometric data.

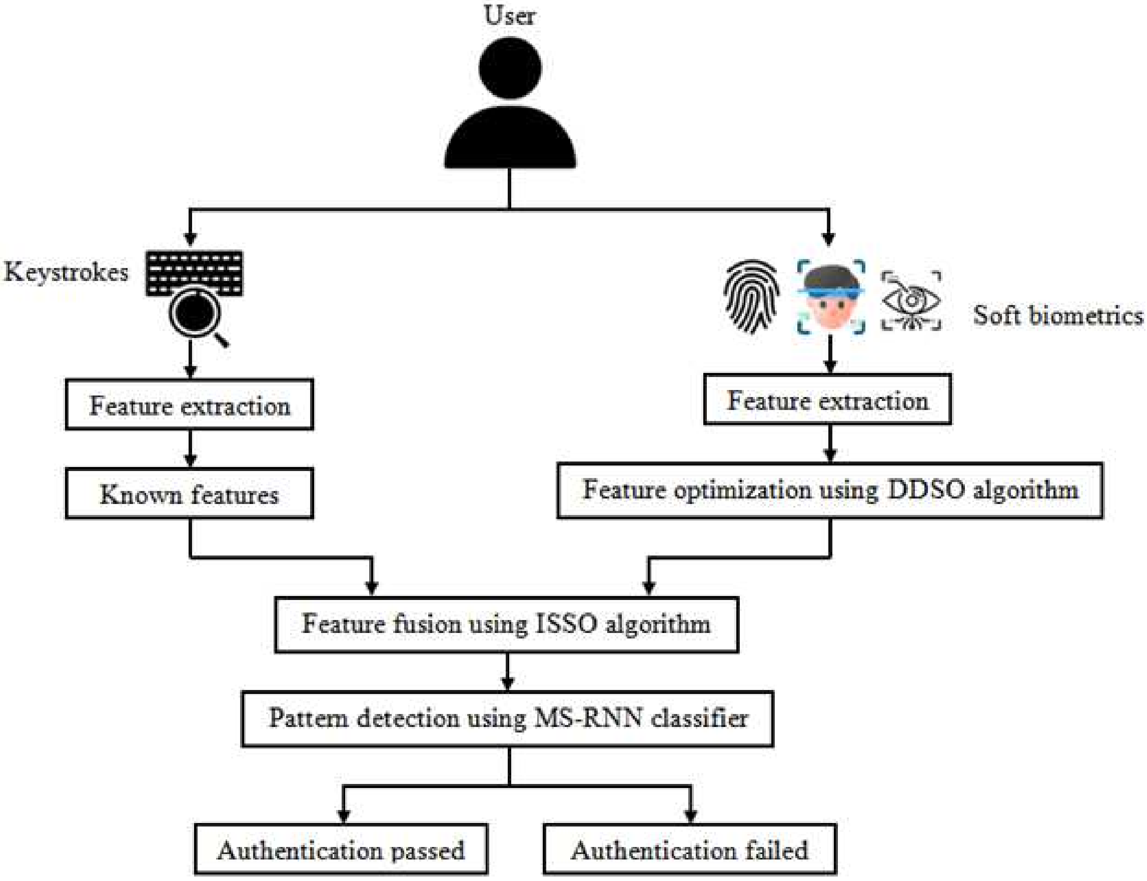

Figure 1: Overall conceptual design of proposed technique

To optimize the feature selection process, a feature optimization algorithm called DDSO is utilized. The fused feature set, consisting of the selected keystroke features and optimal soft biometric features, is then constructed using the ISSO algorithm. ISSO combines the two feature sets in an intelligent and optimized manner, aiming to enhance the authentication accuracy by leveraging the complementary information provided by keystrokes and soft biometrics. Pattern detection and classification are performed using the MS-RNN classifier.

4 Methodology

In this section, we present a detailed explanation of the proposed optimization approach for dynamic keystroke pattern recognition using a hybrid deep learning technique and multiple soft biometric factors. The methodology encompasses three key processes: feature optimization, feature fusion, and pattern detection and classification.

4.1 Feature optimization using DDSO algorithm

Dynamic drone squadron optimization (DDSO) refers to an optimization algorithm specifically designed for optimizing the performance and coordination of drone squadrons. This algorithm aims to maximize the efficiency and effectiveness of a group of drones operating together in a coordinated manner. DDSO involves dynamically adjusting the parameters and behaviors of individual drones within the squadron based on real-time feedback and environmental conditions. DDSO algorithm starts with the parameter initialization.

$$X = departure + offset() \tag{1}$$

Table 1: Summary of Research Gaps

Ref	Methodology	Technique	Findings	Research gaps
[21]	Accurate user authentication	MINIBAG+ AR-ONENB	Accuracy, precision, RMSE	User convenience and cost-effectiveness are major challenges
[22]	Non-conventional keystroke dynamics	SVM+ACO	FAR and FRR	Lacks continuous monitoring capabilities once the user logs in.
[23]	User authentication using keystroke	ONENB+SITS	Accuracy, precision, recall and F-measure	Inefficiency when processing images with low resolution
[24]	Smartphone authentication	ANN+LSTM	FAR and FRR	One-time validation does not provide sufficient security measures.
[25]	User authentication on smartphones	Support vector regression (SVR)	Equal error rate (EER)	The system relies on single behavioral biometrics
[26]	Authentication for mobile phone	RF+KNN+PSO	EER	False rejection rate significantly impacts the system's performance
[27]	User authentication Keystroke	CNN+ERR	Accuracy, precision, EER	Obtaining accurate force touch information poses challenges
[28]	Keystroke dynamics user authentications	Multi-factored with PIN	Accuracy, precision, recall and F-measure	The system fails to address data dimensionality issues adequately
[29]	Continuous user authentication	R-RCM	FAR and FRR	High miss rates
[30]	Keystroke dynamics user authentication	KDA-FACT	Accuracy, precision, recall and F-measure	The system is prone to overfitting problems
[31]	Continuous authentication keystroke	CNN+RNN	FRR, FAR and EER	Requires additional hardware, increasing costs
[32]	Keystroke dynamics for user authentication	Dynamic time warping	Accuracy, precision, recall and F-measure	The training process for the data necessitates more time

$$SD = Calculate(X) \tag{2}$$

where the formulas for calculating the standard deviation of the experimental coordinate are shown and the perturbation motion is represented by the departure coordinate, offset ().

$$X_1 : \overline{gbc} + \left(D_1 \times \left(\overline{gbc} - \overline{cbc_{Drone}}\right)\right) \tag{3}$$

$$X_2 : \overline{cbc_{Drone}} + \left(H(0,1) \times \left(\sqrt{u(0,1)_c} - \overline{cbc_{Drone}}\right)\right) \tag{4}$$

where $H(0,1)$ are drawn from a Gaussian distribution with D_1 a user-defined constant and $u(0,1)_c$ represent a range drawn from a uniform distribution from 0 to 1. It $\overline{gbc}$ represents the global best coordinates and $\overline{cbc_{Drone}}$ is marked with the current best. The B represents the number of drones in each array, C represents the dimension, the upper bounds are the sequence uN, and the lower bounds are the sequence LN. T-shaped function and normal transfer function as follows.

$$T\left(X_h^k(s)\right) = \frac{1}{1 + E^{-x_s^h(s)}} \tag{5}$$

where $X_h^k(s)$ is the iteration's disturbance of the continuous value of the hth drone in the kth dimension. In this instance, a T-shaped function is used to convert the output of the sigmoid operation into binary values.

$$p_h^k = (s+1) = \begin{cases} 0, & \text{if } rand < T\left(X_h^k(s)\right) \\ \\ 1, & \text{if } rand > T\left(X_h^k(s)\right) \end{cases} \tag{6}$$

where p_h^k and $X_h^k(s)$ denote the state of the h-th drone and the perturbation when iterating in the K-th dimension. Aircraft transfer operations must traverse a unique search space is defined as follows.

$$v\left(X_h^k(s)\right) = \left| Erf\left(\frac{\sqrt{\pi}}{2} X_h^k(s)\right)\right| \tag{7}$$

$$v\left(X_h^k(s)\right) = \left| \frac{\sqrt{\pi}}{2} \int_0^{\frac{\sqrt{\pi}}{2} X_h^k(s)} E^{-s^2} cs \right| \tag{8}$$

$$p_h^k(s+1) = \begin{cases} (p_h^k(s)^{-1}), & \text{if } rand < v\left(X_h^k(s)\right) \\ \\ p_h^k(s), & \text{if } rand > v\left(X_h^k(s)\right) \end{cases} \tag{9}$$

where $p_h^k(s)$ and $X_h^k(s)$ specify the position of the h-th drone and the perturbation in the kth dimension when iterating to sand $p_h^k(s)^{-1}$ represents the complement of $p_h^k(s)$.

$$fitness = \alpha\gamma r(C) + \beta \frac{|r|}{|B|} \tag{10}$$

where $\alpha\gamma r(C)$ is the KNN classifier's classification error rate. In addition, B represents the overall features from the dataset, while r indicates the selected best optimal features. The parameters $\alpha \in [0, 1]$ and $\beta = (1-\alpha)$ are linked to the relevance of the subset length and the quality of the classification, respectively. The algorithm 1 describes the working process involved in the feature optimization using DDSO algorithm.

4.2 Feature fusion using ISSO algorithm

Feature fusion refers to the process of combining multiple sets of features extracted from different sources or modalities into a single unified feature representation. Improved sperm swarm optimization (ISSO) is a metaheuristic algorithm inspired by the collective behavior of sperm cells to solve optimization problems. The following function represents the probability $proj_a$ of compute the optimal solution for feature fusion using the roulette wheel selection:

$$proj_a = Exp\left(\frac{-Beta \cdot fit_a}{worstfit_a}\right) \tag{11}$$

$$proj_a = \frac{proj_a}{\sum_{a-1}^{rpop} fit_a} \tag{12}$$

where Pop is the size of the population, selection pressure Beta = 8, fit_a chromosome fitness equals the lowest fitness achieved. The following formula is used to calculate the initial sperm velocity:

$$U_0 = damp \cdot U_a \cdot Log_{10}(xG_1) \tag{13}$$

Algorithm 1 Feature optimization using DDSO

```
Input  : Number of data, known features, maximum iteration
Output : Best optimal features
Initialize the random population
Define firmware using $X = departure + offset()$
If h=0,g=1
While Do
Compute T-shaped function and typical transfer function
$T\left(X_h^k(s)\right) = \frac{1}{1+E^{-x_s^h(s)}}$
Compute transfer functions using discrete search space
$v\left(X_h^k(s)\right) = \left|Erf\left(\frac{\sqrt{\pi}}{2}X_h^k(s)\right)\right|$
If not discard then
Compute subset of features and fitness function $\alpha\gamma r(C) + \beta\frac{|r|}{|B|}$
Find a best output value
End if
end
```

where U_a is the ongoing sperm speed, an irregular $xG(pH)$ esteem somewhere in the range of 7 and 14, and the damping factor (from 0 to 1). Register the individual and worldwide best arrangements as follows.

$$currentbestsol(s) = log_{10}(xG_2) \cdot log_{10}(temp_1) \cdot (p_{Tbest_a} - p_a(s)) \tag{14}$$

$$globalbestsol(s) = log_{10}(xG_3) \cdot log_{10}(temp_2) \cdot (p_{thbest_a} - p_a(s)) \tag{15}$$

The velocity of the sperm is evaluated in the following ways: where xG_2 is the current location of the sperm at iteration t, xG_3 is the global best location, and p_{Tbest_a} is the personal best location of sperm a at iteration s. Temp1 and Temp2 are random temperature values between 35.1 and 38.5 ^{o}C, and are random $xG(pH)$ values between 7 and 14.

$$\begin{aligned} U_0 &= damp \cdot U_a \cdot Log_{10}(xG_1) \\ &+log_{10}(xG_2) \cdot log_{10}(temp_1) \cdot (p_{Tbest_a} - p_a(s)) \\ &+log_{10}(xG_3) \cdot log_{10}(temp_2) \cdot (p_{thbest_a} - p_a(s)) \end{aligned} \tag{16}$$

On each iteration toward achieving the global optimal solution, the sperm's current position is computed to update the position.

$$p_a(s) = p_a(s) + p_a(s) \tag{17}$$

Before assessing fitness, velocity and position limits are imposed to prevent the method from departing from the global optima solution. The values for the maximum and minimum speeds are determined as follows.

$$U_{Max} = 0.1 * (Uar_{Max} - Uar_{Min}) \tag{18}$$

$$U_{Min} = -U_{Max} \tag{19}$$

where U_{max} and U_{min} are the respective maximum and minimum position limits, as well as the speed limit and the minimum speed limit. The population is then merged, sorted, and truncated once more for the next iteration after the velocity and position update is finished. After that, the population's fitness is examined and updated to determine whether the new values are superior to the previous global best solution. The working process of feature fusion using ISSO is described in Algorithm 2.

Algorithm 2 Feature fusion using ISSO

```
Input  : vectors
Output : parameters
Initialize the random population
Set the number of population (rPop),maximum iteration (MaxIter) and iter=0
If i=0 , j=1
while (iter<MaxIter)
Use Roulette Wheel to SELECT parents.
Define roulette wheel selection $proj_a = Exp\left(\frac{-Beta \cdot fit_a}{worstfit_a}\right)$
Compute initial sperm velocity $U_0 = damp \cdot U_a \cdot Log_{10}(xG_1)$
Compute maximum and minimum velocity $U_{Max} = 0.1 * (Uar_{Max} - Uar_{Min})$
Find best output values
End if
end
```

4.3 Pattern detection and classification

Pattern detection and classification refer to the process of identifying and categorizing patterns or trends in data based on their underlying characteristics or features. The multi-stage recurrent neural network (MS-RNN) classifier is a type of neural network architecture that is specifically designed for sequence data analysis, such as keystroke patterns. RNNs maintain an internal memory that allows them to consider previous inputs, which is crucial when dealing with dynamic keystroke patterns where the timing and order of key presses are significant. Additionally, RNNs offer a flexible architecture that accommodates varying sequence lengths, making them applicable to our dynamic keystroke dataset, where users may exhibit different typing speeds and durations. The capability of RNNs to handle variable-length sequences aligns with the dynamic and continuous nature of keystroke patterns.A distinct level c, a concealed state h, an update step g, and three gates are present in each layer: The following is the consensus for the time calculation: input i, forget f, and output o.

$$j_T = \sigma(L_{yj} y_T + a_{yj} + L_{ej} e_{T-1} + a_{yj}) \tag{20}$$

$$j_T = \sigma(L_{yg} y_T + a_{yg} + L_{eg} e_{T-1} + a_{eg}) \tag{21}$$

$$O_T = \sigma(L_{yo} y_T + a_{yo} + L_{eo} e_{T-1} + a_{eo}) \tag{22}$$

$$d_T = g_1 d_{T_1} + j_T \quad tanh(L_{yf} y_T + c_{yf} + L_{ef} e_{T+1} + a_{ef}) \tag{23}$$

$$e_T = o_T \quad tanh(d_{T-1}) \tag{24}$$

Here, σ is tanh is a function of sigmoid activation, a function of hyperbolic, and $\odot$ represents element wise multiplication. The volume normalization modification starts as follows

$$\tilde{y_j} = \frac{y_j - \mu_A}{\sqrt{\sigma_A^2 + \in}} \tag{25}$$

Input is shifted

$$x_j = \gamma \tilde{y_j} + \beta \tag{26}$$

where γ and β are parameter educated during preparation along with other options. Module normalization change AM (,β) is introduced into,

$$\begin{pmatrix} g_T \\ j_T \\ o_T \\ f_T \end{pmatrix} = An(L_e e_{T_1}; \gamma_e \beta_e) + \ AN(L_y y_T; \gamma_n \beta_n) \tag{27}$$

$$d_T = \sigma(g_T) d_{T-1} + \sigma(j_T)\ tanh(f_T) \tag{28}$$

$$e_T = \sigma(o_T)\ tanh(AM(d_T; \gamma_d, \beta_d)) \tag{29}$$

Continuous input terms are specifically defined. Hyper parameter optimization can be expressed by the equation:

$$y_{Best} = Arg\ Min\ g(y) | y \in Y \tag{30}$$

where $g(y)$ denotes a decrease in points, y_{best} denotes the hyper parameter combination that results in the score $g(y)$ with the lowest value, and the Y denotes the domain of hyper parameter values. Y is transformed into y_{best} using the maximum normalization method:

$$y' = \frac{y - Min(y)}{Max(y) - Min(y)} \tag{31}$$

where y is the real charge of the characteristic, $Min(y)$ and $Max(y)$ is the bare minimum and maximum of this characteristic and y is the default assessment. The working function of pattern detection and classification using MS-RNN is described in Algorithm 3.

Algorithm 3 Pattern detection and classification using MS-RNN

```
Input       :Fused features (Keystrokes and soft-bios)
Output      : Authentication  passed and Authentication failed
1  Define the normalization
   $\tilde{y_j} = \frac{y_j - \mu_A}{\sqrt{\sigma_A^2 + \in}}$
2  Compute the module normalization using
3  Define the hyper parameter
   $\begin{pmatrix} g_T \\ j_T \\ o_T \\ f_T \end{pmatrix} = An(L_e e_{T_1}; \gamma_e \beta_e) + \ AN(L_y y_T; \gamma_n \beta_n)$
4  Update the positions
5  Determine the maximum normalization using
   $y' = \frac{y - Min(y)}{Max(y) - Min(y)}$
6  End
```

5 Simulation Results

This section focuses on the simulation results and comparative analysis of various dynamic keystroke pattern recognition techniques, including our proposed ISSO+MS-RNN technique. Our proposed technique is implemented on the Google Colab simulation environment with the Python programming language. To validate the performance of our approach, we conducted experiments using the KBOC16 Corpus dataset. The simulation results of our ISSO+MS-RNN technique were compared with existing techniques, evaluating them based on several measures, including accuracy, precision, recall, F-measure, Matthews correlation coefficient (MCC), dice coefficient, equal error rate (EER), false rejection rate (FRR), and false acceptance rate (FAR). The dataset used in this study was collected by capturing the keystroke patterns of users while interacting with an End User License Agreement (EULA). The dataset, known as the KBOC16 Corpus, includes keystroke sequences obtained from 300 subjects. Table 2 provides a comprehensive description of the dataset, which serves as the foundation for the analysis and evaluation of the proposed techniques in this study.

Table 2: Dataset description

Description	**Value**
Number of users	300
Number of features	20
Samples per user	24
Average separation between sessions	30 days

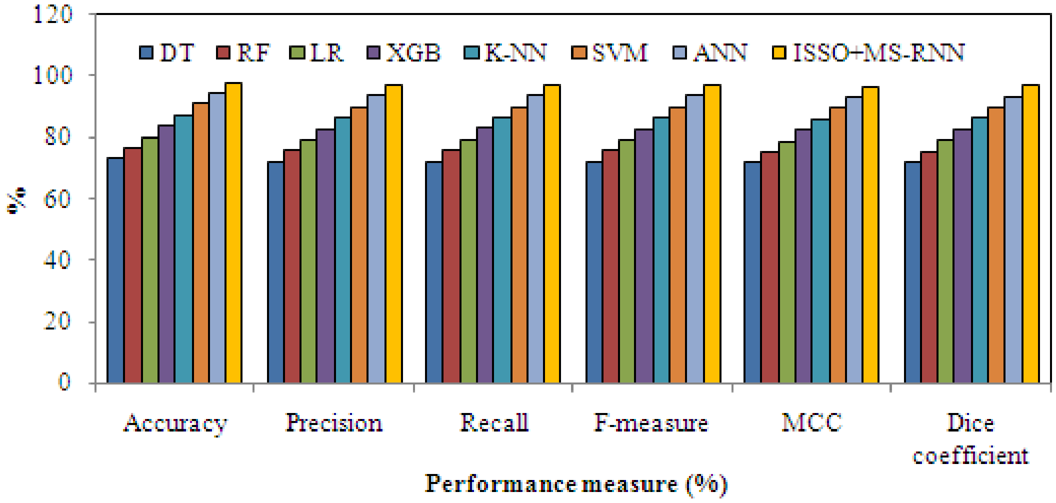

Figure 2: Performance measure comparison of proposed and benchmark techniques

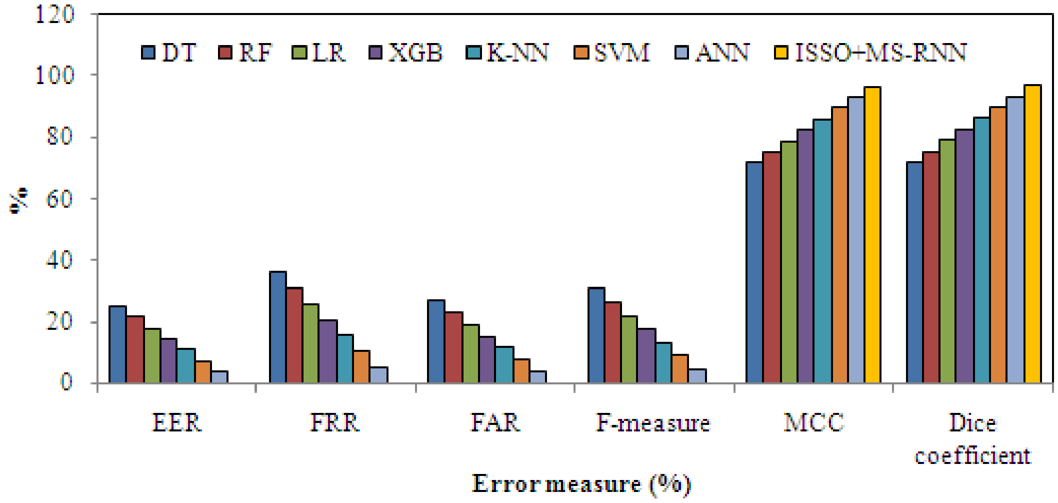

Figure 3: Error measure comparison of proposed and benchmark techniques

Table 3 presents a comparison of the results obtained from the proposed technique and existing techniques for the KBOC16 Corpus dataset. The table showcases the performance evaluation measures used to assess the effectiveness of the different techniques in terms of accuracy, precision, recall, F-measure, MCC, dice coefficient, EER, FRR, and FAR. The techniques evaluated include decision tree (DT), random forest (RF), logistic regression (LR), XGBoost (XGB), k-nearest neighbors (K-NN), support vector machine (SVM), artificial neural network (ANN), and the proposed ISSO+MS-RNN technique.

Table 3: Results comparison of proposed and existing techniques for KBOC16 Corpus dataset

Technique	Performance measure (%)						Error measure (%)		
	Accuracy	Precision	Recall	Rank-1	MCC	Dice coefficient	EER	FRR	FAR
DT	72.880	72.002	72.047	72.024	71.547	71.781	25.248	36.022	26.848
RF	76.448	75.570	75.615	75.592	75.115	75.349	21.659	30.898	23.059
LR	80.016	79.138	79.183	79.160	78.683	78.917	18.070	25.775	19.270
XGB	83.584	82.706	82.751	82.728	82.251	82.485	14.481	20.652	15.481
K-NN	87.152	86.274	86.319	86.296	85.819	86.053	10.892	15.528	11.692
SVM	90.720	89.842	89.887	89.864	89.387	89.621	7.303	10.405	7.903
ANN	94.288	93.410	93.455	93.432	92.955	93.189	3.714	5.281	4.114
ISSO+ MS-RNN	97.856	96.978	97.023	97.000	96.523	96.757	0.125	0.158	0.325

Table 4: Results comparison of proposed and existing state-of-art techniques for KBOC16 Corpus dataset

Ref	Technique	Performance measure (%)						Error measure (%)		
		Accuracy	Precision	Recall	Rank-1	MCC	Dice coefficient	EER	FRR	FAR
[21]	MINIBAG	83.036	72.558	59.141	65.166	92.251	89.941	25.949	14.978	24.193
[22]	SVM+ACO	84.271	74.593	62.298	67.893	92.607	90.509	23.797	13.743	22.204
[23]	ONENB+ SITS	85.506	76.628	65.455	70.602	92.963	91.077	21.645	12.508	20.215
[24]	ANN+LSTM	86.741	78.663	68.612	73.294	93.319	91.645	19.493	11.273	18.226
[25]	SVR	87.976	80.698	71.769	75.972	93.675	92.213	17.341	10.038	16.237
[26]	RF+KNN+ PSO	89.211	82.733	74.925	78.636	94.031	92.781	15.189	8.803	14.248
[27]	CNN+ERR	90.446	84.768	78.082	81.288	94.387	93.349	13.037	7.568	12.259
[28]	MF-PIN	91.681	86.803	81.239	83.929	94.743	93.917	10.885	6.333	10.270
[29]	R-RCM	92.916	88.838	84.396	86.560	95.099	94.485	8.733	5.098	8.281
[30]	KDA-FACT	94.151	90.873	87.553	89.182	95.455	95.053	6.581	3.863	6.292
[31]	CNN+RNN	95.386	92.908	90.709	91.796	95.811	95.621	4.429	2.628	4.303
[32]	Dynamic time warping	96.621	94.943	93.866	94.402	96.167	96.189	2.277	1.393	2.314
Our	ISSO+MS- RNN	97.856	96.978	97.023	97.000	96.523	96.757	0.125	0.158	0.325

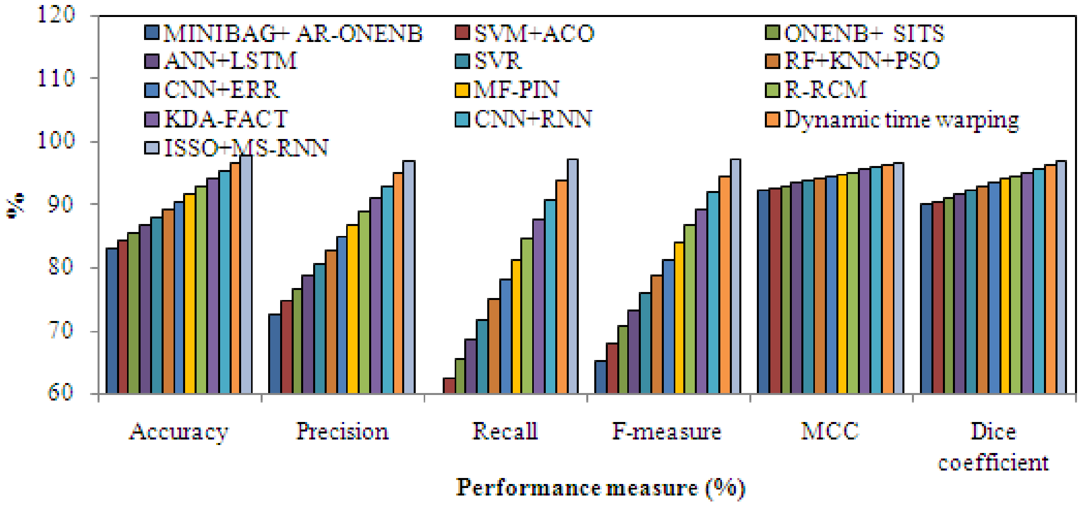

Figure 4: Performance comparison analysis of proposed and existing state of the art techniques

Fig.2 shows the performance comparative analysis of proposed and existing techniques. Fig.3 shows the error measure comparative analysis of proposed and existing techniques. ISSO+MS-RNN technique achieves the highest Dice coefficient of 96.757%, outperforming all the previous techniques. It demonstrates a remarkable 3.568% increase compared to ANN.ISSO+MS-RNN outperform tra-

Table 5: Results of proposed technique with respect to Real-time data

Feature combination		Performance measure (%)						Error measure (%)		
Key stroke	Soft biometric	Accuracy	Precision	Recall	Rank-1	MCC	Dice coefficient	EER	FRR	FAR
Weighted sum	Height	97.856	96.589	97.102	96.845	97.035	96.789	0.235	0.149	0.214
Product	Height	97.868	96.601	97.114	96.857	97.047	96.801	0.248	0.162	0.227
Max	Height	97.881	96.614	97.127	96.869	97.060	96.814	0.260	0.174	0.239
Sum	Height	97.893	96.626	97.139	96.882	97.072	96.826	0.273	0.187	0.252
Weighted sum	Weight	97.905	96.638	97.151	96.894	97.084	96.838	0.285	0.199	0.264
Product	Weight	97.918	96.651	97.164	96.906	97.097	96.851	0.298	0.212	0.277
Max	Weight	97.930	96.663	97.176	96.919	97.109	96.863	0.310	0.224	0.289
Sum	Weight	97.942	96.675	97.188	96.931	97.121	96.875	0.323	0.237	0.302
Weighted sum	Gender	97.954	96.687	97.200	96.943	97.133	96.887	0.335	0.249	0.314
Product	Gender	97.967	96.700	97.213	96.956	97.146	96.900	0.348	0.262	0.327
Max	Gender	97.979	96.712	97.225	96.968	97.158	96.912	0.360	0.274	0.339
Sum	Gender	97.991	96.724	97.237	96.980	97.170	96.924	0.373	0.287	0.352
Weighted sum	Age	98.004	96.737	97.250	96.992	97.183	96.937	0.385	0.299	0.364
Product	Age	98.016	96.749	97.262	97.005	97.195	96.949	0.398	0.312	0.377
Max	Age	98.028	96.761	97.274	97.017	97.207	96.961	0.410	0.324	0.389
Sum	Age	98.040	96.773	97.286	97.029	97.219	96.973	0.423	0.337	0.402
Average		**97.948**	**96.681**	**97.194**	**96.937**	**97.127**	**96.881**	**0.329**	**0.243**	**0.308**

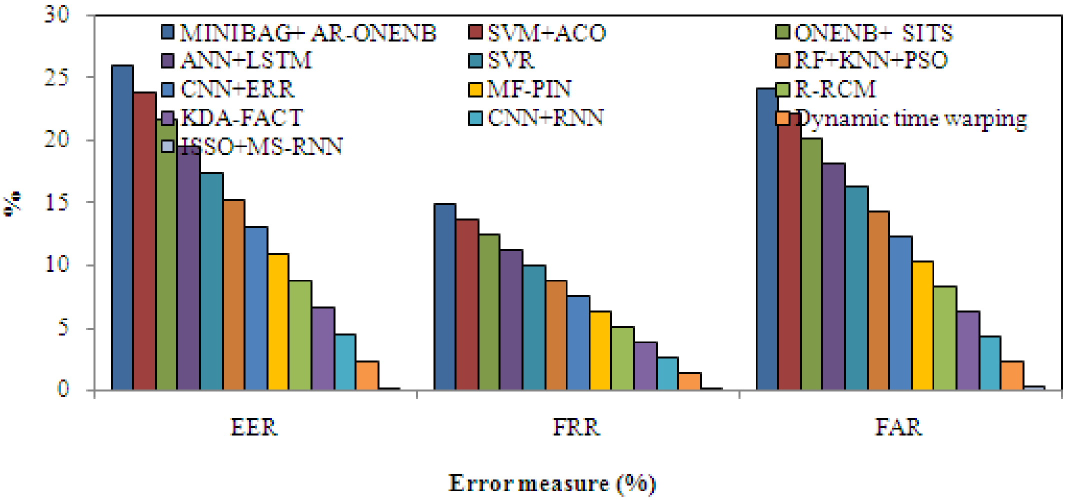

Figure 5: Error measure comparison of proposed and existing state of the art techniques

ditional and ML techniques across various evaluation metrics, indicating an improvement in overall performance. The method effectively addresses the challenges faced by previous methods in terms of accuracy, robustness, and adaptability to dynamic keystroke patterns. Table 4 presents a comparison of performance measures for various state-of-the-art techniques, including the proposed ISSO+MS-RNN technique. Fig.4 and 5 shows the performance measure comparative analysis of proposed and existing state of the art techniques.ISSO+MS-RNN technique outperforms than other techniques, achieving the highest performance measures. It achieves an accuracy of 97.856%, precision of 96.978%, recall of 97.023%, Rank-1 of 97%, MCC of 96.523%, and Dice coefficient of 96.757%. ISSO+MS-RNN achieve higher accuracy, precision, recall, and F-measure compared to existing techniques. The optimization process by ISSO and the use of MS-RNN contribute to enhanced feature selection and improved classification accuracy, reducing errors in keystroke pattern recognition. ISSO efficiently selects the most relevant features from the pool of multiple keystroke features, reducing data dimensionality and enhancing the discriminative power of the model. MS-RNN combines the strengths of recurrent neural networks with multiple soft biometric factors, providing a more nuanced understanding of keystroke patterns and improving overall classification performance. Table 5 presents the results of the proposed technique for keystroke pattern recognition with respect to real-time data, considering different feature combinations. Overall, the accuracy and other performance measures remain consistently high for most feature combinations, indicating the effectiveness of the proposed technique in real-time data scenarios.

6 Conclusion

An innovative approach is proposed for dynamic keystroke pattern recognition using multiple soft biometric factors. Here, we utilized the DDSO or optimal feature selection, and ISSO for integrate the features and MS-RNN for recognizing and classifying keystroke patterns. Our ISSO+MS-RNN are validated by KBOC dataset, ensuring the reliability and effectiveness of our approach. In terms of accuracy, our method achieves an impressive 97.856%, surpassing all the compared techniques, which shows a substantial increase of 1.435% compared to the closest competitor, the dynamic time warping method, which stands at 96.621%. The precision of our ISSO+MS-RNN is equally remarkable at 96.978%, showcasing its ability to correctly identify positive instances. In terms of error measures, our method achieves an extremely low EER of 0.125%, shows its ability to balance false acceptance and false rejection rates effectively. From the results we highlight its potential for real-time applications that require accurate and reliable keystroke pattern recognition.Our technique achieves significant improvements in performance compared to existing state-of-the-art techniques, with higher accuracy and lower error rates. The sophisticated nature of the algorithm, while contributing to its superior performance, might require substantial computational power and memory. It potentially limits its applicability in resource-constrained environments with limited processing capabilities. For real-time case often demand low-latency responses, the computational complexity is drawback for scenarios where quick decision-making is crucial.

References

[1] Hosseinzadeh, D.; Krishnan, S. (2008). Gaussian mixture modeling of keystroke patterns for biometric applications, *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 38(6), 816–826, 2008.

[2] Urtiga, E.V.C. ; Moreno, E.D. (2011). Keystroke-based biometric authentication in mobile devices, *IEEE Latin America Transactions*, 9(3), 368–375, 2011.

[3] Ahmed, A.A.; Traore, I. (2013). Biometric recognition based on free-text keystroke dynamics, *IEEE transactions on cybernetics*, 44(4), 458–472, 2013.

[4] Sitova, Z.; Sedenka, J.; Yang, Q.; Peng, G.; Zhou, G.; Gasti, P.; Balagani, K.S. (2015). HMOG: New behavioral biometric features for continuous authentication of smartphone users, *IEEE Transactions on Information Forensics and Security*, 11(5), 877–892, 2015

[5] Morales, A.; Fierrez, J.; Tolosana, R.;Ortega-Garcia, J.; Galbally, J.; Gomez-Barrero, M.; Anjos, A.; Marcel, S. (2016). Keystroke biometrics ongoing competition, *IEEE Access*, 4, 7736—7746, 2016.

[6] Mondal, S.; Bours, P. (2017). Person identification by keystroke dynamics using pairwise user coupling, *IEEE Transactions on Information Forensics and Security*, 12(6), 1319-1329, 2017.

[7] Venkatesan, V.K.; Kuppusamy Murugesan, K.R.; Chandrasekaran, K.A.; Thyluru Ramakrishna, M; Khan, S.B.; Almusharraf, A ; Albuali, A. (2023). Cancer Diagnosis through Contour Visualization of Gene Expression Leveraging Deep Learning Techniques, *Diagnostics*, 3(22), 3452, 2023.

[8] Alpar, O. (2017). Frequency spectrograms for biometric keystroke authentication using neural network based classifier, *Knowledge-Based Systems*, 116, 163–171, 2017.

[9] Mondal, S.; Bours, P. (2017). A study on continuous authentication using a combination of keystroke and mouse biometrics, *Neurocomputing*, 230, 1–22, 2017.

[10] Goodkind, A.; Brizan, D.G.; Rosenberg, A. (2017). Utilizing overt and latent linguistic structure to improve keystroke-based authentication, *Image and Vision Computing*, 58, 230–238, 2017.

[11] Kim, J.; Kim, H.; Kang, P. (2018). Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection, *Applied Soft Computing*, 62, 1077–1087, 2018.

[12] Muliono, Y.; Ham, H.; Darmawan, D. (2018). Keystroke dynamic classification using machine learning for password authorization, *Procedia Computer Science*, 135, 564–569, 2018.

[13] Awasthi, M. A.; T R, M.; Joshi, D. R.; Pandey, D. A. K; Saxena, D. R.; Goswami, S (2022). Smart Grid Sensor Monitoring Based on Deep Learning Technique with Control System Management in Fault Detection, *International Journal of Communication Networks and Information Security (IJCNIS)*, 14(3), 123–137, 2022.

[14] Pisani, P.H.; Giot, R.; De Carvalho, A.C.; Lorena, A.C. (2016). Enhanced template update: Application to keystroke dynamics, *Computers and Security*, 60, 134–153, 2016.

[15] 15. Ogbanufe, O.; Kim, D.J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, *Decision Support Systems*, 106, 1–14, 2018.

[16] Chang, C.; Eude, T.; Obando Carbajal, L.E. (2016). Biometric authentication by keystroke dynamics for remote evaluation with one-class classification, *In Advances in Artificial Intelligence: 29th Canadian Conference on Artificial Intelligence, Canadian AI 2016, Victoria, BC, Canada, May 31-June 3, 2016.* Proceedings 29,(21–32), Springer International Publishing.

[17] Ali, M.L.; Monaco, J.V.; Tappert, C.C.; Qiu, M. (2017). Keystroke biometric systems for user authentication, *Journal of Signal Processing Systems*, 86, 175–190, 2017.

[18] Senthil Kumar, T.; Suresh, A.; Karumathil, A. (2014). Improvised classification model for cloud based authentication using keystroke dynamics, *In Frontier and Innovation in Future Computing and Communications*, Springer Netherlands, 885–893, 2014.

[19] Neha; Chatterjee, K. (2019). Biometric re-authentication: An approach towards achieving transparency in user authentication, *Multimedia Tools and Applications*, 78, 6679–6700, 2019.

[20] 20. Shi, Y.; Wang, X.; Zheng, K.; Cao, S. (2023). User authentication method based on keystroke dynamics and mouse dynamics using HAD, *Multimedia Systems*, 29(2), 653–668, 2023.

[21] Baskaran, N. K.; Mahesh, T. R. (2023). Performance Analysis of Deep Learning based Segmentation of Retinal Lesions in Fundus Images, *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 1306–1313, 2023.

[22] Alsultan, A.; Warwick, K.; Wei, H. (2017). Non-conventional keystroke dynamics for user authentication, *Pattern Recognition Letters*, 89, 53–59, 2017.

[23] Ho, J.; Kang, D.K. (2018). One-class naive Bayes with duration feature ranking for accurate user authentication using keystroke dynamics, *Applied Intelligence*, 48(6), 1547–1564, 2018.

[24] Lamiche, I.; Bin, G.; Jing, Y.; Yu, Z.; Hadid, A. (2019). A continuous smartphone authentication method based on gait patterns and keystroke dynamics, *Journal of Ambient Intelligence and Humanized Computing*, 10(11), 4417–4430, 2019.

[25] Wang, Y.; Wu, C.; Zheng, K.; Wang, X. (2019). Improving reliability: User authentication on smartphones using keystroke biometrics, *IEEE Access*, 7, 26218–26228, 2019.

[26] Saini, B.S.; Singh, P.; Nayyar, A.; Kaur, N.; Bhatia, K.S.; El-Sappagh, S.; Hu, J.W. (2020). A Three-Step Authentication Model for Mobile Phone User Using Keystroke Dynamics, *IEEE Access*, 8, 125909–125922, 2020.

[27] Huang, A.; Gao, S.; Chen, J.; Xu, L.; Nathan, A. (2020). High Security User Authentication Enabled by Piezoelectric Keystroke Dynamics and Machine Learning, *IEEE Sensors Journal*, 20(21), 1303–13046, 2020.

[28] Kim, D.I.; Lee, S.; Shin, J.S. (2020). A new feature scoring method in keystroke dynamics-based user authentications, *IEEE Access*, 8, 27901–27914, 2020.

[29] Kiyani, A.T.; Lasebae, A.; Ali, K.; Rehman, M.U.; Haq, B. (2020). Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach, *IEEE Access*, 8, 156177–156189, 2020.

[30] Kim, J.; Kang, P. (2020). Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features, *Pattern Recognition*, 108, 107556, 2020.

[31] Lu, X.; Zhang, S.; Hui, P.; Lio, P. (2020). Continuous authentication by free-text keystroke based on CNN and RNN, *Computers and Security*, 96, 101861, 2020.

[32] Toosi, R.; Akhaee, M.A. (2021). Time–frequency analysis of keystroke dynamics for user authentication, *Future Generation Computer Systems*, 115, 438–447, 2021.

[33] Ramu, T.; Suthendran, K.; Arivoli, T. (2019). Machine learning based soft biometrics for enhanced keystroke recognition system, *Multimedia Tools and Applications*, 1–17, 2019.

[34] Shanmugavalli, V.; Suresh Kumar, S.; Nithya Kalyani, S. (2023). A Hybrid Machine Learning Technique for Multiple Soft Biometric Based Dynamic Keystroke Pattern Recognition System, *Neural Processing Letters*, 1–27, 2023.

[35] Shen, M.; Shen, J.; Yu, L. (2023). Neural integrated Markov model for effective script identification and classification in biometric system, *Journal of Radiation Research and Applied Sciences*, 100694, 2023

[36] Gona, A.; Subramoniam, M.; Swarnalatha, R. (2023). Transfer learning convolutional neural network with modified Lion optimization for multimodal biometric system, *Computers and Electrical Engineering*, 108, 108664, 2023.

[37] Shakil, S.; Arora, D.; Zaidi, T. (2023). Feature identification and classification of hand based biometrics through ensemble learning approach, *Measurement: Sensors*, 25, 100593, 2023.

[38] Coelho, K.K.; Tristao, E.T.; Nogueira, M., Vieira, A.B.; Nacif, J.A. (2023). Multimodal biometric authentication method by federated learning, *Biomedical Signal Processing and Control*, 85, 105022, 2023.

Cite this paper as:
Shanmugavalli, V.; Rajiv Kannan, A. (2024). Optimizing dynamic keystroke pattern recognition with hybrid deep learning technique and multiple soft biometric factors, *International Journal of Computers Communications & Control*, 19(2), 6097, 2024.
https://doi.org/10.15837/ijccc.2024.2.6097