*Computers, Materials & Continua*
DOI: 10.32604/cmc.2022.026457
***Article***

Tech Science Press

# Artificial Intelligence Techniques Based Learner Authentication in Cybersecurity Higher Education Institutions

**Abdullah Saad AL-Malaise AL-Ghamdi[1] and Mahmoud Ragab[2,3,4,*]**

[1]Information Systems Department, Faculty of Computing and Information Technology King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Centre of Artificial Intelligence for Precision Medicines, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[4]Mathematics Department, Faculty of Science, Al-Azhar University, Naser City, 11884, Cairo, Egypt
*Corresponding Author: Mahmoud Ragab. Email: mragab@kau.edu.sa
Received: 27 December 2021; Accepted: 11 February 2022

**Abstract:** Education 4.0 is being authorized more and more by the design of artificial intelligence (AI) techniques. Higher education institutions (HEI) have started to utilize Internet technologies to improve the quality of the service and boost knowledge. Due to the unavailability of information technology (IT) infrastructures, HEI is vulnerable to cyberattacks. Biometric authentication can be used to authenticate a person based on biological features such as face, fingerprint, iris, and so on. This study designs a novel search and rescue optimization with deep learning based learning authentication technique for cybersecurity in higher education institutions, named SRODL-LAC technique. The proposed SRODL-LAC technique aims to authenticate the learner/student in HEI using fingerprint biometrics. Besides, the SRODL-LAC technique designs a median filtering (MF) based preprocessing approach to improving the quality of the image. In addition, the Densely Connected Networks (DenseNet-77) model is applied for the extraction of features. Moreover, search and rescue optimization (SRO) algorithm with deep neural network (DNN) model is utilized for the classification process. Lastly, template matching process is done for fingerprint identification. A wide range of simulation analyses is carried out and the results are inspected under several aspects. The experimental results reported the effective performance of the SRODL-LAC technique over the other methodologies.

**Keywords:** Cybersecurity; authentication; biometrics; security; higher education institution; deep learning

## 1 Introduction

The use of digital learning environment (DLE) is increasing in the area of higher education institutions (HEI). Digitalization is the key solution to present problems: it enhances flexibility

to higher educational study [1] and makes them available for every student, notwithstanding their personal life situations, disabilities, geo-graphical location, or exceptional global or local circumstance (for example COVID19). Also, increases the opportunity for different student populations in line with European higher education policy. This policy indicates a stronger commitment to enhancing the opportunity of different learners. Moreover, legislation associated with online education and services has been proposed [2]. Also, In the EU, legislation for accessibility, security, and data transmission has become effective that has been increasing the awareness of these problems amongst end users. Meanwhile, the digitalization processes bring greater opportunities and also present various problems to HEI. Because of the possibility of impersonation, several online programs or online universities still provide the final examination in person and on campus as the only legitimate choice [3]. Thus, enhancing learner authentication, emerging online educations, and mode of e-assessment is very important.

An effective and reliable authentication scheme is the only assurance for the students' authorship and identity of the exams, assignments, or other online activities [4]. When HEI provides usable and secure system for e-authentication, they are capable of producing more reliable environments for every student, including distant learners, adult and SEND students. The pandemic highlights the requirement for strong authentication in HEI [5]. In addition, with the lack of IT infrastructure and teams, education institutions must have system in place for preventing identification and cybersecurity problems. Conventionally, biometric authentication has been modernized into on-boarding process and offers touchless solutions. But education can be a use case for biometric techniques as its aim is to resolve digital verification and identification [6].

Biometric technologies work as a password but provide the user with improved peace of mind and security. The technique employs human features like voice or speaker recognition, facial recognition, or fingerprint recognition, to find the user. Biometrics is utilized for replacing passwords as well as streamlining into present multi-factor authentication system [7]. Biometric multi-factor authentication is a powerful authentication system. With an appropriate biometric authentication in place, academic administrator no longer needs to worry about cybersecurity and identification problems. Streamlined biometric authentication into present security platform comes with more advantages [8]. With biometrics, education institution uses distinct biometric models to remotely verify the identity and guarantee security of teachers and students. Decreasing the digital risk included in online education could lead to better outcomes and adaption resistance while using online education platforms.

This study designs a novel search and rescue optimization with deep learning based learning authentication technique for cybersecurity in higher education institutions, named SRODL-LAC technique. The proposed SRODL-LAC technique designs a median filtering (MF) based preprocessing technology for optimizing the quality of the image. In addition, the Densely Connected Networks (DenseNet-77) model is applied for the extraction of features. Moreover, search and rescue optimization (SRO) algorithm with deep neural network (DNN) model is utilized for the classification process. Lastly, template matching process is done for fingerprint identification. For ensuring the enhanced performance of the SRODL-LAC technique, a comprehensive simulation analysis is carried out and the results are inspected under several aspects.

The rest of the paper is organized as follows. Section 2 offers the related works, Section 3 discusses the proposed model, Section 4 validates the results, and Section 5 concludes the work.

## 2 Literature Review

Monaco et al. [9] respond to the institution's needs of higher learning undertakes great access control effort, by adapting identification technology as they become accessible, to guarantee that student of records is accessing the system and taking the exam online course. Statistics Performance on stylometry, keystroke, and integration of both methods were attained on information from thirty students taking examinations in university courses. Laamanen et al. [10] examine SEND student view regarding the usage of e-authentication system, including perceived advantages and disadvantages of new technique-enhanced assessment.

Guillén-Gámez et al. [11] focus on examining the perception of a group of students on the effect on the teaching-learning method of biometric authentication system named Smowl. To satisfy these objectives, researchers developed quasi-experiment research with 2 groups of fifty students, one utilizing Smowl technique and the other not. The result shows a comparison of the perception of these two groups, and find out that student who has utilized this method is highly favourable towards these tools.

Goyal et al. [12] introduced an approach based on incorporation of signature of a person, face recognition, and voice authentication technique to identify in e-learning scheme. The aforementioned methods are extensively utilized for authenticating identity of the individual. The major concerns are to demotivate unknown users from taking the examinations on behalf of the learners. To prevent the fraudulent management of e-learning systems, the verification-based voice recognition method has been deliberated as an effective method in the study.

Kamaraj et al. [13] verify the identity of learners by extracting the prosodic feature of the speech signals. TIMIT Acoustic-Phonetic Continuous Speech Corpus is utilized for the authentication of learners via articulation and prosodic characteristics namely formants, energy, and pitch. The articulation features include formants (F1-F7), and prosodic features include pitch (F0). From this dataset, during the testing process, 160 learners have been utilized and in the training process, two hundred learners have been utilized. The formants and pitch have been extracted by linear prediction analysis. The first 7 formants have been utilized for authentication purposes. The feature set comprises 8 features and that are fed to the Guassian mixture method. In the Gaussian mixture method, parameter is evaluated from the testing and training data through the iterative expectation-maximization. Log probability scores are calculated by this parameter, later this score is normalized to make decision.

AV et al. [14] presented the use of Keystroke dynamics-based authentication (KDA) as a solution to the verification of users in online examination and present a comprehensive study on the process of KDA, the factor that affects the efficiency of KDA, the application in distinct fields, as well as some keystroke dynamics-based data sets for authenticating the user at the time of online examination.

## 3 The Proposed Model

In this study, an effective SRODL-LAC technique has been developed for biometric authentication in HEIs. The proposed SRODL-LAC technique incorporates several stages of operations such as MF based preprocessing, DenseNet-77 based feature extraction, DNN based classification, SRO based hyperparameter tuning. The design of SRO algorithm aids in appropriately choosing the hyperparameter values of the DenseNet-77 module. Fig. 1 illustrates the overall procedure of SRODL-LAC technique.

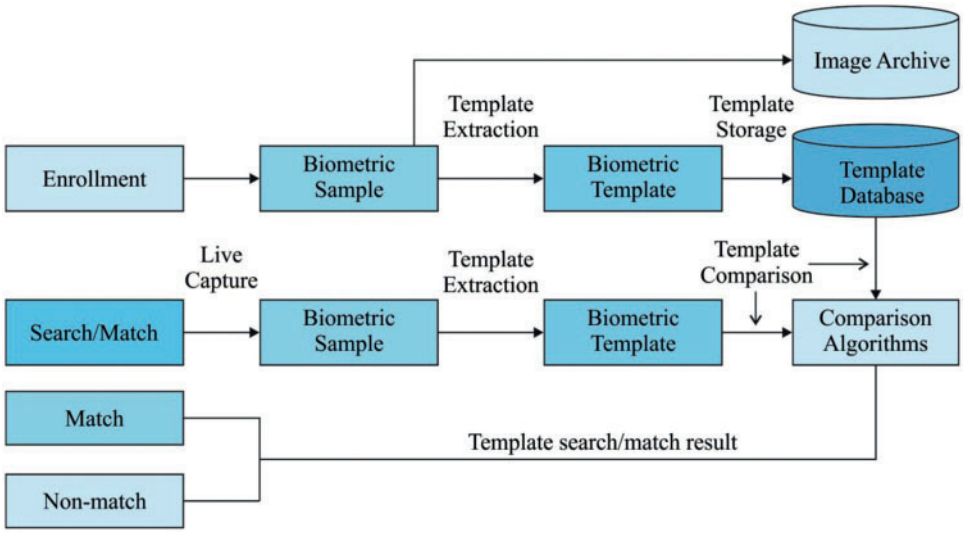


**Figure 1:** Overall process of SRODL-LAC technique

### *3.1 Pre-processing*

MF because of its specificity has the maximum application in healthcare image noise removal [15]. The key concept behindhand median filtering is to provide an $m \times n$ neighborhood for assembling each neighborhood in the ascending order, choose the median values of the ordered number, and replace the central pixel. It can be formulated by Eq. (1):

$$y_{(m,n)} = median\{x_{(i,j)},\ (i,\ j) \in C\}, \tag{1}$$

In which $C$ denotes the centered neighborhood around position $(m,\ n)$ of the image.

### *3.2 DenseNet Based Feature Extraction*

In this method, we employed DenseNet-77 at the feature extraction of the CBIR technique. Using DenseNet-77 for feature calculation exhibit improvements in computational complexity and segmentation accuracy. The initial layer computes lower-level key points from the image, viz., corner, and edge data, and the deep layer calculates higher-level key points, viz., chrominance, and structure data. The extracted feature maps are improved by the FPN that calculate the key point using enhanced object representations at different scales for the RPN model. DenseNet [16] method is an improved or advanced version of Resnet, in which the present layer belongs to each layer. DenseNet comprises the set of dense blocks that are successively connected to one another through the additional pooling and convolutional layers amongst successive dense blocks. DenseNet presents the complex transformation that leads to enhancing the problem of the absence of the target position data for the top-level key point to certain extent. DenseNet decreases the overall parameters that make it cost-effective. Moreover, it assists in calculating the key point and encourages them to recycle which makes them applicable for regional classification in retinal images. Therefore, we used the DenseNet-77 as a feature extractor for Mask-RCNN. Also, it indicates the query sampled size must be accommodated beforehand calculating key points from the paid layer [17]. The DenseNet-77 has two possible differences from conventional DenseNet: (i) it has a small amount of parameters when compared to the actual method and (ii) the layer inside each dense block is altered for overcoming the computation difficulty.

### *3.3 Optimal DNN Based Authentication*

The feature vectors derived from the DenseNet model are passed into the DNN model for the authentication process. DNN is an extended version of Multilayer Perceptron (MLP), which comes under the kind of Feed Forward Neural Networks (FFNN) with many layers comprising of input, output, and hidden layers. Every individual layer includes some neurons and is linked to the neurons in the forward course. It can be represented as follows: as $O : \mathbb{R}^m \times \mathbb{R}^n$. The input vector $x = x_1, x_2, x_3, \ldots, x_m$ with the size of is, '$m$' and the output vector is $O(x)$ with the size of '$n$'. The processing ability of every individual hidden layer $h_j$ can be represented by

$$h_j(x_j^{l+1}) = f(Z_{ij} + b_j^{(l+1)}) \tag{2}$$

$$Z_{\text{ij}} = x_i^l w_{ij}^{(l,l+1)} \tag{3}$$

The neurons in the low end are linked to the neuron $j$. In Eqs. (8) and (9), $x_i^{(l)}$ indicates a neuron $i$ activation function at layer $l$ and $Z_{ij}$ indicates the involvement of neuron $i$ at layer $l$ to the activation of neuron $j$ at layer $l + 1$. The function $f$, $w_{ij}^{(l,l+1)}$ represent the weight and $b_j^{l+1}$ denotes bias of neuron $j$. It makes use of softmax function to classify the data. The multiple stacking of hidden layer MLP is known as DNN [18]. Fig. 2 showcases the infrastructure of DNN technique.

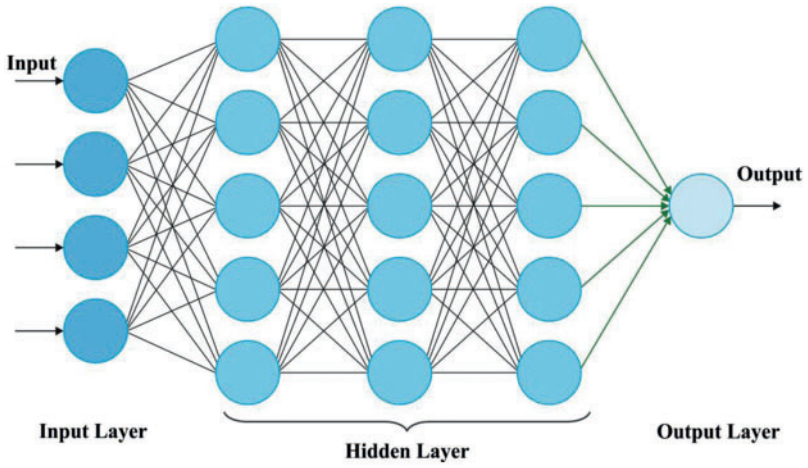


**Figure 2:** Structure of DNN model

The DNN model with several hidden layers can be defined using Eq. (4):

$$H_l(x) = H_l(H_{l-1}(H_{l-2}(\ldots(H_1(x))))) \tag{4}$$

The DNN model involves a set of two hidden layers. It receives the input as $x = x_1, x_2, x_3, \ldots, x_m$ and output will be $o = o_1, o_2, \ldots, o_{c-1}, o_c$. The DNN with every individual hidden layer holds ReLU, a nonlinear activation function. It assists in reducing the condition of gradient vanishing problems. The ReLU is quicker and simpler for training the models with several hidden states. The loss function can be represented as an optimum variable and it is needed to accomplish improved outcomes. The targeted and predicted value variances can be determined via the loss function, as given below.

$$d(t, p) = ||t - p||_2^2 \tag{5}$$

In which, $t$ and $p$ denote target and predicted values correspondingly. The loss function assists in identifying the forecasted values that vary from the targeted values. The target fed into the algorithm along with the features for calculating the loss function and classifying the attacks. The negative log likelihood with $t$ and likelihood distribution $p(pd)$ is employed for predicted and target classes correspondingly in multiclass classification. It can be expressed in the following equation as below:

$$d(t, p(p,\ d)) = -logp(pd)_t \tag{6}$$

For adjusting the hyperparameter values of the DenseNet model, the SRO algorithm is utilized. The SAR technique was presented by Shabani et al. [19] dependent upon process of detecting the lost people or people from distress. The SAR function consists of 2 phases that are social and individual stages. During the social stage, the search is dependent upon clues initiated by set, and the quality of present clues from defining novel regions in which optimum clue is initiated. During the individual stage, exploring was complete by individual members of set irrespective of the place of clues establish from others. This technique begins with arbitrary initialized of populations $N$ of dimensional $D$, whereas optimum $N/2$ place vector is chosen to human place matrix $U$ but rest procedure a memory matrix H. The clue matrix CL was generated by append $U$ and $H$ matrices as demonstrated in (7). The $H$, and CL matrices were upgraded to combined as social as well as individual stages. The effort of humans from social stage was explained in Eq. (8), where $k \neq i$ and $(j = 1,\ \ldots,\ D)$

$$CL = \begin{bmatrix} U_{1,1} & \cdots & U_{1,D} \\ \vdots & \ddots & \vdots \\ U_{N,1} & \cdots & U_{N,D} \\ H_{1,1} & \cdots & H_{1,D} \\ \vdots & \ddots & \vdots \\ H_{N,1} & \cdots & H_{N,D} \end{bmatrix} \tag{7}$$

$$U'_{i,j} = \begin{cases} \begin{cases} CL_{k,j} + r1 \times (U_{i,j} - CL_{k,j}),\ if\ f(CL_k) > f(U_i) \\ U_{k,j} + r1 \times (U_{i,j} - CL_{k,j})\ otherwise\ if\ r_2 < SE\ or\ j = j_{rand} \end{cases} \\ U_{i,j},\ otherwise \end{cases} \tag{8}$$

where $U'_{i,j}$ and $U_{i,j}$ represents the novel place and existing location to $j^{th}$ dimensional of $i^{th}$ human correspondingly. $CL_{k,j}$ refers the place to $j^{th}$ dimensional of $k^{th}$ establish clue. $f(U)$ and $f(CL)$ are FF values to $U_i$ and $CL_k$ correspondingly. $r1$ and r2 imply the uniform distribution number from the interval of $[-1, 1]$ and $[0, 1]$ correspondingly, in which $r1$ refers the similar to every dimensional and r2 signifies the varying to all dimensions. $j_{rand}$ defines the arbitrary number difference amongst 1 and $D$ that creates minimum one dimensional of $U'_{i,j}$ varying in $U_{i,j}$. The algorithmic parameters SE is named as social effect distinct in zero and one. It controls the effects of set members on each one from social stage [20]. During the individual stage, search was complete around its existing place by humans. The formula to effort of humans from the individual stage is written as:

$$U'_i = U_i + r3 \times (CL_k - CL_m),\ i \neq k \neq m \tag{9}$$

where $k$ and $m$ stand for the arbitrary numbers distinct amongst [1, N]. r3 denotes the uniformly distributed number from range of zero and one. In SAR technique, the boundary controls of novel

places of individuals are completed by the subsequent formula.

$$U'_{i,j} = \begin{cases} \text{-}if \dfrac{U_{i,j} + U_j^{\max} U_{i'_J}, + U_J^{\min} 2}{2}, if\, U_{i,j} < U_j^{\min}\, U'_{i,j} > U_j^{\max} \end{cases} \tag{10}$$

$$U'_{i,j} = \begin{cases} \dfrac{U_{i,j} + U_j^{\max}}{2},\ if\ U'_{i,j} > U_j^{max} \\ \dfrac{U_{i,j} + U_j^{\min}}{2}\ if\ U'_{i,j} < U_j^{min} \end{cases} \quad (j = 1,\ D) \tag{11}$$

where $U_j^{\min}$ and $U_j^{\max}$ are the minimal and maximal bounds to $j^{th}$ dimensional correspondingly. The memory matrix (H) and human place matrix (U) were obtaining upgrades then all phases from all iterations. Once the fitness value of novel place $f(U'_i)$ is superior to preceding one $f(U_i)$, next the preceding place $U_i$ is obtain saved from any arbitrary place of $H$ based on Eq. (12), but a novel place $U'_i$ is saved from $U$ utilizing in Eq. (13). Else, this novel place is rejected and memory upgrade is not occurring.

$$H_n = \begin{cases} U_i,\ if\ f(U'_i) < f(U_i) \\ H_n,\ otherwise \end{cases} \tag{12}$$

$$U_i = \begin{cases} U'_i,\ if\ f(U'_i) < f(U) \\ U_i,\ otherwise \end{cases} \tag{13}$$

In (12), $H_n$ implies the place of $n^{th}$ saved clues from the memory matrix and $n$ refer the arbitrary integer from the range of $(1,\ N/2)$. This memory upgrade procedure improves the ability of technique to define global optimal. Time factor is paramount significance from SAR functions, as delay from finding lost people it could be injured is outcome from its deaths. So, SAR function is complete in this manner which the huge feasible region is explored from shortest feasible time. Therefore, afterward, a particular amount of searches, when a human is not defined optimum clue around his/her existing place, afterward he/she leaves which place and is move to entirely novel place. This performance is modeled by written as represented in Eqs. (14) and (15). The algorithmic parameter $\mu$ is fixed as $70 \times D$.

$$FA_i = \begin{cases} FA_i + 1,\ if\ f(U'_i) > f(U) \\ 0,\ otherwise \end{cases} \tag{14}$$

$$U_{i,j} = U_j^{\min} + r4 \times (U_j^{\max} - U_j^{\min}),\ j = 1, \ldots D \tag{15}$$

where r4 implies the uniformly distributed arbitrary number lying from the range *zero* to one.

### *3.4 Template Matching Process*

Template matching can be performed by utilizing the DNN system [21]. The DNN utilizes Euclidean distance that is estimated as follows:

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \ldots + (x_n - y_n)^2}. \tag{16}$$

The DNN method allocates a class label to all the minutiae. Next, the k closest member is found by calculating the Euclidean distance among the minutiae. In this study, the value allocated for k is 2. Therefore, the process finds two nearest minutiae for all the minutia. Later, during matching, a local matching can be done to find out that minutiae in the query fingerprint match with the minutiae in the fingerprint template in the database. Next, a global matching can be performed for finding minutiae

of the query fingerprint matches with the minutiae of the template fingerprints. According to that, a matching score is created that provides an indication of either the fingerprints match with any of the fingerprints in the database.

## 4 Performance Validation

The performance validation of the SRODL-LAC technique takes place using different biometric fingerprint images. The results are inspected under five distinct runs of execution.

Fig. 3 illustrates the confusion matrices presented by the SRODL-LAC methodology on the biometric authentication process under five runs. The results indicated that the SRODL-LAC technique has accomplished effective authentication outcomes under every run. For instance, with run-1, the SRODL-LAC technique has categorized 105 instances into accept class and 11128 instances into reject class. Besides, with run-2, the SRODL-LAC approach has classified 106 instances into accepting class and 11126 instances into reject class. Moreover, with run-3, the SRODL-LAC method has categorized 104 instances into accept class and 11125 instances into reject class. Furthermore, with run-4, the SRODL-LAC algorithm has classified 104 instances into accepting class and 11128 instances into reject class. Eventually, with run-5, the SRODL-LAC system has considered 104 instances into accepting class and 11125 instances into reject class.

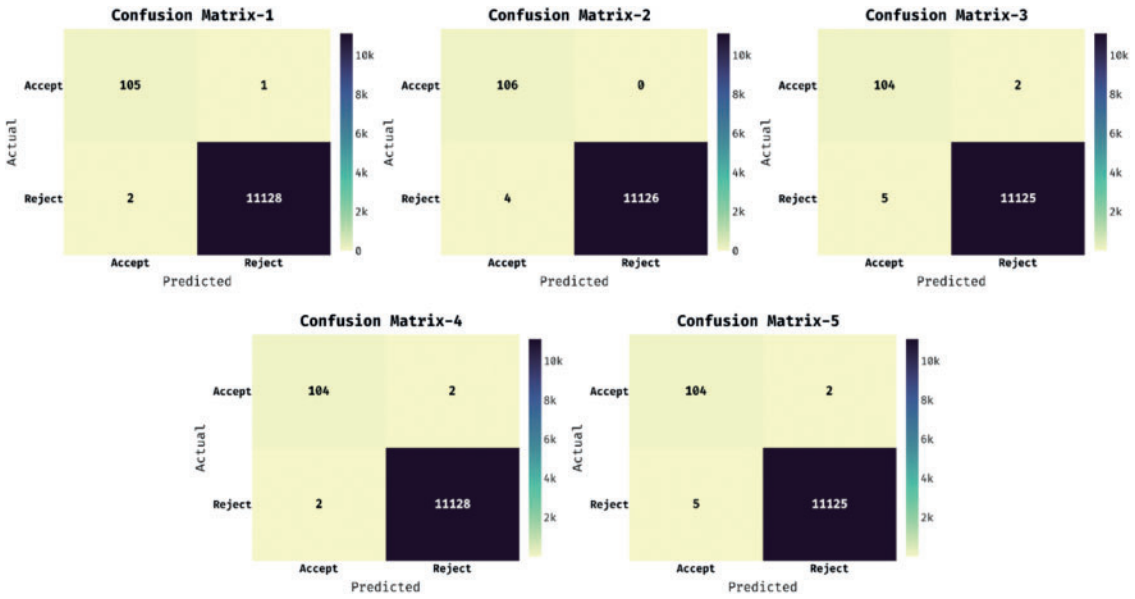


**Figure 3:** Confusion matrix of SRODL-LAC technique

Tab. 1 and Fig. 4 illustrate the result analysis of the SRODL-LAC technique on the applied test runs. The results show that the SRODL-LAC technique has resulted in increased values of accuracy. At the same time, the SRODL-LAC technique has demonstrated reduced values of FAR, FRR, EER<, and CT. For instance, with run-1, the SRODL-LAC technique has provided FAR, FRR, accuracy, EER, and CT of 0.0002, 0.0094, 0.9997, 0.0003, and 59 s respectively. Along with that, with run-2, the SRODL-LAC system has offered FAR, FRR, accuracy, EER, and CT of 0.0004, 0.0000, 0.9996, 0.0004, and 61 s correspondingly. Likewise, with run-3, the SRODL-LAC approach has provided FAR, FRR, accuracy, EER, and CT of 0.0004, 0.0189, 0.9994, 0.0006, and 58 s respectively.

Similarly, with run-4, the SRODL-LAC methodology has provided FAR, FRR, accuracy, EER, and CT of 0.0002, 0.0189, 0.9996, 0.0004, and 60 s correspondingly. At last, with run-5, the SRODL-LAC algorithm has offered FAR, FRR, accuracy, EER, and CT of 0.0004, 0.0189, 0.9994, 0.0006, and 59 s correspondingly.

**Table 1:** Result analysis of proposed srodl-lac technique on different runs

| No. of runs | FAR | FRR | Accuracy | EER | CT (s) |
|---|---|---|---|---|---|
| Run-1 | 0.0002 | 0.0094 | 0.9997 | 0.0003 | 59.0 |
| Run-2 | 0.0004 | 0.0000 | 0.9996 | 0.0004 | 61.0 |
| Run-3 | 0.0004 | 0.0189 | 0.9994 | 0.0006 | 58.0 |
| Run-4 | 0.0002 | 0.0189 | 0.9996 | 0.0004 | 60.0 |
| Run-5 | 0.0004 | 0.0189 | 0.9994 | 0.0006 | 59.0 |
| Average | 0.0003 | 0.0132 | 0.9995 | 0.0005 | 59.4 |

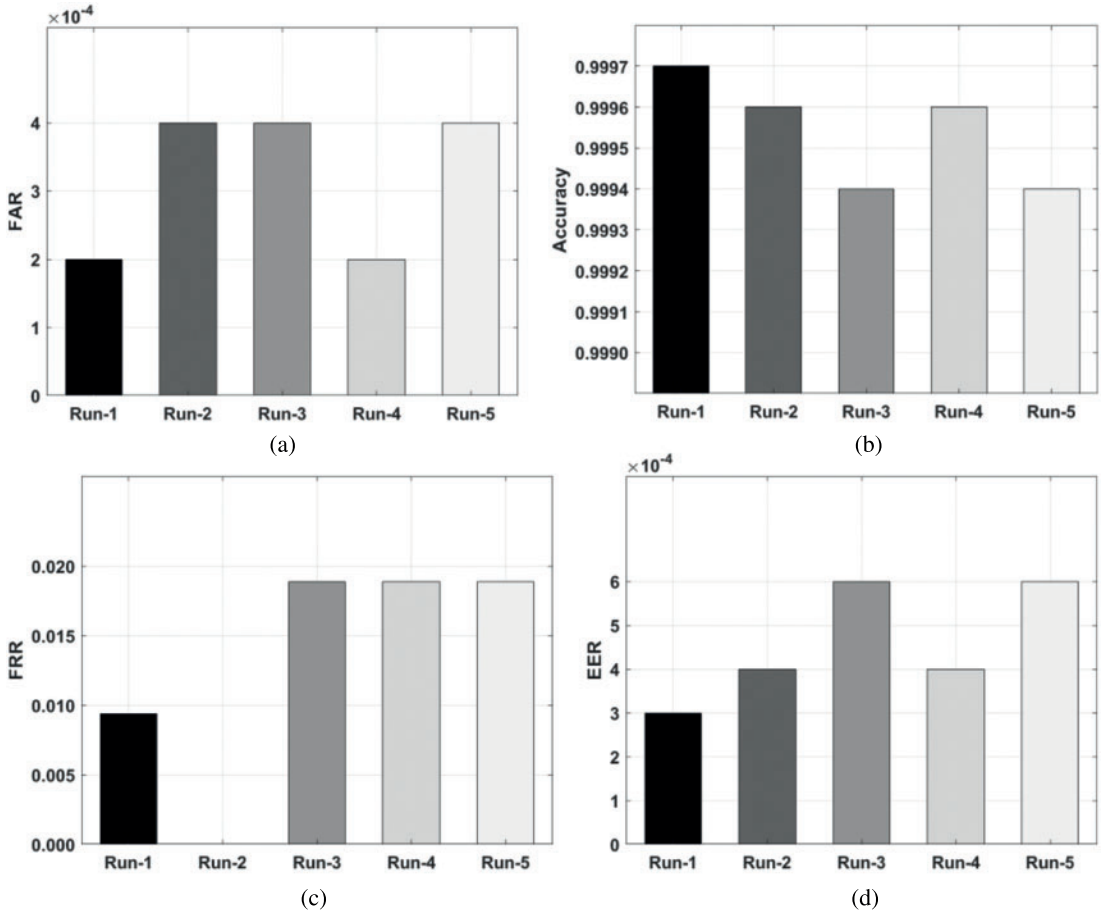


**Figure 4:** Result analysis of SRODL-LAC technique with distinct runs. (a) FAR, (b) Accuracy, (c) FRR, and (d) EER

Comparative result analysis of the SRODL-LAC approach with current DL models takes place in Tab. 2 and Fig. 5. The results show that the VGG-16 and CNN methodologies have obtained ineffective performance over the other methods. At the same time, the FCN-CRF technique has attained slightly increased performance. In line with, the LSTM and ResNet-152 models have resulted in moderately improved outcomes over the other methods except DenseNet-161 model. Though the DenseNet-161 model has showcased reasonable performance with the accuracy, EER, and CT of 98.83%, 1.17%, and 131 s, the presented SRODL-LAC technique has accomplished superior results with the accuracy, EER and CT of 99.95%, 0.05%, and 59 s respectively.

**Table 2:** Result analysis of proposed SRODL-LAC technique with existing methods

| Methods | Accuracy | EER | CT (s) |
|---|---|---|---|
| SRODL-LAC | 99.95 | 0.05 | 59 |
| LSTM | 97.87 | 2.13 | 089 |
| CNN | 95.22 | 4.78 | 092 |
| FCN-CRF | 96.13 | 3.87 | 098 |
| ResNet-152 | 97.71 | 2.29 | 102 |
| DenseNet-161 | 98.83 | 1.17 | 131 |
| VGG-16 | 95.43 | 4.57 | 127 |

Tab. 3 illustrates the comparative analysis of SRODL-LAC methodology with ML approaches interms of various measures [22]. Fig. 6 showcases the sensitivity and specificity analysis of the proposed SRODL-LAC approach with ML models. From the figure, it can be clear that the DT method has accomplished minimum outcome with the sensitivity and specificity of 92.83% and 88.24%. Also, the SVM system has gained somewhat higher outcomes with the sensitivity and specificity of 93.90% and 98.89%. Besides, the RF technique has resulted in moderately increased performance with the sensitivity and specificity of 94.54% and 92.67%. But, the KNN system has reached reasonable outcomes with the sensitivity and specificity of 95.65% and 94.54%, the projected SRODL-LAC technique has depicted the other methods with the maximal sensitivity and specificity of 98.68% and 99.97%.

Fig. 7 illustrates the accuracy analysis of the proposed SRODL-LAC technique with ML models. From the figure, it is apparent that the DT process has accomplished least outcome with an accuracy of 89.65%. At the same time, the KNN model has gained somewhat improved results with an accuracy of 92.37%. Along with that, the RF model has resulted in moderately increased performance with an accuracy of 95.47%. Though the SVM model has reached effective outcomes with an accuracy of 97.86%, the presented SRODL-LAC technique has outperformed the other techniques with the maximum accuracy of 99.95%.

Fig. 8 exhibits the F-score and precision analysis of the presented SRODL-LAC system with ML techniques. From the figure, it is obvious that the DT approach has accomplished least outcome with the precision and F-score of 84% and 90.47%. Simultaneously, the RF model has gained somewhat increased outcomes with the precision and F-score of 92.95% and 87.95%. Likewise, the SVM methodology has resulted in moderately superior performance with the precision and F-score of 94.71% and 97.76%. Followed by, the KNN method has reached reasonable outcome with the precision

and F-score of 96.90% and 95.09%, the presented SRODL-LAC methodology has demonstrated the other techniques with the higher F-score and precision of97.67% and 96.68%.

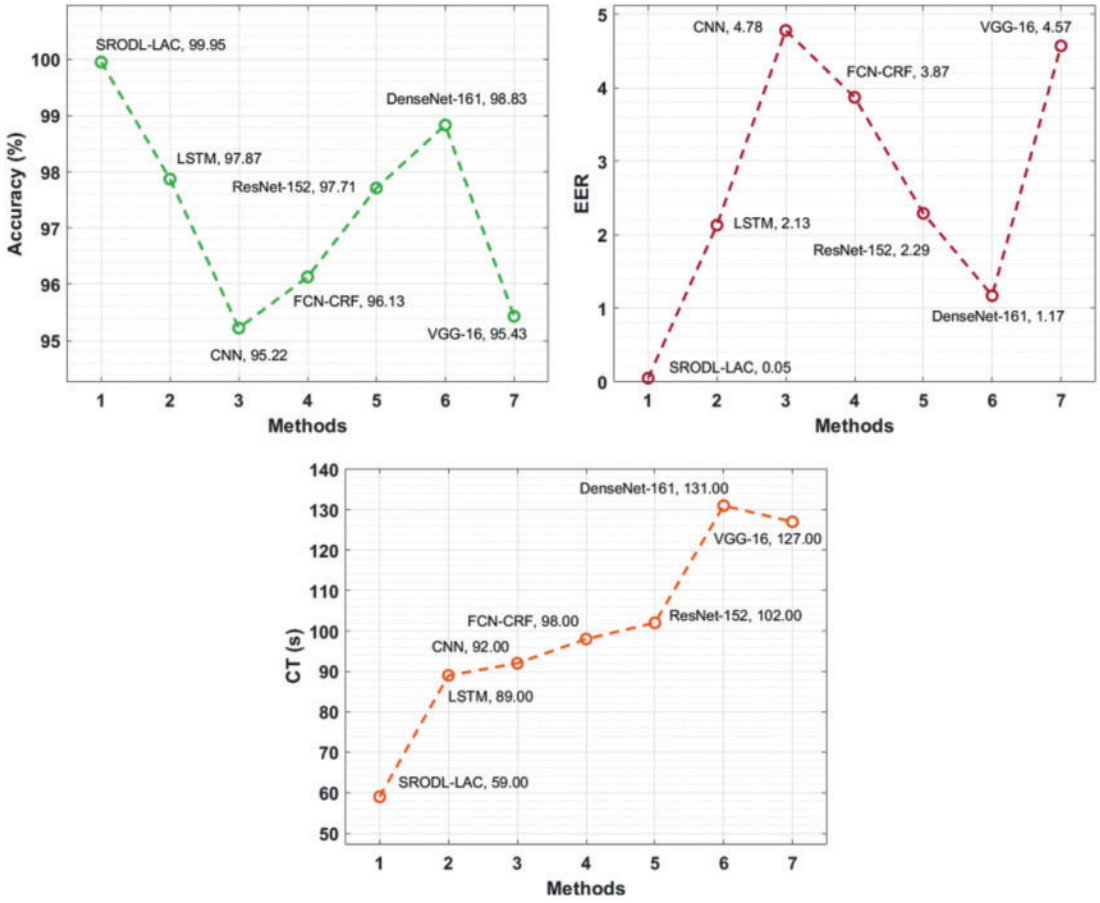


**Figure 5:** Comparative analysis of SRODL-LAC technique

**Table 3:** Comparative analysis of SRODL-LAC technique with existing methods

| Methods | Sensitivity | Specificity | Accuracy | Precision | F-score |
|---|---|---|---|---|---|
| SRODL-LAC | 98.68 | 99.97 | 99.95 | 96.68 | 97.67 |
| KNN | 95.65 | 94.54 | 92.37 | 96.90 | 95.09 |
| DT | 92.83 | 88.24 | 89.65 | 84.00 | 90.47 |
| SVM | 93.90 | 98.89 | 97.86 | 94.71 | 97.76 |
| RF | 94.54 | 92.67 | 95.47 | 92.95 | 87.95 |

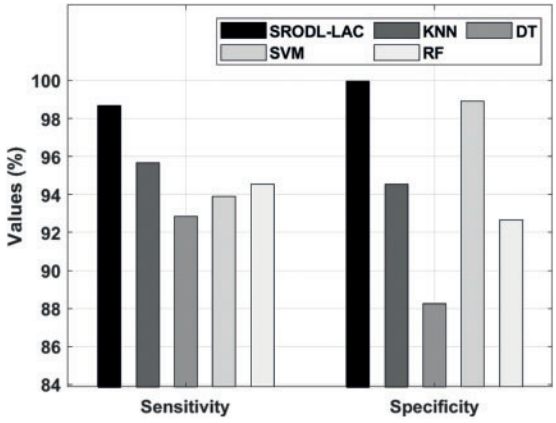


**Figure 6:** Sensitivity and specificity analysis of SRODL-LAC technique

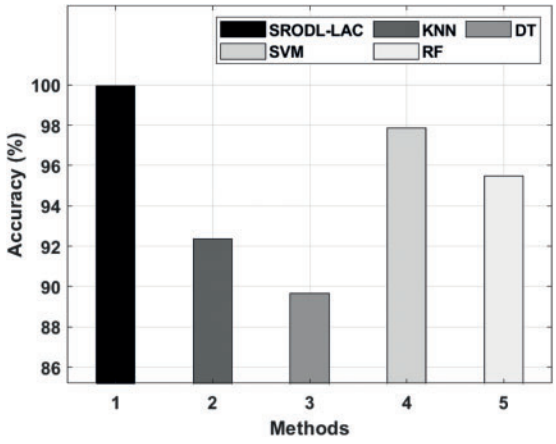


**Figure 7:** Accuracy analysis of SRODL-LAC technique

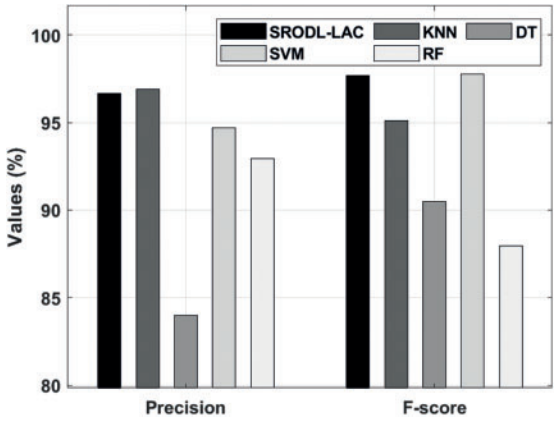


**Figure 8:** Precision and F-score analysis of SRODL-LAC technique

## 5 Conclusion

In this study, an SRODL-LAC technique has been developed for biometric authentication in HEIs. The proposed SRODL-LAC technique incorporates several stages of operations such as MF based preprocessing, DenseNet-77 based feature extraction, DNN based classification, SRO based hyperparameter tuning. The design of SRO methodology aids in appropriately choosing the hyperparameter values of the DenseNet-77 model. For ensuring the enhanced performance of the SRODL-LAC technique, a comprehensive simulation analysis is carried out and the results are inspected under several aspects. The experimental results reported the outstanding performance of the SRODL-LAC technique over the other techniques. Therefore, the SRODL-LAC technique can be applied as an effective approach for biometric authentication in HEIs. In future, the authentication performance can be improved by using fusion based DL models.

**Acknowledgement:** The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number (IFPRC-154-611-2020) and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

**Funding Statement:** This project was supported financially by Institution Fund projects under grant no. (IFPRC-154-611-2020).

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Lati *et al.,* "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[2] D. Chen, P. Wawrzynski and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustainable Cities and Society*, vol. 66, pp. 102655, 2021.

[3] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li *et al.,* "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[4] H. HaddadPajouh, A. Dehghantanha, R. Khayami and K. K. R. Choo, "A deep recurrent neural network based approach for internet of things malware threat hunting," *Future Generation Computer Systems*, vol. 85, pp. 88–96, 2018.

[5] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan and K. K. R. Choo, "A Privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5110–5118, 2020.

[6] J. Chandramohan, R. Nagarajan, M. A. kumar, T. Dineshkumar, G. Kannan *et al.,* "Attendance monitoring system of students based on biometric and gps tracking system," *International Journal of Advanced Engineering, Management and Science*, vol. 3, no. 3, pp. 241–246, 2017.

[7] M. B. Srinidhi and R. Roy, "A web enabled secured system for attendance monitoring and real time location tracking using biometric and radio frequency identification (RFID) technology," in *2015 Int. Conf. on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, pp. 1–5, 2015.

[8] I. Bandara, F. Ioras and M. P. Arraiza, "The emerging trend of blockchain for validating degree apprenticeship certification in cybersecurity education," in *INTED2018 Proc.: 12th Int. Technology, Education and Development Conf.*, Valencia, Spain, pp. 7677–7683, 2018.

[9] J. V. Monaco, J. C. Stewart, S. H., Cha and C. C. Tappert, "Behavioral biometric "verification of student identity in online course assessment and authentication of authors in literary works," in *2013 IEEE Sixth Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, Arlington, VA, USA, pp. 1–8, 2013.

[10] M. Laamanen, T. Ladonlahti, S. Uotinen, A. Okada, D. Bañeres *et al.,* "Acceptability of the e-authentication in higher education studies: Views of students with special educational needs and disabilities," *International Journal of Educational Technology in Higher Education*, vol. 18, no. 1, pp. 4, 2021.
[11] F. D. G. Gámez, I. G. Magariño and S. J. Romero, "Analysis of the perception of students about biometric identification," *International Journal of Web-Based Learning and Teaching Technologies*, vol. 10, no. 3, pp. 1–18, 2015.
[12] M. Goyal and R. Krishnamurthi, "An enhanced integration of voice-, face-, and signature-based authentication system for learning content management system," in *Biometric Authentication in Online Learning Environments*, IGI Global, pp. 70–96, 2019. https://doi.org/10.4018/978-1-5225-7724-9.ch004.
[13] A. Kamaraj, S. Nidhyananthan and K. Sundaram, "Voice biometric for learner authentication: Biometric authentication," in *Biometric Authentication in Online Learning Environments*, IGI Global, pp. 150–181, 2019. https://doi.org/10.4018/978-1-5225-7724-9.ch007.
[14] S. K. AV and M. Rathi, "Keystroke dynamics: A behavioral biometric model for user authentication in online exams," In *Research Anthology on Developing Effective Online Learning Courses*, IGI Global, pp. 1137–1161, 2021. https://doi.org/10.4018/978-1-7998-8047-9.ch056.
[15] Z. Gao, "An adaptive median filtering of salt and pepper noise based on local pixel distribution," in *The Proc. of the 2018 Int. Conf. on Transportation & Logistics, Information & Communication, Smart City (TLICSC 2018)*, Chengdu City, China, pp. 473–483, 2018.
[16] Y. Wang, H. Li, P. Jia, G. Zhang, T. Wang *et al.,* "Multi-scale densenets-based aircraft detection from remote sensing images," *Sensors*, vol. 19, no. 23, pp. 5270, 2019.
[17] T. Nazir, A. Irtaza and V. Starovoitov, "Optic disc and optic cup segmentation for glaucoma detection from blur retinal images using improved mask-RCNN," *International Journal of Optics*, vol. 2021, pp. 1–12, 2021.
[18] K. N. Rao, K. V. Rao and P. V. G. D. P. Reddy, "A hybrid intrusion detection system based on sparse autoencoder and deep neural network," *Computer Communications*, vol. 180, pp. 77–88, 2021.
[19] A. Shabani, B. Asgarian, S. A. Gharebaghi, M. A. Salido and A. Giret, "A new optimization algorithm based on search and rescue operations," *Mathematical Problems in Engineering*, vol. 2019, pp. 1–23, 2019.
[20] S. Priyadarshani, K. R. Subhashini and J. K. Satapathy, "Maiden application of search and rescue optimization algorithm for automatic generation control of interconnected power system," in *2020 IEEE Int. Conf. on Electronics, Computing and Communication Technologies (CONECCT)*, Bangalore, India, pp. 1–6, 2020.
[21] V. M. Praseetha, S. Bayezeed and S. Vadivel, "Secure fingerprint authentication using deep learning and minutiae verification," *Journal of Intelligent Systems*, vol. 29, no. 1, pp. 1379–1387, 2019.
[22] J. M. Song, W. Kim and K. R. Park, "Finger-vein recognition based on deep densenet using composite image," *IEEE Access*, vol. 7, pp. 66845–66863, 2019.