Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.025672
Article

Tech Science Press

Implicit Continuous User Authentication for Mobile Devices based on Deep Reinforcement Learning

Christy James Jose[1,*] **and M. S. Rajasree**[2]

[1]Government Engineering College, Idukki, 685603, India
[2]APJ Abdul Kalam Technological University, Thiruvananthapuram, 695016, India
*Corresponding Author: Christy James Jose. Email: christy@gecidukki.ac.in
Received: 01 December 2021; Accepted: 21 February 2022

Abstract: The predominant method for smart phone accessing is confined to methods directing the authentication by means of Point-of-Entry that heavily depend on physiological biometrics like, fingerprint or face. Implicit continuous authentication initiating to be loftier to conventional authentication mechanisms by continuously confirming users' identities on continuing basis and mark the instant at which an illegitimate hacker grasps dominance of the session. However, divergent issues remain unaddressed. This research aims to investigate the power of Deep Reinforcement Learning technique to implicit continuous authentication for mobile devices using a method called, Gaussian Weighted Cauchy Kriging-based Continuous Czekanowski's (GWCK-CC). First, a Gaussian Weighted Non-local Mean Filter Preprocessing model is applied for reducing the noise present in the raw input face images. Cauchy Kriging Regression function is employed to reduce the dimensionality. Finally, Continuous Czekanowski's Classification is utilized for proficient classification between the genuine user and attacker. By this way, the proposed GWCK-CC method achieves accurate authentication with minimum error rate and time. Experimental assessment of the proposed GWCK-CC method and existing methods are carried out with different factors by using UMDAA-02 Face Dataset. The results confirm that the proposed GWCK-CC method enhances authentication accuracy, by 9%, reduces the authentication time, and error rate by 44%, and 43% as compared to the existing methods.

Keywords: Deep reinforcement learning; gaussian weighted; non-local; mean filter; cauchy kriging regression; continuous czekanowski's; implicit continuous authentication; mobile devices

1 Introduction

The use of passwords and keys permits users in accessing the personal information by means of safeguarding against unauthorized attempts. However, research studies conducted on this domain have shown that users frequently select passwords that are easy to remember or combination of weak passwords to safeguard their data, despite passwords being easy to predict. Moreover, with the swift evolutions in mobile devices stimulate the users to utilize these devices in regular monitoring and storing the delicate health data. So, to bridge the gap between authentication and usability, there has been a transformation towards biometric authentication models employing certain biological features, like, fingerprints and face, behavioral features like keystroke, swipe patterns and so on. In addition, implicit continuous authentication, specifically on mobile devices, is gaining more awareness in recent years. As against user authentication performed only at the entry point when the device is locked, authentication methods regulate whether biometric traits correspond to a user in a continuous manner. In this manner, users can monitor in a continuous manner and hence do not require to persistently perturb concerning security and privacy despite devices are lost.

A novel gait-based continuous authentication method applying multimodal learning called, GaitCode [1] on cooperatively recorded accelerometer and ground contact force data from smart wearable devices was proposed in [1]. Despite improvement observed in error rate and false acceptance rate, the authentication accuracy, time and error rate involved in the overall implicit continuous authentication process was not focused. To address this issue in this work, by applying filter function for temporal data as preprocessing results in continuous denoised images, therefore improving the authentication time and accuracy. Also, Cauchy distribution function is used to reduce the error rate by scaling the different face images for validation.

An Extremal Openset Rejection (EOR), comprising of a two-fold mechanism involving identification and a verification step distinctly based on sparse representation was proposed in [2]. Despite improvement found in verification accuracy, the sensitivity and specificity involved in continuous monitoring was not focused. To address this issue in this work, Continuous Czekanowski's Classification performed with the aid of continuous function ensures improved sensitivity and specificity.

1.1 Objective

- To develop a novel GWCK-CC method to guarantee implicit continuous authentication for mobile devices.
- Eradication of noise to achieve denoising of images using Gaussian Weighted Non-local Mean Filter Preprocessing model.
- Extraction of the important features with minimization in dimensionality, utilizing Cauchy Kriging Regression Feature Extraction model.
- To enhance the classification accuracy among normal users and hackers with lesser time, employing Continuous Czekanowski's Classification.

1.2 Organization of Paper

The structure of the paper is organized as follows. Related work is provided in Section 2. In Section 3, the design of the proposed method, Gaussian Weighted Cauchy Kriging-based Continuous Czekanowski's (GWCK-CC) implicit continuous authentication on mobile devices along with the algorithm is presented. Evaluation of the algorithms with the detailed experimental setup is provided in Section 4. In 5 detailed discussions is given with the aid of table and graph. Finally, the concluding remarks are provided in Section 6.

2 Related Works

In today's world with the advancement in technology, the modern smart phone has become a vital part of every person's life. Security concerns have thus elevated with the increasing utilization of smart phone owing to the huge availability and accessibility of personal files, and banking and business information. Also, continuous authentication is not an easy task and several research works has been conducted in this area.

2.1 Biometric-based Authentication

Biometric solution employing feature fusion approach integrating both handcrafted and non-handcrafted features was proposed in [3]. But, it failed to improve the performance by using UBIPr, Color FERET and Ethnic Ocular databases. A behavior-based authentication using swipe was utilized in [4] with the objective of authenticating the user in a continuous manner. On the other hand, activity patterns were employed in [5] using random forest, support vector and Bayes for analyzing continuous authentication of smart phone users.

More than 140 papers pertaining to recent behavioral continuous authentication methods were investigated in [6]. In [7], an in depth analysis of whether continuous authentication is possible or not for mobile banking application was investigated. However, the reliability and practicability was not focused. Also, larger dataset was not considered. To address on this aspect, one class SVM was designed in [8] for ensuring context aware implicit authentication.

2.2 Continuous Authentication on Mobile Devices

A hierarchical implicit authentication mechanism using binary support vector machine with radial basis function for ensuring accuracy was proposed in [9]. In [10], an intelligent add-on for smart phones to validate continuous authentication of users was proposed. Data augmentation method called, Kernel Ridge Regression with Truncated Gaussian Radial Basis Function was designed in [11]. But, the time was reduced by using small dataset.

In [12] a novel biosignal authentication mechanism ensuring continuous, seamless, and secure user authentication was provided by means of coupling. Yet another continuous authentication using blockchain for IoT environment called, CAB-IoT was proposed in [13]. However, the accuracy aspect was not focused with AT&T Database of faces. To address this issue, a periodical authentication mechanism employing Deep Auto Encoder and Softmax Regression (DAE-SR) for ensuring accuracy was proposed in [14].

2.3 Continuous User Authentication Progress and Challenges

A review of non-intrusive active user authentication using biometrics to investigate the merits and demerits of authentication system was investigated in [15]. An overview of numerous continuous authentication systems on mobile devices was analyzed in [16]. Sensitive information was retained in mobile devices and to ensure privacy and security deep-learning based authentication system via user pattern was proposed in [17]. With this the false acceptance rate were said to be minimized drastically.

Yet another patch-based CNN model via user-disjoint and cross-factor protocols was designed in [18] for detecting face's representation in a continuous fashion to consider RECOD-MPAD and OULU-NPU dataset. A survey of numerous types and methods of authentication to specifically secure the smart phone access was proposed in [19]. Machine Learning techniques were introduced in [20] to preserve cyberspace attacks. Dissimilar machine learning (ML) techniques were developed in [21] to minimize the time complexity. Continuous authentication systems were developed in [22] for enhancing the security and privacy. A novel technique termed implicit imitation was introduced in [23] to accelerate reinforcement learning. Machine learning techniques were designed in [24] for identifying the several cyber threats. Reinforcement learning was investigated in [25] by using continuous control applications.

Based on the aforementioned materials and methods, in this work, Gaussian Weighted Cauchy Kriging-based Continuous Czekanowski's (GWCK-CC) for implicit continuous authentication on mobile devices is proposed. The detailed description of the proposed GWCK-CC method is presented in the following sections.

3 Methodology

Conventional authentication method authenticates the validity of an entity or system analytically at the inception of the communication session and determines either it is authenticated or not. Hence, they are said to be susceptible to security menaces that take dominance of the active sessions involved. Hence, there necessitates an intense requirement to handle this issue continuously authenticating the identity of users in the course of the whole session. Fig. 1 given below shows the block diagram of Gaussian Weighted Cauchy Kriging-based Continuous Czekanowski's (GWCK-CC) method towards implicit continuous authentication for mobile devices.

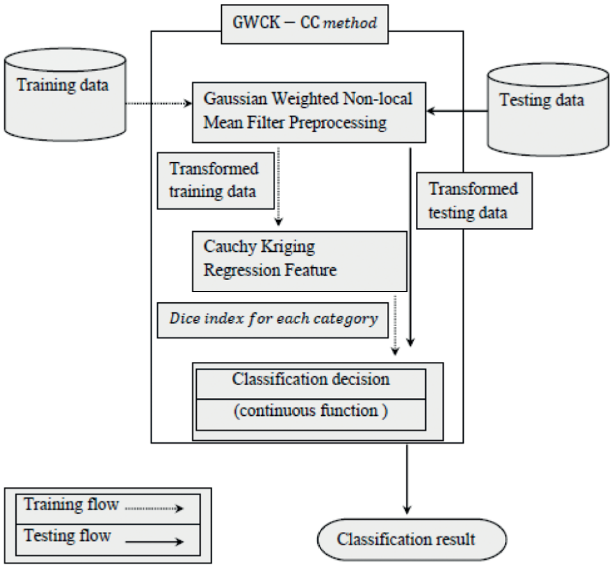

Figure 1: Block diagram of Gaussian Weighted Cauchy Kriging-based Continuous Czekanowski's (GWCK-CC)

In this work, GWCK-CC method is proposed to enhance the performance of implicit continuous user authentication. The proposed GWCK-CC method is split into three layers. They are input layer, three hidden layers and finally the output layer. First, face images acquired from UMDAA-02 Face Dataset [26] are provided as input to the input layer. Followed by which the input face images are transferred to the first hidden layer 'HL1'. Preprocessing of continuous faces images using Gaussian Weighted Non-local Mean Filter is employed that in turn improves the face quality image. After that, the preprocessed output or the denoised continuous images is given to the second hidden layer 'HL2' to perform feature extraction using Cauchy Kriging Regression. These continuous extracted feature results are sent to the third hidden layer 'HL3'. With the continuous extracted features, input face images are classified using Continuous Czekanowski's Dice Index. Finally, the classified output results are generated in the output layer. Fig. 2 shows the structure of GWCK-CC.

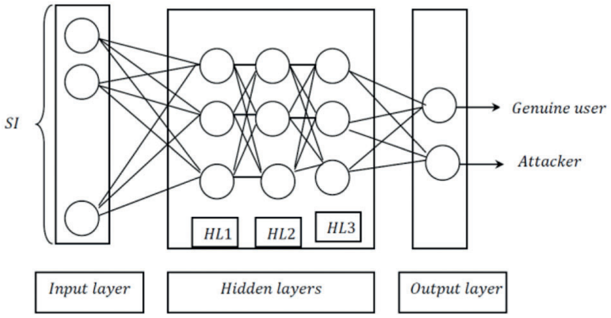

Figure 2: Structure of GWCK-CC

As shown in the above figure, the data collection module in the input layer acquires all users' sensor data from UMDAA-02 Face Dataset [26] via twelve distinct sensors for implicit continuous authentication. In the proposed GWCK-CC method, the data collection module in the input layer gets the user's each single minute gesture during operation on their smart phones, and records the swift and instant readings of the twelve sensors when the screen is on. In the data collection phase, the data collection module captures users' behavioral patterns with smart phone usage are constructed into smart phones by twelve sensors. The collected face data from mobile devices are stored in a secured buffer for data preprocessing.

3.1 Gaussian Weighted Non-local Mean Filter Preprocessing Model

Sensor data collected from smart phones necessitates preprocessing phase for feasible handling of noise and temporal calibration for series inception. The targeted sensory data consist readings of twelve distinct sensors, which are front facing camera 'FFC', touch screen 'TS', gyroscope 'G', accelerometer 'A', magnetometer 'M', light sensor 'LS', GPS 'GPS', Bluetooth 'B', WiFi 'WiFi', proximity sensor 'ProS', temperature sensor 'TempS' and pressure sensor 'PreS' respectively. Let us denote the collected data reading as '$P_i^{(t)} \in R^d$', refers to collected pixel data 'P' for user 'i' at time 't' for a total dimension '$d = 12$' (i.e., from 23 distinct sensors). The pixel data reading over a period of time is then represented by a vector as given below.

$$PV = \{P_{FFC}, P_{TS}, P_G, P_A, P_M, P_{LS}, P_{GPS}, P_B, P_{WiFi}, P_{ProS}, P_{TempS}, P_{PreS}\} \quad (1)$$

Next, with the acquired input images, preprocessing is performed in the first hidden layer by employing Gaussian Weighted Non-local Mean Filter model to improve the face quality images. The preprocessing model converts the collected time domain data for implicit continuous authentication into temporal stream of data that are used as inputs. Fig. 3 shows the structure of–Gaussian Weighted Non-local Mean Filter model.

As shown in the above figure, the basic principle of the Gaussian Weighted Non-local Mean Filter is to restore the noisy pixel gray-value data 'PD(i)' of pixel data 'i' with a weighted mean of the mean of pixel gray-values of all the pixels on the image. This is mathematically expressed as given below.

$$PD(i) = \sum_{j \in SWS} W_{ij} PD(j) \quad (2)$$

From the above Eq. (2), '$j \in SWS$' refers to the search window size (i.e., '$(2n + 1) * (2n + 1)$'), with weight of two pixels 'i' and 'j' denoted as 'W_{ij}'. The weight is mathematically expressed as given below.

$$W_{ij} = \frac{1}{Z_i}\left[-\frac{[V(N_i) - V(N_j)]^2}{\alpha^2} - \frac{[P(N_i) - P(N_j)]^2}{\beta^2}\right] \quad (3)$$

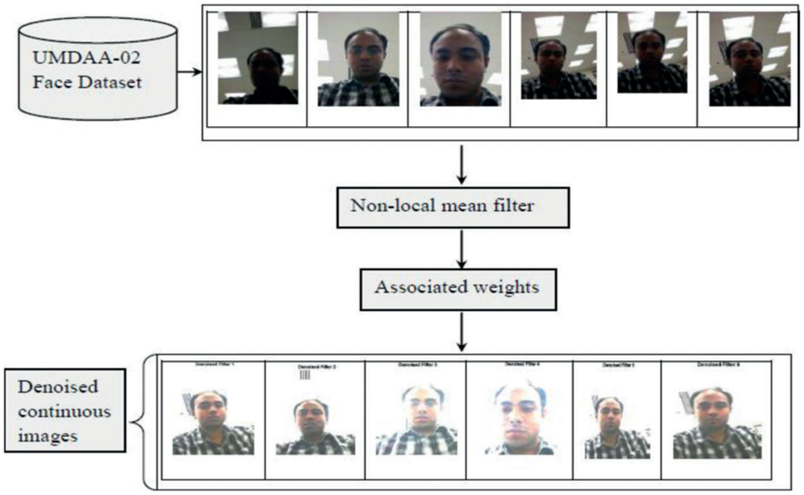

Figure 3: Structure of gaussian weighted non-local mean filter preprocessing

From the above Eq. (3), the weight function is represented as vector ‘V’ of pixel gray-value data from the neighborhood ‘N_i’ centered at ‘i’ with probability pixel gray-value data from the neighborhood ‘$P(N_i)$’ along with two filtering parameters ‘α’, ‘β’ with respect to normalizing term ‘Z_i’. The first filtering parameter ‘α’ determines the non-local means averaging weight, the value of which is chosen within ‘(0.75 to 1)’ for high visual quality. The second filtering parameter ‘β’ determines the level of and is assigned to be between ‘(50 to 100)’ that provides a fine-grained balance between background leveling and pixel enhancement in denoised images.

The first term ‘$\frac{[V(N_i)-V(N_j)]^2}{\alpha^2}$’ hence refers to the Euclidean distance of pixel gray-value data between two neighborhoods ‘N_i’ and ‘N_j’ within the searching window ‘SW’. In a similar manner, the second term refers to the Euclidean distance of pixel gray-value data probabilities between two same neighborhoods ‘N_i’ and ‘N_j’ acquired from the probability image. With this the preprocessed data is acquired that in turn improve the quality of face image for further processing.

3.2 Cauchy Kriging Regression Feature Extraction Model

In our work, feature extraction is performed with the purpose of dimensionality reduction. The preprocessed set of data is reduced to more manageable groups for further processing. With this, the new set of extracted features possesses distinct values upon comparison with the original preprocessed feature values. In our work, Cauchy Kriging Regression Feature Extraction is employed to extract the pertinent features for performing continuous authentication with lesser the error rate. Fig. 4 given below shows the structure of Cauchy Kriging Regression Feature Extraction model.

As shown in the above figure, let us consider the preprocessed sampling images or the denoised continuous images ‘$SI = SI_1, \ SI_2, \ \ldots, \ SI_n$’ as input for extracting the pertinent features. Then, the denoised continuous sampling images obtained at different time interval are mathematically formulated as given below.

$$SI_1 = \{a_{11}, a_{12}, a_{13}, \ldots, a_{1n}\}; \ SI_2 = \{a_{21}, a_{22}, a_{23}, \ldots, a_{2n}\}\ldots; \ SI_m = \{a_{m1}, a_{m2}, a_{m3}, \ldots, a_{mn}\} \quad (4)$$

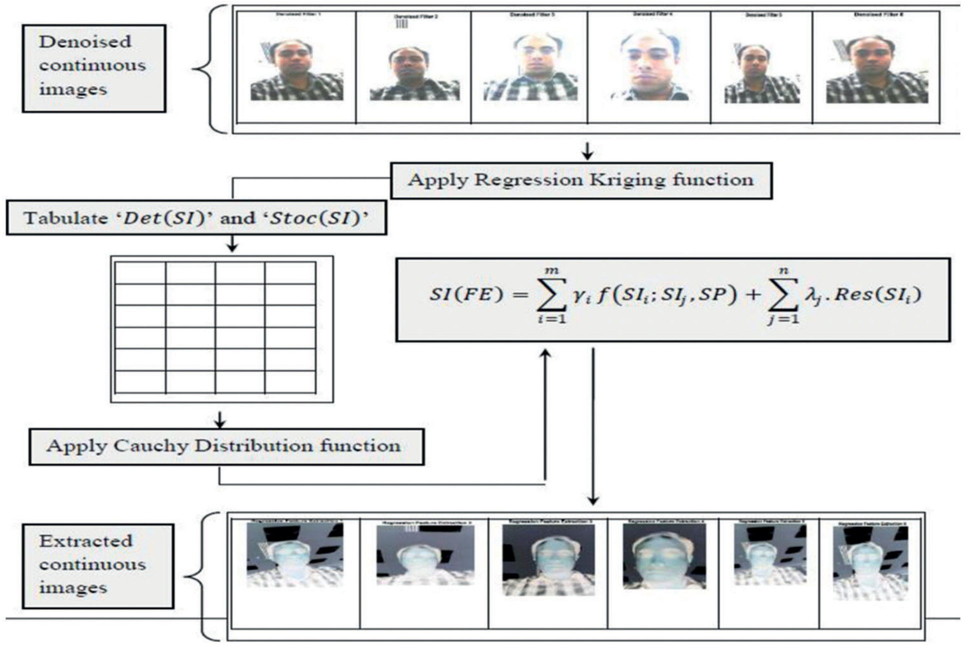
Denoised continuous images
Apply Regression Kriging function
Tabulate ‘Det(SI)’ and ‘Stoc(SI)’
$SI(FE) = \sum_{i=1}^{m} \gamma_i f(SI_i; SI_j, SP) + \sum_{j=1}^{n} \lambda_j . Res(SI_i)$
Apply Cauchy Distribution function
Extracted continuous images

Figure 4: Structure of cauchy kriging regression feature extraction

The above distinct preprocessed denoised continuous sample images as input for reducing the error rate. Regression Kriging ‘Z(SI)’ modeled as sum of deterministic sample image ‘Det(SI)’ and stochastic sample image ‘Stoc(SI)’ is formulated as given below.

$$Z(SI) = Det(SI) + Stoc(SI) \tag{5}$$

From the above Eq. (5), both deterministic and stochastic sample images are employed for regression owing to the reason that while performing continuous authentication, both inherent randomness and deterministic. Next, by combining the deterministic and stochastic sample images, the features to be extracted are formulated as given below.

$$SI(FE) = \sum_{i=1}^{m} \gamma_i f(SI_i;\ SI_j,\ SP) + \sum_{j=1}^{n} \lambda_j.Res(SI_i) \tag{6}$$

$$f(SI_i;\ SI_j,\ SP) = \frac{1}{\pi SP\left[1 + \left(\frac{SI_i - SI_j}{SP}\right)^2\right]} = \frac{1}{\pi(SP)}\left[\frac{SP^2}{(SI_i - SI_j) + SP^2}\right] \tag{7}$$

From the above Eqs. (6) and (7), the features to be extracted from the sampled preprocessed images ‘SI (FE)’ are obtained based on the deterministic coefficient ‘γ_i’, stochastic kriging weights ‘λ_j’, residual ‘Res’ at ‘SI_i’ and finally, Cauchy distribution function ‘$f(SI_i; SI_j, SP)$’ respectively. The Cauchy distribution function results are obtained according to the scaling parameters ‘SP’ with which the orientation of the sampled preprocessed images ‘SI_i’ and ‘SI_j’ are made. Finally, the corresponding response is mathematically formulated as given below.

$$P = SI(FE[b_1]) = \{b_1^{(1)},\ b_1^{(2)},\ b_1^{(3)},\ \ldots,\ b_1^{(n)}\};\ SI(FE[b_2]) = \{b_2^{(1)},\ b_2^{(2)},\ b_2^{(3)},\ \ldots,\ b_2^{(n)}\};\ \ldots;\ SI(FE[b_m]) = \{b_m^{(1)},\ b_m^{(2)},\ b_m^{(3)},\ \ldots,\ b_m^{(n)}\} \tag{8}$$

From the above Eq. (8), finally, the extracted features of face images at different time intervals or implicit continuous extracted image is obtained. With the corresponding continuous response as in 'SI(FE[b])', the error rate with which the classification can be made is improved. This is owing to the reason that by employing the Cauchy distribution function the scale parameter 'SP' obtains different orientation of the preprocessed sample images, contributing to minimum error rate.

3.3 Continuous Czekanowski's Classification Model

With the extracted continuous features, classification between genuine and attackers are made by means of Continuous Czekanowski's Classification model. Then, the Continuous Czekanowski's Classification for continuous face recognition is mathematically expressed as given below.

$$CCC = \frac{2|P\ \cap Q|}{R|P| + |Q|} \tag{9}$$

From the above Eq. (9), the Continuous Czekanowski's Classification 'CCC' results are arrived at based on the ground truth image 'Q' and the computed continuous extracted image 'P' respectively. In addition, 'R' defines the mean value of 'P' over the pixels where both 'P' and 'Q' are positive and mathematically formulated as given below.

$$R = \frac{\sum_i p_i q_i}{\sum_i p_i Sign(q_i)} \tag{10}$$

With the above classified results, face recognition is ensured therefore paving mechanisms for implicit continuous user authentication with maximum sensitivity and specificity. The pseudo code representation of Gaussian Weighted Cauchy Kriging Continuous Czekanowski's-based implicit continuous authentication is given below.

As given in the objective of Gaussian Weighted Cauchy Kriging Continuous Czekanowski's-based implicit continuous authentication algorithm is to ensure the accurate face recognition with minimum time and error rate. With this objective deep reinforcement learning is designed with one input layer, three hidden layers and one output layer. Raw continuous face input images obtained from the UMDAA-02 Face Dataset [26] is obtained as input. Next, preprocessing on the raw continuous face input images are performed by non-local mean function. Followed by, which the essential and pertinent continuous feature is extracted by employing Cauchy kriging function. Next, the continuous extracted features are utilized for classification. Continuous Czekanowski's function is applied for validation. The results of continuous Czekanowski's function are given to the output layer for providing final classification results via activation function. If the activation function provides output '1', then the user is genuine user. On the other hand, if the activation function provides the output as '0', the user is attacker or intruder and thus the phone goes to the locked state. In this way, implicit continuous user authentication is achieved with maximum accuracy.

Algorithm 1: Gaussian Weighted Cauchy Kriging Continuous Czekanowski's-based implicit continuous authentication

```
Input: Dataset '$DS$', Images '$I = I_1, I_2, \ldots, I_n$'
Output: Accurate and timely implicit continuous authentication
Step 1: Inxitialize pixel data vector 'PV', search window size 'SWS'
Step 2: Initialize filtering parameters '$\alpha$', '$\beta$'
Step 3: Initialize deterministic coefficient '$\gamma_i$', stochastic kriging weights '$\lambda_j$'
Step 4: Begin
//input layer
Step 5: For each Dataset '$DS$'
    Step 6: Formulate pixel data vector '$PV$' as in Eq. (1)
    //hidden layer 1 – preprocessing
    Step 7: Restore the noisy pixel gray-value data '$PD(i)$' as in Eq. (2)
    Step 8: Estimate non-local mean weight as in Eq. (3)
    Step 9: Return preprocessed data or preprocessed continuous sampling images '$SI = SI_1, SI_2, \ldots, SI_n$'
Step 10: End for
//hidden layer 2 – feature extraction
Step 11: For each preprocessed continuous sampling images '$SI = SI_1, SI_2, \ldots, SI_n$' as in Eq. (4)
    Step 12: Formulate Regression Kriging as in Eq. (5)
    Step 13: Extract pertinent features as in Eqs. (6) and (7)
    Step 14: Return extracted data or extracted continuous response images '$P$' as in Eq. (8)
Step 15: End for
//hidden layer 3 – classification
Step 16: For each continuous extracted response images '$P$'
    Step 17: Estimate Continuous Czekanowski□s Classification as in Eq. (9)
Step 18: End for
//output layer
Step 19: If '$R = 1$'
    Step 20: Then the user is genuine
Step 21: End if
Step 22: If '$R = 0$'
    Step 23: Then the user is intruder
Step 24: End if
Step 25: End for
Step 26: End
```

4 Experimental Setup

Simulation analysis of proposed Gaussian Weighted Cauchy Kriging-based Continuous Czekanowski's (GWCK-CC) is implemented in MATLAB simulator. The results are analyzed using the UMDAA-02 Face Dataset (UMDAA-02-FD). The UMDAA-02-FD dataset includes number of front-facing camera images. The dataset is used for face Detection and verification tasks. The results of GWCK-CC method is compared with the existing Gait-based Continuous authentication (GaitCode) [1], Extremal Openset Rejection (EOR) [2], and Existing Continuous Dice Coefficient. The performance metrics used for analyzing the implicit continuous authentication process is user authentication accuracy, user authentication time, error rate, sensitivity and specificity with respect to different face images.

5 Discussion

Comparative analysis of implicit continuous authentication of mobile devices is performed using Gaussian Weighted Cauchy Kriging-based Continuous Czekanowski's (GWCK-CC) and compared with two different methods Gait-based Continuous authentication (GaitCode) [1], Extremal Openset Rejection (EOR) [2], and Existing Continuous Dice Coefficient. Performance analysis is made with five distinct parameters namely user authentication accuracy, user authentication time, error rate, sensitivity and specificity for different numbers of face images.

5.1 Performance Analysis of User Authentication Accuracy

The first and foremost parameter of significance for implicit continuous authentication is the user authentication accuracy. Higher the user authentication accuracy, higher the validation performance for mobile devices and therefore efficient the method is said to be. The user authentication accuracy is mathematically formulated as given below.

$$\mathrm{USA} = \sum_{i=1}^{n} \left(\frac{\mathrm{SI_{CA}}}{\mathrm{SI_i}} \right) * 100 \tag{11}$$

From the above Eq. (11), the user authentication accuracy 'USA' is measured based on the sample face images correctly authenticated '$\mathrm{SI_{CA}}$' to the sample images involved in the simulation process '$\mathrm{SI_i}$' of implicit continuous authentication for mobile devices. Tab. 1 given below provides the tabulation results for user authentication accuracy using four different methods, GWCK-CC, existing GaitCode [1], EOR [2], and Existing Continuous Dice Coefficient.

Table 1: Tabulation for user authentication accuracy

Face images	User authentication accuracy (%)			
	GWCK-CC	GaitCode	EOR	Existing continuous dice coefficient
500	97	95	92	90
1000	96.35	94.15	92.15	89.55
1500	96	94	90	88
2000	95.25	93.55	88.15	86
2500	94.25	91.25	86.35	84.15
3000	94	90	85	83
3500	93.15	89.15	84.15	82.45
4000	93	88.35	84	80
4500	92.55	88	81.55	79.15
5000	92	81	78	77

Tab. 1 shows the user authentication accuracy results of 5000 different face images acquired from different users at different time for simulation. From the above table it is inferred that the user authentication accuracy is inversely proportional to the different face images provided as input. In other words, increasing the face images results in the increase in the number of faces acquired from single users at a session and also increases in the stack value, therefore reducing a significant amount of correct authentication of face images. However, with simulations conducted for 500 face images, 485, 475, 460 and 450 faces were correctly authenticated using GWCK-CC, [1,2] and Existing Continuous Dice Coefficient. With this the user authentication accuracy using the four methods were observed to be 97%, 95%, 92%, and 90% respectively, therefore increasing the user authentication accuracy using GWCK-CC. The reason for that improvement is to apply GWCK-CC. The preprocessing is employed to separate the face area from the background segment. The process of preprocessing here starts by extracting pertinent features that differentiate between same faces acquired at different time intervals of continuous face images from the aligned face which is generated from the preprocessing stage. As a result, the user authentication accuracy is improved using GWCK-CC method by 4%, 10%, and 13% as compared to [1,2], and Existing Continuous Dice Coefficient respectively.

5.2 Performance Analysis of User Authentication Time

The second parameter of significance is the time consumed in authentication the user or the respective sample face images-based implicit continuous authentication for mobile devices. Lower the user authentication time is sooner the user or the particular sample face images are said to be validated and accordingly authenticated is performed. With minimum time consumed in the overall process, the genuineness of the user is measured at the initial stage itself. The user authentication time is mathematically formulated as given below.

$$\mathrm{UAT} = \sum_{i=1}^{n} \mathrm{SI_i} * \mathrm{Time}\ [\mathrm{AUTHENTICATION}] \tag{12}$$

From the above Eq. (12), the user authentication time 'UAT' is measured based on the sample face images provided as input '$\mathrm{SI_i}$' and the time consumed in performing the actual authentication process 'Time [AUTHENTICATION]'. It is measured in terms of milliseconds (ms). Fig. 5 given below provides the tabulation results for user authentication time using four different methods, GWCK-CC, existing GaitCode [1], EOR [2], and Existing Continuous Dice Coefficient.

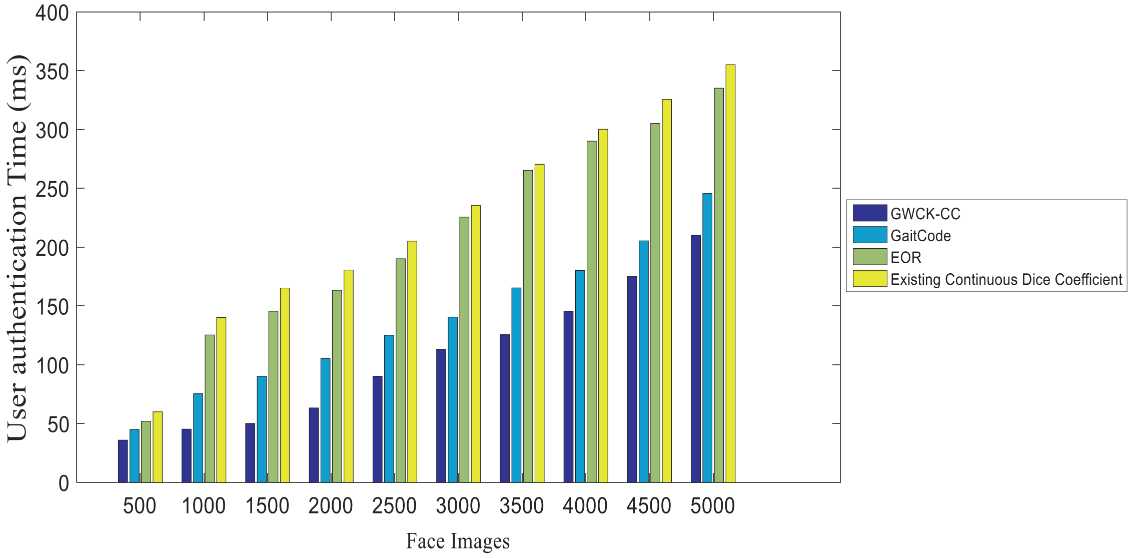

Figure 5: Graphical representation of user authentication time

Fig. 5 given above illustrates the user authentication time for performing implicit continuous authentication process. Here, x axis refers to the number of face images provided as input in the input layer and y axis refers to the user authentication time. From the above figure it is inferred that an increase in the number of face images results in the increase in the user authentication time. In other words increasing the face images causes increase in the number of continuous face images for a specific user for the corresponding session therefore causes significant increase in the user authentication time also. However, simulations conducted with 500 face images consumed 0.072 ms for predicting single face image data using GWCK-CC, 0.09 ms using [1], 0.104 ms using [2], and 0.120 ms using Existing Continuous Dice Coefficient. With this, the overall user authentication time using the four methods was observed to be 36, 45 ms [1], 52 ms [2] and 60 ms Existing Continuous Dice Coefficient respectively. From the simulation results, the user authentication time using GWCK-CC was comparatively lesser than [1,2], and Existing Continuous Dice Coefficient. The reason behind the improvement was due to the application of Gaussian Weighted Non-local Mean Filter Preprocessing model to achieve the noise reduction. It concentrates on identifying projection that maximizes the total non-local mean of the projected continuous image or data. So, the small variations in the background are eliminated in an automatic manner. Therefore, the procedure was faster. Owing to this fact, the overall user authentication time using GWCK-CC was said to be comparatively lesser than 26% [1], 51% [2], and 54% Existing Continuous Dice Coefficient respectively.

5.3 Performance Analysis of Error Rate

The error rate measures the difference between the actual user data and the predicted user data. While performing active authentication on mobile devices implicit continuous user authentication should be ensured in such a manner that the falsification of user authentication should be avoided. In other words, the error rate is mathematically formulated as given below.

$$\mathrm{ER} = \frac{1}{n}\sum_{i=1}^{n}(\mathrm{SI(DO)} - \mathrm{SI(MO)}) * 100 \tag{13}$$

From the above Eq. (13), the error rate 'ER' is measured based on the desired output of the sample images 'SI(DO)' and the model output of the sample images 'SI(MO)'. It is measured in terms of percentage. Tab. 2 given below provides the tabulation results for error rate using four different methods, GWCK-CC, existing GaitCode [1], EOR [2], and Existing Continuous Dice Coefficient.

Table 2: Tabulation for error rate

Face images	Error rate (%)			
	GWCK-CC	GaitCode	EOR	Existing continuous dice coefficient
500	2	4	7	9
1000	3.55	4.85	8.15	9.55
1500	4	5.35	11.35	12.45
2000	7	12.05	16	17
2500	8.25	14	15.35	17.55
3000	9.15	14.35	16	18
3500	11.35	15.15	16.15	18.25
4000	12	16.25	17	19
4500	12.45	17	18.25	20.55
5000	13	17.35	19	21

Tab. 2 shows the error rate for 5000 different face images. From the table it is inferred that increasing the face images causes a swift increase in the error rate also. However, simulation results shows that with 500 face images used for simulation with 480 images correctly authenticated, the model output using the four methods were observed to be 470, 460, 445, and 435. With this, the overall error rate was found to be 2%, 4%, 7% and 9% respectively. With this the error rate using the proposed GWCK-CC method was found to be comparatively lesser than [1,2] and Existing Continuous Dice Coefficient. The reason was due to the application of Gaussian Weighted Cauchy Kriging Continuous Czekanowski's-based implicit continuous authentication algorithm. Preprocessing is performed using Gaussian weight. Cauchy Kriging function is applied to reduce the dimensionality and validation is performed for implication continuous authentication on mobile devices. The error rate using GWCK-CC method is reduced by 32% compared to [1], 46% compared to [2], and 52% compared to Existing Continuous Dice Coefficient.

5.4 Performance Analysis of Sensitivity

Sensitivity rate compares the total number of face images that has been performed with implicit continuous authenticated with the total number of face images actually present. The main objective behind the measure of sensitivity is to predict the positive instances (TP) in the face video image dataset. In other words, the resultant value of sensitivity refers to that the subjects or face images predicted to have performed implicit continuous authentication. It is mathematically expressed as given below.

$$\text{Sen} = \frac{\text{TP}}{\text{TP} + \text{FN}} * 100 \tag{14}$$

From the above Eq. (14), sensitivity 'Sen' is measured based on the true positive rate 'TP' and the false negative rate 'FN' respectively. It is measured in terms of percentage (%). Fig. 6 given below provides the tabulation results for sensitivity rate using four different methods, GWCK-CC, existing GaitCode [1], EOR [2], and Existing Continuous Dice Coefficient.

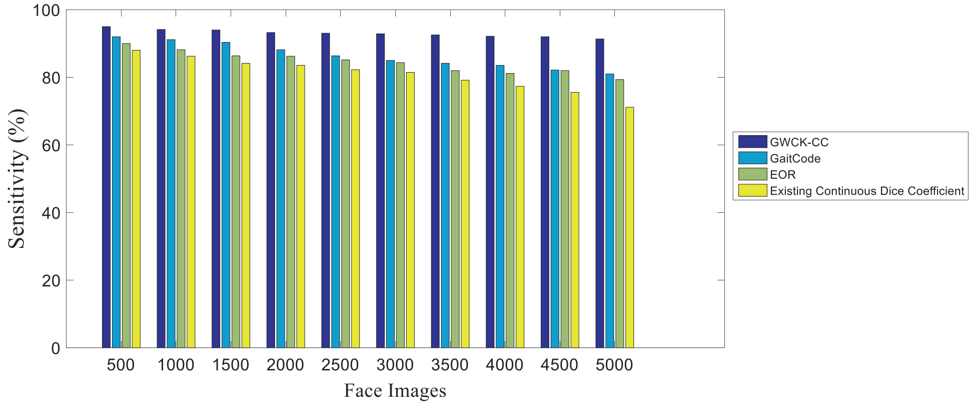

Figure 6: Graphical representation of sensitivity

Fig. 6 given above shows the sensitivity results for 5000 different face images collected from UMDAA-02 Face Dataset collected at different time instances. As shown in the above figure, increasing the number of face images causes a decrease in the sensitivity rate. In other words while increasing the face images for active authentication on mobile devices also decreases in a small amount. However, simulations with 500 faces show a true positive rate of 475, 460, 450 and 440 using the four methods, GWCK-CC method, GaitCode [1], EOR [2], and Existing Continuous Dice Coefficient. In a similar manner, the false negative rates were observed to be 25, 40, 50 and 60 using the GWCK-CC method, GaitCode [1], EOR

[2], and Existing Continuous Dice Coefficient. With this the overall sensitivity were observed to be 95% using GWCK-CC method, 92% using [1], 90% using [2], and 88% using Existing Continuous Dice Coefficient. The sensitivity was higher due to the application of Cauchy Kriging Regression for Feature Extraction using GWCK-CC method. Also, by applying Cauchy Kriging Regression results, the time complexity and as memory capacity are reduced. Only the projected continuous images are stored. Moreover, with the Cauchy Kriging Regression the residuals are found to be orthogonal to each other. Hence it circumvents redundant information, which in due course imparts comprehensive data compression and allows implicit continuous authentication for mobile devices. As a result, the sensitivity rate using GWCK-CC method is improved by 8%, 10%, 15% compared to [1,2], and Existing Continuous Dice Coefficient respectively.

5.5 Performance Analysis of Specificity

The specificity on the other end refers to the percentage ratio of negatives that are correctly identified (i.e., the proportion of those face images that has not been performed with implicit continuous authentication and also the face images that are correctly identified as not performed with implicit continuous authentication).

$$\mathrm{Spe} = \frac{\mathrm{TN}}{\mathrm{TN} + \mathrm{FP}} * 100 \tag{15}$$

From the above Eq. (15), specificity 'Spe' is measured based on the true negative rate 'TN' and the false positive rate 'FP' respectively. It is measured in terms of percentage (%). Tab. 3 given below provides the tabulation results for specificity rate using four different methods, GWCK-CC, existing GaitCode [1], EOR [2], and Existing Continuous Dice Coefficient.

Table 3: Tabulation for specificity

Face images	Specificity (%)			
	GWCK-CC	GaitCode	EOR	Existing continuous dice coefficient
500	94	90	88	85
1000	92.15	88.15	86.15	83.25
1500	91	86.35	84.25	82.15
2000	90.55	86	83	81
2500	90.25	84.25	82.15	80.55
3000	90	84	82	79
3500	88.35	83.15	81.85	78.15
4000	88	83	81	77
4500	87.25	82.55	80.25	76.15
5000	87	82	77	74

Tab. 3 given above shows the specificity for four different methods namely GWCK-CC, existing GaitCode [1], EOR [2], and Existing Continuous Dice Coefficient. Specificity is a measure of how well the implicit continuous authentication is measured in identifying the true negatives, the percentage ratio of true negatives out of all the face samples images involved in the simulation that do not have the condition (true negatives and false positives). From the figure a decreasing trend is set to be seen using all the four methods. However, simulation performed with 500 face sample images shows a true negative of 470, 450, 440, and 425 using the four methods, GWCK-CC, existing GaitCode [1], EOR [2], and Existing Continuous Dice Coefficient, false positive of 30, 50, 60 and 75 respectively. With this, the overall specificity rate was observed to be 94%, 90%, 88% and 85% using GWCK-CC, existing GaitCode [1], EOR [2] and Existing Continuous Dice Coefficient, therefore contributing towards the required objective. The reason behind the specificity improvement was due to the application of Continuous Czekanowski's Classification. Then, it performs not only continuous authentication but also correct authentication. Due to this, the specificity rate using GWCK-CC [1] method was found to be better by 6%, 9%, and 13% compared to [1,2] and Existing Continuous Dice Coefficient respectively.

6 Conclusion

In this paper, we proposed the use of a Gaussian Weighted Cauchy Kriging-based Continuous Czekanowski's (GWCK-CC) implicit continuous authentication on mobile devices. The objective for the authentication method was to ensure smooth process on mobile devices without the fear of the data or information being hacked. In this study, for each session, the face images of user were acquired continuously in a temporal basis. Gaussian weight was applied to the input continuous images to obtain fine-grained denoised images. Next, pertinent continuous features of the sample face images were extracted by employing Cauchy Kriging Regression. Finally, the classified output using Continuous Czekanowski's function was utilized to differentiate between normal and abnormal users. Compared with the continuous authentication results of the state-of-the-art methods, the user authentication accuracy, user authentication time, error rate, sensitivity and specificity of the generated GWCK-CC is relatively strong, which can accomplish very consequential effects and ensure robust authentication. The managerial and technical implications are based on the proposed method theory. To conduct the experiments, the results are implemented by using UMDAA-02-FD with higher authentication accuracy by 9%, lesser authentication time, and error rate by 44%, and 43% than the state of art works. The proposed GWCK-CC method limitation is that it failed to identify the different types of attack. In the future, instead of using deep learning, other variant in the deep learning can be utilized to extract features. In addition, ensemble learning could be employed to categorize the valid and invalid set of activities of user.

Funding Statement: The authors received no specific funding for this study.

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

References

[1] I. Papavasileiou, Z. Qiao, C. Zhang, W. Zhang, J. Bi *et al.,* "GaitCode: Gait-based continuous authentication using multimodal learning and wearable sensors," *Smart Health*, vol. 19, pp. 1–18, 2021.

[2] P. Perera and V. M. Patel, "Face-based multiple user active authentication on mobile devices," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1240–1250, 2019.

[3] P. Kumari and K. R. Seeja, "A novel periocular biometrics solution for authentication during covid-19 pandemic situation," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 10321–10337, 2021.

[4] A. B. A. Ali, V. Ponnusamy, A. Sangodiah, R. Alroobaea, N. Z. Jhanjhi *et al.,* "Smartphone security using swipe behavior-based authentication," *Intelligent Automation & Soft Computing*, vol. 29, no. 2, pp. 571–585, 2021.

[5] M. A. Alqarni, S. H. Chauhdary, M. N. Malik, M. Ehatisham-ul-Haq and M. A. Azam, "Identifying smartphone users based on how they interact with their phones," *Human-Centric Computing and Information Sciences*, vol. 10, no. 7, pp. 1–14, 2020.

[6] M. Abuhamad, A. Abusnaina, D. Nyang and D. Mohaisen, “Sensor-based continuous authentication of smartphones’ users using behavioral biometrics: A contemporary survey,” *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 65–84, 2021.

[7] Ö. D. Incel, S. Gunay, Y. Akani, Y. Barlas, O. E. Basar *et al.,* “DAKOTA: Sensor and touch screen-based continuous authentication on a mobile banking application,” *IEEE Access*, vol. 9, pp. 38943–38960, 2021.

[8] R. Wang and D. Tao, “Context-aware implicit authentication of smartphone users based on multi-sensor behavior,” *IEEE Access*, vol. 7, pp. 119654–119667, 2019.

[9] S. Vhaduri, S. V. Dibbo and W. Cheung, “HIAuth: A hierarchical implicit authentication system for IoT wearables using multiple biometrics,” *IEEE Access*, vol. 9, pp. 116395–116406, 2021.

[10] F. Anjomshoa, M. Aloqaily, B. Kantarci, M. Erol-Kantarci and S. Schuckers, “Social behaviometrics for personalized devices in the internet of things era,” *IEEE Access*, vol. 5, pp. 12199–12213, 2017.

[11] Y. Li, H. Hu, G. Zhou and S. Deng, “Sensor-based continuous authentication using cost-effective kernel ridge regression,” *IEEE Access*, vol. 6, pp. 32554–32565, 2018.

[12] F. Nakayama, P. Lenz, S. Banou, M. Nogueira, A. Santos *et al.,* “A continuous user authentication system based on galvanic coupling communication for s-health,” *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–11, 2019.

[13] F. H. Al-Naji and R. Zagrouba, “CAB-IoT: Continuous authentication architecture based on blockchain for internet of things,” *Journal of King Saud University-Computer and Information Sciences*, pp. 1–18, 2020. [Online]. Available: https://doi.org/10.1016/j.jksuci.2020.11.023.

[14] V. Shankar and K. Singh, “An intelligent scheme for continuous authentication of smartphone using deep auto encoder and softmax regression model easy for user brain,” *IEEE Access*, vol. 7, pp. 48645–48654, 2019.

[15] P. A. Thomas and K. P. Mathew, “A broad review on non-intrusive active user authentication in biometrics,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–22, 2021. [Online]. Available: https://doi.org/10.1007/s12652-021-03301-x.

[16] I. Stylios, S. Kokolakis, O. Thanou and S. Chatzis, “Behavioral biometrics & continuous user authentication on mobile devices: A survey,” *Information Fusion*, vol. 66, pp. 76–99, 2021.

[17] M. Abuhamad, T. Abuhmed, D. Mohaisen and D. Nyang, “AUToSen: Deep learning based implicit continuous authentication using smartphone sensors,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5008–5020, 2020.

[18] W. R. Almeida, F. A. Andaló, R. Padilha, G. Bertocco, W. Dias *et al.,* “Detecting face presentation attacks in mobile devices with a patch-based CNN and a sensor-aware loss function,” *PLOS ONE*, vol. 15, no. 9, pp. 1–24, 2020.

[19] S. Gupta, A. Buriro and B. Crispo, “Demystifying authentication concepts in smartphones: Ways and types to secure access,” *Mobile Information Systems*, vol. 2018, pp. 1–16, 2018.

[20] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed and M. Xu, “A survey on machine learning techniques for cyber security in the last decade,” *IEEE Access*, vol. 8, pp. 222310–222354, 2020.

[21] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen *et al.,* “Performance comparison and current challenges of using machine learning techniques in cyber security,” *Energies*, vol. 10, no. 13, pp. 1–30, 2020.

[22] V. M. Patel, R. Chellappa, D. Chandra and B. Barbello, “Continuous user authentication on mobile devices: Recent progress and remaining challenges,” *IEEE Signal Processing Magazine*, vol. 33, no. 4, pp. 1–24, 2016.

[23] C. Boutilier and B. Price, “Accelerating reinforcement learning through implicit imitation,” *Journal of Artificial Intelligence Research*, vol. 19, no. 1, pp. 569–629, 2003.

[24] K. Shaukat, S. Luo, S. Chen and D. Liu, “Cyber threat detection using machine learning techniques: A performance evaluation perspective,” in *2020 Int. Conf. on Cyber Warfare and Security (ICCWS)*, Islamabad, Pakistan, pp. 1–6, 2020. https://doi.org/10.1109/ICCWS48432.2020.9292388.

[25] B. Recht, “A tour of reinforcement learning: The view from continuous control,” *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 2, pp. 253–279, 2019.

[26] U. Mahbub, S. Sarkar, V. M. Patel and R. Chellappa, “Active user authentication for smartphones: A challenge data set and benchmark results,” in *2016 IEEE 8th Int. Conf. on Biometrics Theory, Applications and Systems (BTAS)*, Niagra Falls, NY, USA, pp. 1–8, 2016.